Informatica® Managed File Transfer
10.5.3

Managed File Transfer User Guide

Informatica Managed File Transfer Managed File Transfer User Guide
10.5.3
December 2022

Publication Date: 2022-12-13

Table of Contents

Preface

Use the *Managed File Transfer User Guide* to learn how to get started with Managed File Transfer and how to automate data exchanges with channel partners and run the full range of file transfer tasks. The guide describes the Managed File Transfer dashboard and provides information about workflows, tasks, services, users, logs and reports, encryption, and Managed File Transfer system settings.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

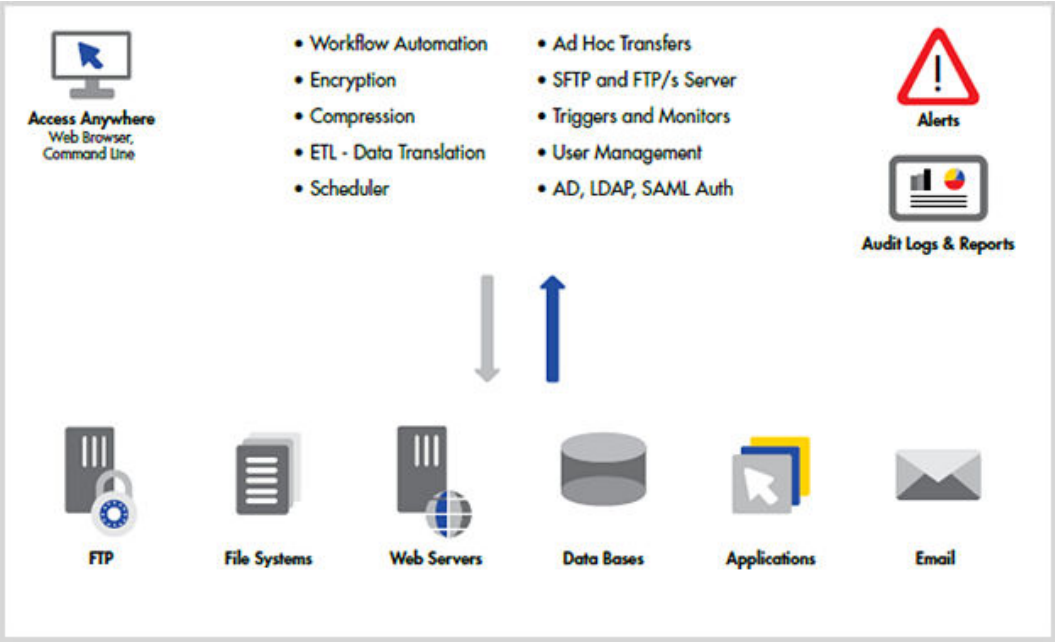
Introduction

Managed File Transfer is an enterprise-level solution that automates, streamlines, and secures document file transfer for organizations, and is fully integrated with the Informatica product suite. With its comprehensive features and intuitive interface, Managed File Transfer will reduce operational costs, improve the quality of data transmissions and meet stringent compliance requirements. It seamlessly integrates with Informatica products to offer secure, efficient, comprehensive, and auditable data exchange with customers and partners.

With Managed File Transfer, you can run workflows to transfer, encrypt and process the files with B2B Data Exchange. You can schedule file transfers and monitor folders for incoming files that require immediate processing. You can securely encrypt and decrypt files, and use SFTP, SCP, FTPS, AS2, or HTTPS protocols to ensure safe file transmission. Managed File Transfer tracks all file transfer activity and allows you to view activity in the dashboard or in PDF format to address auditing needs.

With Managed File Transfer you can fully automate data exchanges with channel partners, both large and small, for greater efficiency and improved operational performance. When integrated with Informatica tools, you harness advanced data transformation, data quality, and data management for data in virtually any format or of any complexity.

The following figure shows the platforms and features that Managed File Transfer supports:



Note: You must use Managed File Transfer with Informatica B2B Data Exchange or Informatica Cloud B2B Gateway. You cannot use Managed File Transfer features independently of B2B Data Exchange or Cloud B2B Gateway. Also, you cannot use Managed File Transfer for any operations other than file transfer operations.

For more information, see the Statement of Support.

Managed File Transfer General Features

Managed File Transfer has the following features:

- Runs on Windows and Unix.
- Includes a browser-based administrator interface with a customizable dashboard, advanced graphical components and drag-n-drop support.
- Supports popular file transfer protocols including SFTP, SCP, FTP/s, HTTP/s, AS2, Web Services, SMTP, POP3, MLLP, and IMAP.
- Provides client components for connecting to internal and external systems for sending and retrieving files.
- Provides server components to allow systems and users to connect to Managed File Transfer for uploading and downloading files.
- Logs all file transfer activity in a central database with an optional SYSLOG feed.
- Produces a wide variety of management and analytical reports.
- Allows clustering for high availability (active-active) and load balancing.
- Controls user access with role-based permissions and extensive security controls.
- Includes key management tools for Open PGP Keys, SSH Keys and SSL Certificates.
- Works with the optional Managed File Transfer Gateway to keep files out of the DMZ and close inbound ports into the internal (private) network.

Informatica Managed File Transfer can be used for a variety of file transfer needs including workflow automation, ad-hoc file transfers and document collaboration. It can simplify system-to-system, user-to-system and user-to-user file transfers.

Workflow Automation

- Provides a graphical interface for creating multi-step workflows; no scripting or programming required.
- Includes an integrated scheduler for running workflows and file transfers at future dates/times.
- Triggers workflows based on events, such as an upload/download event or the presence of a new file in a folder.
- Provides APIs and commands for running workflows from customer applications and 3rd party schedulers.
- Encrypts, signs, verifies and decrypts files using the Open PGP encryption standard.
- Accesses files and directories on network shares with support for NFS, SMB and CIFS.
- Connects to SQL Serve and Oracle.
- Translates data to/from Excel, XML, Delimited text and Fixed Width file formats.
- Calls customer programs and scripts as part of an overall workflow.
- Connects to enterprise messaging systems including Websphere MQ, SonicMQ, ActiveMQ and SwiftMQ.
- Compresses and extracts files using ZIP, GZIP and TAR standards.

- Supports large files with auto-resume and integrity checks to help guarantee delivery.
- Allows workflow jobs to be prioritized and segmented with job queues and run priorities.
- Sends email alerts and text messages for failed and completed transfers.

Ad-Hoc File Transfers and Collaboration

- Provides an HTTPS File Transfer Portal for browser-based file transfers.
- Allows access to authorized network folders through the browser.
- Includes the Shared Drive file system for collaboration, sharing and synchronizing documents across devices.
- Provides delivery of sensitive messages and documents through email notifications with secure HTTPS links.
- Integrates with Active Directory (AD), LDAP, and SAML for user authentication.
- Allows self-registration of users with administrator approval.

Getting Started

Authorized users can utilize the Managed File Transfer browser-based dashboard to perform configuration and monitoring within the product. Follow these steps to get started with Managed File Transfer.

1. Review and modify the "Global Settings" on page 752 for Managed File Transfer.
2. Set up "Admin Users" on page 576 and "Admin Groups" on page 581 with their applicable roles and permissions.
3. To enable Web Users, for example trading partners, to connect to Managed File Transfer to upload or download files, perform the following steps:
    a. Configure the "Login Methods Management" on page 647, the "Web User Settings" on page 641 and "Web User Templates" on page 622 for Web Users.
    b. Create the "Web Users" on page 589 and "Web User Groups" on page 614 authorized to work with Managed File Transfer.
    c. Configure the protocols and ports (SFTP server, FTP/s server, HTTP/s server) through the "Service Manager" on page 516 page.
    d. Define "Trigger Manager" on page 206 to execute specified actions when certain conditions are met.
4. To automate and schedule file transfers in Managed File Transfer, perform the following steps:
    a. Create Chapter 3, "Resources" on page 42 for any systems you wish to connect to for sending/retrieving data (e.g. SFTP servers, FTP servers, database servers, mail servers, etc.).
    b. Set up Keys and Certificates for any Chapter 9, "Encryption" on page 700 requirements.
    c. Create Chapter 4, "Workflows" on page 100 of any tasks that need to be automated (for example, file transfers, data conversions, file encryption, compression, etc.).

d. "Scheduling Projects" on page 187 Projects to run at future dates and times. Additionally you can execute Projects through folder "Monitors" on page 197.

Note: The term "Admin Users" is used to indicate those individuals that are allowed to perform administration functions in Managed File Transfer. The term "Web Users" indicates the credentials for connecting to a service (e.g. SFTP, HTTPS, etc.) in Managed File Transfer.

Screen Tips

- Required fields are indicated with a red asterisk *.
- On-line help is available on each page by clicking the ? icon.
- By default, the Managed File Transfer administrator will timeout your browser session after 60 minutes of inactivity. This session timeout can be configured in the "Security Settings" on page 585.
- If a variable can be used within a field, the ${var} icon appears beside the field when the field is selected. Click the icon to open a drop-down list of available system and user-defined variables in the open Project.

  Note: Use the buttons and links provided in Managed File Transfer to navigate. Do not use the Back, Forward or Refresh buttons in your browser since it may cause out of sync issues.

Login

Follow the steps below to login to Managed File Transfer:

1. From your browser, type the URL where Managed File Transfer is installed, using the format *https://[hostname]:[https-portnumber]/informaticamft* or *http://[hostname]:[http-portnumber]/informaticamft*.
   - *[hostname]* is the host name or IP address of the Managed File Transfer server
   - *[portnumber]* is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, http://myserver:8000 or https://myserver:8002.
2. Login with your User Name and case-sensitive Password. The default User Name is **Administrator** and the default Password is **Administrator**.

Note: The System Name is only displayed if this system is a member of the Managed File Transfer cluster. For more information, see "Clustering" on page 772.

CHAPTER 2

Dashboard

The Managed File Transfer Dashboard is displayed after login. The Dashboard provides drop-down menus and links to quickly access features within Managed File Transfer, along with customizable Gadgets that display vital system statistics and file transfer activity.

The page header displays the Managed File Transfer environment name, the system name of the local server (when running in cluster mode) and the logged in Admin User. The last login time and date for the Admin User can be displayed by hovering over the user name.

Each Admin User has their own Dashboard named "My Dashboard", which can be tailored to display only those "Gadgets" on page 31 which are important to them. Admin Users can create additional Dashboards as needed, each with their own set of Gadgets. If the Admin User has the Dashboard Manager Role, these customized Dashboards can be shared with other Admin Users.

Main Menu Bar

To access a Managed File Transfer feature, select it from a drop-down list on the main menu bar.

Dashboard Page Toolbar

The "Manage Dashboards" on page 31 page toolbar allows you to add custom gadgets and edit the dashboard layout.

- Select a different Dashboard by clicking the button (located on the left side of the Dashboard name) and then choose the dashboard to display. Alternatively, you can choose "Manage Dashboards" on page 31 to create a new Dashboard.
- Add "Gadgets" on page 31 to the Dashboard by clicking the **Add Gadget** button.
- Edit the dashboard column layout by clicking the **Edit Layout** button. From that dialog, you can select a single column, two column, or three column layout.
- Refresh the statistics and data on every Gadget by clicking the **Refresh** button.

Organize Gadgets

"Gadgets" on page 31 can be organized on your Dashboard by selecting the Gadget header and dragging the Gadget to another area on the Dashboard page. A blue drop zone will appear above or below the destination Gadget. Hover over a drop zone and release the mouse button to place the Gadget in the new location.

Manage Dashboards

The Manage Dashboard page allows Admin Users to add, edit, or delete Dashboards they have created. Admin Users with the Dashboard Manager "Admin Roles Management" on page 584 can share a Dashboard with all other Admin Users.

Page Toolbar

Use the page toolbar to perform the following actions:

- Click the **Add Dashboard** button to create a new Dashboard. Specify the following fields:
  Name

  Provide a name for the Dashboard. This appears in the Dashboard header.

  Share With Everyone

  Admin Users with the Dashboard Manager Role can make the Dashboard available to all other Admin Users. Admin Users can select the shared Dashboard by clicking the button (located on the left side of the Dashboard name).
- Click the **Done** button to return to the Home page.

Manage Dashboard Actions

The following actions are available by selecting the Actions icon:

- Click the **View** button to select the Dashboard to display on the Home page.
- Click the **Edit** button to update the name and sharing option.
- Click the **Delete** button to remove the Dashboard. If the Dashboard was shared with other Admin Users, they will no longer be able to access it.

Gadgets

Gadgets allow you to quickly display vital Managed File Transfer statistics and activity from within the Dashboard, as well as to provide quick links to commonly used features in the product. To access an authorized Gadget, you must log in as an Admin User with the appropriate "Admin Roles" on page 583 for that Gadget.

Add A Gadget

Use the following instructions to add a Gadget to a Dashboard:

1. Login to Managed File Transfer.
2. If needed, you can choose a different Dashboard to customize by clicking the button (located on the left side of the Dashboard name) and select a Dashboard.
3. Click the **Add Gadget** button.
4. On the Add Gadget window, select the desired Gadget.
5. The Gadget is added to the Dashboard.

Gadget Options

Click the button on the Gadget header to view the Gadget's options:

Edit the Gadget name and any optional parameters. Each Gadget's optional parameters are detailed in the Available Gadgets section below.

Refresh the data displayed on the Gadget.

View More Details about the information displayed on the Gadget.

Remove the Gadget from the Dashboard.

Service Statistics - Inbound Connections

The Service Statistics Gadget displays Upload and Download file transfer activity for "Service Manager" on page 516. Click on an area of the pie chart to view the "Active Sessions" on page 564 for the selected protocol.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the number of days of file transfer activity to display.

Protocols

Specify the service protocols to display.

Service Status

The Service Status Gadget displays the status and active sessions for each service. Click on the Active Sessions link to view the "Active Sessions" on page 564 for the selected protocol. The More Details link displays the "Service Manager" on page 516 page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Services

Specify the services to display on the Gadget.

Active Sessions - Summary

The Active Sessions -Summary Gadget displays the number of active sessions by service. Click on an area of the pie chart to view the "Active Sessions" on page 564 for the selected protocol.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Services

Specify the services to display on the Gadget.

Active Sessions - Detail

The Active Sessions - Detail Gadget displays the IP address, User, and Protocol for each Active session. The More Details link displays the "Active Sessions" on page 564 page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Services

Specify the services to display on the Gadget.

Rows to Display per Page

Specify the number of active sessions to display on the Gadget.

Job Statistics

The Job Statistics Gadget displays a pie chart of the number of Active, Successful, Failed, or Canceled Jobs. Click the pie chart to view the "Completed Jobs" on page 223 log for the selected status.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the number of days of Job activity to display.

Active Jobs

The Active Jobs Gadget displays details for active Jobs and the number of Jobs in the queue. Click the number of Jobs link to view the "Work with Queued Jobs" on page 220 page.

To customize the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Completed Jobs - Summary

The Completed Jobs - Summary Gadget displays a bar graph of the number of completed Jobs within the specified date and time range.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Status

Narrow the data displayed in the Gadget based on the Job Status.

Group By

Specify the hour, day, or month value the statistics will be grouped by.

Date Range

Specify the scope of the statistics based on date and time.

Recent Completed Jobs

The Recent Completed Jobs Gadget displays to most recent completed Jobs and their completion status. Click the Job Number link to view the "Completed Jobs" on page 223 page for the selected Job. Click the More Details link to view all the Completed Jobs.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Status

Narrow the data displayed in the Gadget based on the Job Status.

Rows to Display per Page

Specify the number of active sessions to display on the Gadget.

File Transfer - Summary

The File Transfer - Summary Gadget displays a bar graph of the number of file transfers within the specified time range.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the scope of the statistics based on date and time.

Group By

Specify the hour, day, or month value the statistics will be grouped by.

Module

Specify the Managed File Transfer modules that will be included in the file transfer statistics.

Recent File Activity

The Recent File Activity Gadget displays the recent files that have been transferred, the module that was used to transfer the file, and the user who initiated the transfer. Click the User link to view their activity in the "Global Search" on page 670 page, or click the More Details link to see all the latest activity on the Global Search page.

To customize the data available within the Gadget, click on the  button (on the Gadget header) an then click the  **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Module

Specify the Managed File Transfer modules that will be included in the file transfer statistics.

Status

Narrow the data displayed in the Gadget based on the file transfer status.

Rows to Display

Specify the number of transfers to display on the Gadget.

Recent Web User Logins

The Recent Web User Logins Gadget displays the most recent Web User Logins, the date and time the Web User logged in, the service they logged in to, and the status of the login attempt. Click the User link to view their account on the "Web User Management" on page 589 management page.

To customize the data available within the Gadget, click on the  button (on the Gadget header) an then click the  **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Protocol

Specify the service protocols to display.

Status

Narrow the data displayed in the Gadget based on the login attempt status.

Rows to Display

Specify the number of Web User logins to display on the Gadget.

Recent Web User Activity

The Recent Web User Activity Gadget displays recent Web User Activity, the modules impacted, and the status of the activity. Click the User link to view that user's activity in the "Global Search" on page 670 page, or click the More Details link to see all the latest activity from every user on the Global Search page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Modules

Specify the Managed File Transfer modules that will be included in the Web User Activity details.

Status

Narrow the data displayed in the Gadget based on the activity status.

Rows to Display

Specify the number of recent Web User activities to display on the Gadget.

Recent Secure Mail Activity

The Recent Secure Mail Activity Gadget displays recent Secure Mail activity, the recipient of the Secure Mail message, and the message status. Click the User link to view the message on the "Package Manager" on page 571 page, or click the More Details link to view all the messages on the Package manager page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Rows to Display

Specify the number of recent Secure Mail activities to display on the Gadget.

Recent Blacklisted IP Addresses - Detail

The Recent Blacklisted IP Addresses Gadget displays IP address that were recently blocked due to invalid login attempts. Click the More Details link to view the "Automatic IP Blacklist" on page 783 page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the scope of the results based on date and time.

Rows to Display per Page

Specify the number of recent blacklisted IP addresses to display on the Gadget.

Recent Triggers

The Recent Triggers Gadget displays recent Trigger activity and the status of the Trigger event. Click the Trigger Name link to view the "Trigger Log" on page 688 for that event, or click the More Details link to view all the Trigger history on the "Trigger Log" on page 688.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Status

Narrow the data displayed in the Gadget based on the activity status.

Rows to Display

Specify the number of recent Triggers to display on the Gadget.

Top Web Users by Transfers

The Top Web Users by Transfers Gadget displays the Web Users who have the most file upload and download activity across each of the selected modules. Click the User link to view their transfers in the "Global Search" on page 670 log.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the scope of the statistics based on date and time.

Module

Specify the Managed File Transfer modules that will be included in the Web User transfer details.

Rows to Display

Specify the number of Web Users to display on the Gadget.

Summarize By

Specify if the Gadget will be summarized by the number of transfers per Web User, or total number of bytes transferred per Web User.

Transfer Type

Specify the type of transfer displayed.

Top Shared Drive Users by Disk Usage

The Top Shared Drive Users by Disk Usage Gadget displays the Web Users who have the most files stored in Shared Drive. Click the User link to view the "Web User Management" on page 589 page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Rows to Display

Specify the number of rows to display on the Gadget.

Top Secure Mail Users By Disk Usage

The Top Secure Mail Users by Disk Usage Gadget displays the Web Users who utilize the largest amount of file storage in Secure Mail. Click the User link to view the "Web User Management" on page 589 page.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Rows to Display

Specify the number of rows to display on the Gadget.

Top Secure Mail Packages by Size

The Top Secure Mail Packages by Size Gadget displays the Web Users who have the largest Secure Mail Packages, and the recipient email address where the Package was sent. Click the User link to view that package in the "Package Manager" on page 571.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Rows to Display

Specify the number of rows to display on the Gadget.

Expiring SSL Certificates

The Expiring SSL Certificates Gadget displays certificates that will be expiring within the specified date range.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the scope of the results based on the number of days before the certificate will expire.

Expiring OpenPGP Keys

The Expiring OpenPGP Keys Gadget displays OpenPGP Keys that will be expiring within the specified date range. Click the More Details link to view the "Work with OpenPGP Keys" on page 724.

To customize the data available within the Gadget, click on the button (on the Gadget header) an then click the **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Date Range

Specify the scope of the results based on the number of days before the key will expire.

Unresolved Jobs

The Unresolved Jobs Gadget displays failed or canceled Jobs that have not been marked Resolved from the Completed Jobs page. Click the Job Number link to view the "Completed Jobs" on page 223 log for the failed job, or click the More Details link to view all the failed or canceled Job history.

To customize the data available within the Gadget, click on the  button (on the Gadget header) an then click the  **Edit** button.

Optional Parameters

The following optional parameters are available:

Title

Specify a title for the Gadget.

Status

Narrow the data displayed in the Gadget based on the Job status.

Rows to Display

Specify the number of failed or canceled jobs to display on the Gadget.

Date Range

Specify the scope of the results based on the number of days.

CHAPTER 3

Resources

Resources are the names and connection properties of the servers, and other data sources, that Managed File Transfer can interact with. Admin users with the Resource Manager role can create and edit Resources. The defined Resources can be used within Managed File Transfer by choosing the Resource names from simple drop-down lists.

Listed below are the Resource types that can be defined in Managed File Transfer.

 "Network Shares" on page 52

The names and connection properties of shared file locations on a network to which Managed File Transfer can connect for accessing files.

 "Database Servers Resource" on page 54

The names and connection properties of the database servers to which Managed File Transfer can connect. Database servers supported include DB2, Oracle, SQL Server 2000 and later, Sybase, Informix, PostgreSQL, and MySQL.

 "FTP Servers Resource" on page 55

The names and connection properties of the FTP servers to which Managed File Transfer can connect to send and receiving files.

 "FTPS Servers Resource" on page 59

The names and connection properties of the FTPS servers (FTP over SSL) to which Managed File Transfer can connect to send and receiving files.

 "SFTP Servers Resource" on page 66

The names and connection properties of the SSH Servers which Managed File Transfer can connect to. These resources can be used for SFTP transfers (SSH File Transfer Protocol), SCP file transfers (Secure Copy) and running remote SSH commands.

 "AS2 Servers Resource" on page 72

The names and connection properties of the AS2 servers (Applicability Statement 2) to which Managed File Transfer can connect to send files.

 "MLLP Servers Resource" on page 76

The names and connection properties of the MLLP servers to which Managed File Transfer can connect to send files.

 "SMTP Servers Resource" on page 78

The names and connection properties of the SMTP servers (Mail Servers) to which Managed File Transfer can connect to send emails.

 "Mail Boxes Resource" on page 79

The names and connection properties of the Mail Boxes (POP-3 and IMAP) to which Managed File Transfer can connect for receiving emails.

 "HTTP Servers Resource" on page 81

The names and connection properties of the HTTP servers to which Managed File Transfer can connect to send and receiving files.

 "HTTPS Servers Resource" on page 83

The names and connection properties of the HTTPS servers (HTTP over SSL) to which Managed File Transfer can connect to send and receiving files.

 "ICAP Resource" on page 87

The name and connection properties of the ICAP servers (for Data Loss Prevention) to which Managed File Transfer can connect to send files and receiving confirmation the files do not contain restricted content.

 "MQ Servers Resource" on page 89

The names and connection properties of the Message Queue servers (MQ) to which Managed File Transfer can connect to send and receiving messages.

 "OpenPGP Key Rings Resource" on page 91

The names of the OpenPGP Key Rings that can be used in Managed File Transfer to encrypt and decrypt files using the OpenPGP standard.

"Informatica MFT Server Resource" on page 92

The names and connection properties of additional Informatica MFT servers to which this Managed File Transfer instance can connect for executing *Projects*.

"Informatica HTTPS Server Resource" on page 96

The names and connection properties of the Informatica HTTPS Servers (HTTPS Service in Managed File Transfer) to which Managed File Transfer can connect to send and receiving files.

Work with Resources

To work with Resources, log in as an Admin User with the **Resource Manager** or Security Officer role and click the **Resources** link from the main menu.

Click the type of Resource to work with. A list of Resources opens on the right-side of the page for that Type. Listed below is an example of Database Servers.

You can filter for any resource types from any field within a resource. You can search for resource using strings, parameters, name of an attribute, the ending or middle string of an email id, a resource name, description string, or any other parameters such as host, user, directory, and so on.

The list of resources can also be sorted by clicking a column name. A sort direction arrow shows the sorted column. Click the column name again to toggle the sort direction.

Page Toolbar

The following actions are available from the page toolbar:

Add a Resource by clicking the **Add** button.

Resource Actions

The following actions are available by selecting the Actions icon.

- Edit a Resource by clicking the icon.
- Copy a Resource by clicking the icon.
- Delete a Resource by clicking the icon.
- View a Resource by clicking the icon.
- View Resource information by clicking the icon.
- "Search Resources" on page 49 to see which Projects and Monitors use the Resource by clicking the icon.
- View the "File Audit Log" on page 690 Audit Log for the Resource by clicking the icon.
- Test a resource by clicking the icon.
- Export a Resource by clicking the **Export** option.
- "Promoting a Resource" on page 50 a Resource by clicking the **Promote** option.
- Edit the "Resource Permissions" on page 45 for a Resource by clicking the icon.

Note: An Admin User must have "Write" "Edit Resource Permissions" on page 46 for the Resource in order to edit or delete it. An Admin User must have "Read" permission to view a Resource either by Resource Type or in the Resource Search Results page.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Resources.
- "Promoting a Resource" on page 50 one or more selected Resources to another Managed File Transfer server.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Resource Permissions

Permissions (authorities) for a Resource can be granted to individual Admin Users and Groups of Admin Users. The following three types of permissions can be granted:

Permission	Description
Read	Allows any Admin User with the Resource Manager role to view the settings for the Resource.
Write	Allows any Admin User with the Resource Manager role to change the settings or delete the Resource.
Use	Allows Admin Users to utilize the Resource when executing a Project.

For instance, you may have a FTP server resource that only certain users should be able to utilize (connect to). If you additionally do not want these users to change the settings on the FTP server, then you would give the Admin Users the permission of **Use** only to that Resource.

Note: By default, the All Users Group will be granted Read/Write/Use permissions to a Resource when it is added. This Public authority will allow other Resource Managers to view/edit the properties for the Resource and other users to utilize the Resource when executing a Project. It is recommended to remove all users permissions from any Resources that should have restricted access. The default permissions for the All Users Group can be changed on the Security Settings page.

Adding Resource Permissions

Follow the instructions below to add permissions to a Resource:

1. Permissions can be added to a Resource using the **Add Permissions** page. To access this page:
   a. Log in as an Admin User with the Security Officer role.
   b. Click the **Resources** link from the main menu.
   c. Click the Resource type to work with.
   d. A list of Resources will be displayed.
   e. Click the  icon next to the Resource for which you wish to edit the permissions.
   f. The current Resource permissions will be displayed.
   g. Click the  **Add Permissions** link (located towards the top of the page).
2. To authorize users to the Resource:
   a. On the left side of the page, select (highlight) the users to assign to the Resource. Multiple entries can be selected by holding down the Ctrl or Shift key while clicking the mouse.
   b. Click the arrow.
   c. The selected users will move to the right side of the page.
3. To authorize groups to the Resource:
   a. On the left side of the page, select (highlight) the groups to assign to the Resource. Multiple entries can be selected by holding down the Ctrl or Shift key while clicking the mouse.
   b. Click the arrow.
   c. The selected groups will move to the right side of the page.

4. Select the permissions for the Users and Groups by clicking the **Read**, **Write** and/or **Use** boxes.
5. Click the **Save** button to apply the changes.

You can set permissions to multiple resources through command line interface. For more information, see the *Command Line Reference* guide.

Edit Resource Permissions

Follow the instructions below to change the permissions for a Resource:

1. Permissions can be edited for a Resource using the **Resource Permissions** page. To access this page:
   a. Log in as an Admin User with the Security Officer role.
   b. Click the **Resources** link from the main menu.
   c. A list of Resource types will be displayed (database servers, FTP servers, HTTP servers, etc.).
   d. Click the Resource type to work with.
   e. A list of Resources will be displayed.
   f. Click the  icon next to the Resource that you wish to edit the permissions for.
   g. The current Resource permissions will be displayed.
2. Select or deselect the permissions for the Users and Groups by checking on or off the boxes next to those users and groups.
3. If desired, click the "Adding Resource Permissions" on page 45 link in the page toolbar to grant permissions to additional Users or Groups.
4. Click the **Save** button to apply the changes.
5. Click the **Done** button to leave the permissions page.

You can set permissions to multiple resources through command line interface. For more information, see the *Command Line Reference* guide.

Additional Functionality

The following additional functionality is available:

Remove All Users

Removes all user permissions from the Resource.

Remove All Groups

Removes all group permissions from the Resource.

Remove All

Removes all user and group permissions from the Resource.

Add Resource

Follow the instructions below to add a new Resource:

1. Log in as an Admin User with the Resource Manager role.

2. Click the **Resources** link from the main menu.
3. On the Resource Types column, click the Resource type to work with.
4. Click the **Add** link in the toolbar to add a new Resource.
5. Type the appropriate information in the boxes for the Resource.
6. Click the **Test** button to test the connection to the Resource. The test results will be displayed in a popup window indicating a success or failure.
7. If the test is successful, click the **Save** button to add the Resource record.

Edit Resource

Follow the instructions below to change the properties (field settings) for a Resource:

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. On the list of Resource types, click the Resource type to work with.
4. Click the Action icon beside the Resource and then click the Edit icon.
5. The current Resource properties are displayed.
6. Make any desired changes to the properties.
7. Click the **Test** button to test the connection to the Resource. The test results will be displayed in a popup window indicating a success or failure.
8. Click the **Save** button to apply the changes to the Resource.

Copy Resource

The Copy Resource function allows you to copy all the attributes of an existing Resource into a new Resource that you can edit. Follow the steps below to copy a Resource:

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. In the list of Resource types in the left column, click the Resource type to work with.
4. From the list of Resources, click the Action icon beside the Resource you wish to copy and then click the Copy icon.
5. After clicking the Copy icon, the process and information for copying a Resource is the same as adding a "Add Resource" on page 46.

Delete Resource

Follow the instructions below to delete a Resource:

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. In the list of Resource types in the left column, click the Resource type to work with.
4. Click the Action icon beside the Resource and then click the icon.
5. To delete multiple Resources, select the appropriate checkboxes and click the **Delete** button.
6. Click the **Confirm** button in the confirmation dialog.

Note: A user must have "Write" "Edit Resource Permissions" on page 46 for the Resource in order to delete it.

Test Resource

Follow the instructions below to test a Resource:

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. In the list of Resource types in the left column, click the Resource type to work with.
4. In the list of Resources, click the icon beside the Resource and then click the Test icon to test the connection to the Resource.
5. The test results are displayed in a popup window indicating a success or failure.
6. Click the **Close** button.

Export Resource

Authorized users can export a Resource as an XML file on their local computer.

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. In the list of Resource types in the left column, click the Resource type to work with.
4. In the list of Resources, click the Action icon and then click the Export icon.
5. Save the exported Resource XML file to your computer.
6. The name of the exported file will be constructed using the Resource name with an .xml extension.

Note: Resource passwords will be replaced with asterisks in the XML file if the Allow Viewing of Resource Passwords is not enabled on the Security Settings page.

Search Resources

You can filter for any resource types from any field within a resource. You can search for resource using strings, parameters, name of an attribute, the ending or middle string of an email id, a resource name, description string, or any other parameters such as host, user, directory, and so on.

Note: It is recommended to enter three or more characters in the search string to narrow down the search results.

To show which Projects and Monitors refer to a particular Resource, an Admin User with the Resource Manager role can select the  **Where Used** option from the Resources action menu. The Resource Search Results page displays the details about the Projects and Monitors that use the Resource. From this page a user can edit a Project, view a Project, and view information about who created or modified the Project.

The Matched Monitors section displays all Monitors that use the particular Resource.

The Matched Projects section displays all Projects that use the particular Resource.

The Projects Avoided section displays all Projects that were not searched because they contain compile errors.

Note: If no Projects or Monitors were found that use a Resource, an option is available to delete the Resource. Be aware that Resources that are referenced by a variable will not be displayed in this list.

Page Toolbar

The following actions are available from the page toolbar:

- Click the **Refresh** button to refresh the search results.
- Click the **Done** button to return to the Resources page.

Resource References Actions

The following actions are available by selecting the  Actions icon:

- Click the  icon to edit the "Project" on page 108.
- Click the  icon to view the Project. If the Project has compilation errors, they are displayed on this page.
- Click the  icon to view creation and modification details about the Project.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Export Page** button to save the visible search results in CSV format.
- Click the **Export Results** button to save all the search results in CSV format.

View Resource

Follow the instructions below to view the properties (settings) for a Resource:

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. In the list of Resource types in the left column, click the Resource type to work with.
4. On the list of Resources in the right column, click the  Action icon and then click the  icon.
5. Click the **Done** button when finished viewing the Resource properties.

Promoting a Resource

Admin Users can copy Resources to other Managed File Transfer installations. This feature is especially useful for promoting Resources from a development installation to a production installation of Managed File Transfer. Follow the steps below to promote Resources:

1. A Resource can be promoted from the **Promote Resources** page. To access this page:
   a. Log in as an Admin User with the Resource Manager role.
   b. Click the **Resources** link from the main menu.
   c. A list of Resource types will be displayed (database servers, FTP servers, HTTP servers, etc.).
   d. Click the Resource type to work with.
   e. A list of Resources will be displayed.
   f. Click the  Action icon beside the Resource and then click the  Promote icon.
   g. The **Promote Resources** page will be displayed.
2. Enter values for the following fields:

   Target Server

   The host name (or IP address) of the Managed File Transfer installation to copy the Resource(s) to. The value specified must be a URL of the form `http://[host]:[port]/informaticamft`, where [host] is the host name or IP address of the target Managed File Transfer installation, and [port] is the port number on which Managed File Transfer server is running, which by default is 8000. An example value would be http://10.1.4.1:8000/informaticamft

   User Name

   The Admin User name to login to the target Managed File Transfer installation.

   Password

   The password for the user to log in with. The password is case sensitive.

   Replace Target Resource(s)?

   Indicate if the Resource should be replaced on the target Managed File Transfer installation if it already exists with the same name.
3. Click the **Promote** button to copy the Resource.

Permissions Required

An Admin User must have the following permissions in order to promote a Resource:

- Resource Manager role on both the source and target Managed File Transfer installations.
- Read permission for the Resource on the source Managed File Transfer installation
- Write permission for the Resource on the target Managed File Transfer installation (if you chose to Replace Target Resource(s)
  Resources can also be promoted to another Managed File Transfer server by using the promoteResource function in the Command Line Utility (INFAMFTCMD). Refer to the Managed File Transfer Command User Guide for more information.

View Resource Information

The Resource information page shows details about the creation and modification of the Resource. Follow the instructions below to view information about the Resource:

1. Log in as an Admin User with the Resource Manager role.
2. Click the **Resources** link from the main menu.
3. In the list of Resource types in the left column, click the Resource type to work with.
4. On the list of Resources in the right column, click the  Action icon beside the Resource you wish to view and click the  More Info icon.
5. Click the **Done** button when finished viewing the Resource details.

Connection Pooling

The pooling of resource connections in Managed File Transfer allows you to maintain a pool of connections for FTP, FTPS, and SFTP resources. The pooling of resource connections improves the performance of Managed File Transfer through the reuse of active connections.

If you do not enable connection pooling, Managed File Transfer creates a connection for each file transfer.

When you enable connection pooling, Managed File Transfer checks for existing connections and uses them for the transfer of files. Based on the connection pooling configuration, if the number of active connections exceeds the maximum active connections allowed in a connection pool, Managed File Transfer creates a connection for the file transfer. If the number of idle connections, exceeds the maximum limit of idle connections, then Managed File Transfer removes the unused connections.

Note: To configure connection pooling, you must define the connection pooling parameter in the `ftp-connectionpool-config.properties` file. For more information about defining the connection pooling parameter, see "Connection Pooling Configuration" on page 52.

Connection Pooling Configuration

To configure connection pooling, define the *maxTotal* property in the following file: `<MFT_HOME/server/config/ftp-connectionpool-config.properties`.

The *maxTotal* property is the maximum number of active connections that Managed File Transfer can use when you enable connection pooling. You can derive the maximum number of active connections that you must provide in the *maxTotal* property, based on the server capacity.

Use the following example to configure the *maxTotal* property:

Consider that Managed File Transfer has 112 connections and each SFTP resource has a maximum of 10 active connections. Based on the server capacity, let us assume that you can use a maximum of 18 connections for a resource out of the 112 connections.

The value of the *maxTotal* property must be 10 * 18 =180.

Network Shares

The Network Shares resource in Managed File Transfer allows access to shared files and folders on a network. The Network Shares resource is based on the standard SMB/CIFS protocol used by most operating systems. The Network Share resource provides the ability to access a network location using either the current Admin User's credentials or different credentials as defined on the Authentication tab.

Network shares can be used when defining "Virtual Folders and Files" on page 586, "Trigger Manager" on page 206 and the WebDocs folder location in the "Global Settings" on page 752.

Advanced configuration options are available and are outlined in the "Advanced Network Shares Configuration" on page 806.

Note: The syntax for referencing a network is: `resource:smb://[ResourceName]/[AdditionalPath]`, where [ResourceName] is the name of the Network Share Resource.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies this network share within Managed File Transfer. This name should be descriptive enough so Admin Users can quickly identify this network share when prompted to choose from a list. The name cannot exceed 50 characters.

Description

A short paragraph describing the network share. The description is optional.

Host

The host name, IP address or NetBIOS name of the server hosting the network share.

Share Name

The name of the share on the host server, optionally followed by a sub-folder location.

Authentication Tab

The Authentication tab contains the following fields:

Use Logged-In User Credentials

The network share resource can use the login credentials of the current Managed File Transfer Web User when accessing a network share. This option is especially useful if the "Login Methods" on page 647 authenticates with Active Directory, LDAP, or IBM i. When used, the logged-in Web User credentials are sent to the destination location so the owner of the file is the Web User. If Use Logged-In User Credentials is not selected, the credentials of the specified Managed File Transfer account are passed as the file owner.

User

The user name (login name) to use when connecting to the network share, if not using the current user's credentials.

Password

The password to use for connecting to the network share, if not using the current user's credentials. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in the Managed File Transfer database.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose Yes if you clicked the Encrypt button for the Password.

Domain

The domain name of the authentication server, if different from the domain of the network share.

Connection Tab

Informatica Managed File Transfer can retry failed connections based on Managed File Transfer's predefined "Advanced Network Shares Configuration" on page 806 returned from the server.

The Connection tab contains the following fields:

Connection Retry Attempts

The number of times to retry the network connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.

Connection Retry Interval

The number of seconds to wait between each connection retry attempt.

Note: For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

Database Servers Resource

Managed File Transfer can connect to a wide variety of database servers including DB2, Oracle, SQL Server, Informix, Sybase, PostgreSQL and MySQL. Managed File Transfer connects to database servers over the network using *JDBC drivers*.

Any SQL statement supported by the database server can be issued by Managed File Transfer Projects including SELECT, UPDATE, INSERT, DELETE, CALL and CREATE statements.

When defining a database server resource in Managed File Transfer, you need to indicate the JDBC driver to use, along with the connection properties (for example, host name, user, password) for that driver.

Note: Only Oracle and SQLServer drivers are included in Managed File Transfer. To enable other databases, manually copy the drivers to the path `/informatica/B2B/MFT/server/userdata/databases`.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the database server. This name should be descriptive enough so users can quickly identify this database server when prompted to choose a Database server from a list. The name cannot exceed 50 characters.

Description

A short paragraph that describes the database server. The description is optional.

JDBC Driver

The JDBC driver to use for connecting to the database. The driver can be selected from the drop-down list. For instance, if connecting to a SQL Server database, select the "com.microsoft.sqlserver.jdbc.SQLServerDriver" driver option.

JDBC URL

The connection URL string for the database. This URL should contain the host name (or IP address) of the database server. Depending on the type of database server, you may additionally need to specify the database port#, database name and other properties in the URL.

Listed below is an example of a URL string for a SQL Server database that is located at the IP address of 10.1.4.1:1433 with the database name of "crm":

jdbc:sqlserver://10.1.4.1;databaseName=crm;portNumber=1433

The URL string must be formatted properly. Use the "JDBC URL Wizard" on page 791 to generate this URL string correctly. Click the  button (located on the right side of the field) to launch the builder.

User

The name of the user connecting to the database server.

Password

The password to use for connecting to the database server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the database server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. Select **Yes** if you clicked the **Encrypt** button for the Password.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

FTP Servers Resource

Managed File Transfer can connect to standard FTP servers for exchanging files. When defining an FTP resource in Managed File Transfer, you need to indicate the FTP connection properties such as the host name (or IP address), user and password.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the FTP server. This name should be descriptive enough so users can quickly identify this FTP server when prompted to choose from a list. The name cannot exceed 50 characters.

Description

A short paragraph that describes the FTP server. The description is optional.

Host

The host name or IP address of the FTP server.

Port

The port number to use for connecting to the FTP server. If left blank, the default port number is 21.

User

The user name to use for connecting to the FTP server.

Password

The password to use for connecting to the FTP server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the FTP server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Connection Tab

The Connection Tab has the following fields:

Use Passive Mode

Indicates whether or not the FTP connection will use Passive or Active mode. Specify **Yes** to use Passive mode. Specify **No** to use Active mode. If neither value is selected, then the default mode of Active will be used.

Note: There are two modes in FTP communications: Active and Passive.

In Active mode, the FTP server will attempt to connect back to a port on the Managed File Transfer FTP client in order perform the data transfer. The challenge with Active mode is that your firewall may block the FTP server from trying to open a port back into your network.

In Passive mode, the FTP server does not need to connect back to a port on the Managed File Transfer FTP client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the FTP server, you may want to change the mode to Passive by selecting **Yes** for this option.

Data Connection Start Port

The starting port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.

Data Connection End Port

The ending port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.

Timeout

The number of seconds to wait when attempting to connect to the FTP server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.

Connection Retry Attempts

The number of times to retry the FTP connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.

Connection Retry Interval

The number of seconds to wait between each connection retry attempt.

Note: For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.

Initial Remote Directory

The initial directory to start in after connecting to the FTP server. If left blank, then the initial directory will be the home directory assigned to the user on the FTP server.

Control Encoding

If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the FTP server, other encodings like UTF-8 can be specified to support more international characters.

Throttle Bandwidth

Limit the inbound and outbound bandwidth used for file transfers based on the policies set on the "Global Settings" on page 752 Bandwidth tab.

Pool Connections

Enable connection pooling to optimize connection performance. When you enable the connection pooling, Managed File Transfer reuses active connections for the file transfer. When the connection pooling is disabled, Managed File Transfer creates a new connection for each file transfer job.

For more information about connection pooling and defining the connection pooling parameter, see "Connection Pooling" on page 51.

Default is false.

Max Idle Connections

The maximum number of idle connection instances that a pool maintains. Managed File Transfer refreshes the pool of idle connections after the maximum number of idle connections are met and creates a new connection.

Default is 8.

Max Active Connections

The maximum number of active connection instances that the pool maintains. Managed File Transfer creates a new connection for the file transfer if the number of active connections is met.

Default is 8.

Min Idle Connections

The minimum number of idle connection instances that a pool maintains. Managed File Transfer creates a new connection for the file transfer if the minimum number of idle connections is met.

Default is 0.

Directory Listing Tab

The Directory Listing tab contains the following fields:

List Parser

The list parser to use for the FTP server connection. If the field is left blank, Managed File Transfer will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used. If you experience problems listing directories, select a different list parser.

Date Format

This field is used if the date returned by the FTP server is different than the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values. Refer to the List Parser Date Format table below for the defaults and options supported by each list parser.

Recent Date Format

Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values. Refer to the List Parser Date Format table below for the defaults and options supported by each list parser.

List Parser Date Format

List Parser Type	Default Date Format	Default Recent Date Format
Unix	MMM d yyyy	MMM d HH:mm
Windows	MM-dd-yy hh:mma MM-dd-yy kk:mm	not applicable

Proxy Tab

The Proxy tab contains the following fields:

Proxy Type

Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.

Note: When using a proxy for an FTP resource, the Use Passive Mode option on the Connection tab should be set to Yes.

Host

The host name or IP address of the proxy server.

Note: If the Proxy Type or Host fields are blank, a direct connection to the target host is implied.

Alternate Host

The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.

Port

The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.

User

The user name to use for connecting to the proxy server.

Password

The password to use for connecting to the proxy server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the proxy server in the FTP server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

FTPS Servers Resource

Managed File Transfer can connect to FTPS (FTP over SSL) servers for secure file exchange. When defining a FTPS resource in Managed File Transfer, you need to indicate the FTPS connection properties such as the host name (or IP address), user and password. Optionally you can specify the certificates to use for authentication.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the FTPS server. This name should be descriptive enough so users can quickly identify this FTPS server when prompted to choose from a list (for example, "Bank FTPS Server" or "Windows FTPS Server in San Diego"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the FTPS server. The description is optional.

Host

The host name or IP address of the FTPS server.

Port

The port number to use for connecting to the FTPS Server. If left blank, the default port number is 21.

User

The user name (login name) to use for connecting to the FTPS server.

Password

The password to use for connecting to the FTPS server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: Note: If you do not wish to store the password for the FTPS server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Connection Tab

The Connection tab contains the following fields:

Use Passive Mode

Indicates whether or not the FTPS connection will use Passive or Active mode. Specify **Yes** to use Passive mode. Specify **No** to use Active mode. If neither value is selected, then the default mode of Active will be used.

Note: There are two modes in FTPS communications: Active and Passive. In Active mode, the FTPS server will attempt to connect back to a port on the Managed File Transfer FTPS client in order perform the data transfer. The challenge with Active mode is that your firewall may block the FTPS server from trying to open a port back into your network.

In Passive mode, the FTPS server does not need to connect back to a port on the Managed File Transfer FTPS client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the FTPS server, you may want to change the mode to Passive by selecting **Yes** for this option.

Data Connection Start Port

The starting port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.

Data Connection End Port

The ending port number to use for the data connection. This should be used when Active (non-Passive) mode is specified and there is a limited range of open ports on your firewall allowed for data connections.

Timeout

The number of seconds to wait when attempting to connect to the FTPS server. A timeout will occur if the connection cannot be established in the specified amount of time. If this field is left blank, the default timeout value of 120 seconds will be used.

Connection Retry Attempts

The number of times to retry the FTPS connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.

Connection Retry Interval

The number of seconds to wait between each connection retry attempt.

Note: For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.

Initial Remote Directory

The initial directory to start in after connecting to the FTPS server. If left blank, then the initial directory will be the home directory assigned to the user on the FTPS server.

Control Encoding

If left blank, Managed File Transfer uses the ISO standard ISO-8859-1. If supported by the FTPS server, other encodings like UTF-8 can be specified to support more international characters.

Throttle Bandwidth

Limit the inbound and outbound bandwidth used for file transfers based on the policies set on the "Global Settings" on page 752 Bandwidth tab.

Pool Connections

Enable connection pooling to optimize connection performance. When you enable the connection pooling, Managed File Transfer reuses active connections for the file transfer. When the connection pooling is disabled, Managed File Transfer creates a new connection for each file transfer job.

For more information about connection pooling and defining the connection pooling parameter, see "Connection Pooling" on page 51.

Default is false.

Max Active Connections

The maximum number of active connection instances that the pool maintains. Managed File Transfer creates a new connection for the file transfer if the number of active connections is met.

Default is 8.

Max Idle Connections

The maximum number of idle connection instances that a pool maintains. Managed File Transfer refreshes the pool of idle connections after the maximum number of idle connections are met and creates a new connection.

Default is 8.

Min Idle Connections

The minimum number of idle connection instances that a pool maintains. Managed File Transfer creates a new connection for the file transfer if the minimum number of idle connections is met.

Default is 0.

Directory Listing Tab

The Directory Listing tab contains the following fields:

List Parser

The list parser to use for the FTPS server connection. If the field is left blank, Managed File Transfer will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used. If you experience problems listing directories, select a different list parser.

Date Format

This field is used if the date returned by the FTPS server is different than the selected list parser's default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the Date Format setting will ignore any User specified values. Refer to the List Parser Date Format table below for the defaults and options supported by each list parser.

Recent Date Format

Specify the date format to use when parsing the recent last modified date for each file. The recent date format is primarily used on UNIX-based systems and appears on entries less than a year old. If your location requires a different recent date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any User specified values. Refer to the List Parser Date Format table below for the defaults and options supported by each list parser.

List Parser Type	Default Date Format	Default Recent Date Format
Unix	MMM d yyyy	MMM d HH:mm
Windows	MM-dd-yy hh:mma MM-dd-yy kk:mm	not applicable

Proxy Tab

The Proxy tab contains the following fields:

Proxy Type

Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.

Note: When using a proxy for an FTPS resource, the Use Passive Mode option on the Connection tab should be set to Yes.

Host

The host name or IP address of the proxy server.

Note: If the Proxy Type or Host fields are blank, a direct connection to the target host is implied.

Alternate Host

The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.

Port

The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.

User

The user name to use for connecting to the proxy server.

Password

The password to use for connecting to the proxy server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the proxy server in the FTPS server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

SSL Tab

The SSL tab contains the following fields:

Connection Type

Indicates if the connection type is **Implicit SSL** or **Explicit SSL**. The preferred connection type is the more modern Explicit SSL standard, however some trading partners may still require Implicit SSL. If this field is left blank, then the default connection type of Explicit SSL will be used.

Security Protocol

Indicates whether SSL or TLS should be used for Explicit SSL connections. TLS is the latest security protocol standard, however many trading partners still use the SSL protocol for Explicit SSL connections. If this field is left blank, then the default security protocol of SSL will be used.

Clear Command Channel

Indicates whether or not to use a clear command channel (CCC) for the FTPS connection. Specify **No** to keep the command channel encrypted. Specify **Yes** to not encrypt the control command channel (however, the actual data transfers will remain encrypted). If neither value is selected, then the default value of **No** will be used.

Note: SSL connections require a Clear Command Channel (CCC) when connecting from behind a NAT firewall.

Data Channel Protection Level

The data channel protection level indicates if the data channel is encrypted. Select **Private** to keep the data channel encrypted. If the FTPS server does not support an encrypted data channel, select **Clear** to leave the data channel unencrypted. The default setting is Private.

Send SSL Close Notify

After the command channel is closed, most servers automatically close the SSL/TLS connection, however some servers do not understand the "close_notify" command. Select **No** to keep Managed File Transfer from sending the "close_notify" command. The default value is Yes.

SSL Context Protocol

Specify the protocol to use when creating the SSLContext. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (TLS) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support TLS 1.0.

Server Certificate Key Store Tab

The settings on the Server Certificate Key Store tab are only required when the FTPS server requires that its connections are authenticated with a certificate. The Server Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store (which contains the trusted certificates) for authenticating the FTPS server.

You can browse for the key store on the file system by clicking the  button next to the field. If a key store is not specified, then the FTPS server will be treated as a trusted server. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

Note: A default key store is provided in Managed File Transfer for holding trusted server certificates. The location of this key store is **[installdirectory]/userdata/keys/x509/trustedCertificates.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Password

The password to use for accessing the Trusted Server Certificate Store. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password with the FTPS server resource, this password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password for the Server Certificate Store is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Server Certificate Store Password.

Type

Indicates if the type of the key store is **JKS** (Java Keystore) or **PKCS12** (Public Key Cryptology Standard). If this field is left blank, the default is JKS.

Client Certificate Key Store Tab

The settings on the Client Certificate Key Store tab are only required when a client requires that its connections are authenticated with a certificate. The Client Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store (which contains the trusted server certificates) for authenticating the FTPS server. You can browse for the key store on the file system by clicking the  button next to the field. If a key store is not specified, then the FTPS server will be treated as a trusted server. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

Note: A default key store is provided in Managed File Transfer for holding private keys. The location of this key store is **[installdirectory]/userdata/keys/x509/privateKeys.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Password

The password to use for accessing the trusted Server Certificate Store. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password with the FTPS server resource, this password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password for the Client Certificate Store is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Client Certificate Store Password.

Alias

Each certificate in the Key Store is identified by an alias name. If the field is left blank, Managed File Transfer will try to determine the correct certificate. If an Alias is specified, Managed File Transfer will only use that certificate for authentication.

Type

Indicates if the type of the key store is **JKS** (Java Keystore) or **PKCS12** (Public Key Cryptology Standard). If this field is left blank, the default is JKS.

Note: The default key stores provided with the installation of Managed File Transfer are JKS.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

SFTP Servers Resource

Informatica Managed File Transfer can connect to SSH Servers for performing SFTP transfers, SCP (Secure Copy) file transfers, and for running SSH remote commands. When you define an SSH Server resource in Managed File Transfer, indicate the connection properties such as the host name or IP address, and User ID. You can specify a password, SSH private key, or both for authentication.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the server. This name should be descriptive enough so a user can quickly identify this server when prompted to choose from a list (for example, Bank SFTP Server). The name cannot exceed 50 characters.

Description

A short paragraph that describes the server. The description is optional.

Host

The host name or IP address of the server.

Port

The port number to use for connecting to the server. If left blank, the default port number is 22.

User

The user name (login name) to use for connecting to the server. A user name is only required if using password authentication or both password and SSH private key authentication.

Password

The password to use for connecting to the server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database. A password is only required if using password authentication or both password and SSH private key authentication.

Note: If you do not wish to store the password for the server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose **Yes** if you clicked the **Encrypt** button for the Password.

Connection Tab

The Connection tab contains the following fields:

Timeout

The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If this field is left blank, the default timeout value is 120.

Connection Retry Attempts

The number of times to retry the connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.

Connection Retry Interval

The number of seconds to wait between each connection retry attempt.

Note: For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.

Initial Remote Directory

The initial directory to start in after connecting to the SFTP server. If left blank, then the initial directory will be the home directory assigned to the user on the SFTP server.

Note: The SCP and SSH tasks do not utilize this field.

Throttle Bandwidth

Limit the inbound and outbound bandwidth used for SFTP and SCP file transfers based on the policies set on the "Global Settings" on page 752 Bandwidth tab.

Note: SSH servers and tasks do not utilize this field.

Pool Connections

Enable connection pooling to optimize connection performance. When you enable the connection pooling, Managed File Transfer reuses active connections for the file transfer. When the connection pooling is disabled, Managed File Transfer creates a new connection for each file transfer job.

For more information about connection pooling and defining the connection pooling parameter, see "Connection Pooling" on page 51.

Default is false.

Max Active Connections

The maximum number of active connection instances that the pool maintains. Managed File Transfer creates a new connection for the file transfer if the number of active connections is met.

Default is 8.

Max Idle Connections

The maximum number of idle connection instances that a pool maintains. Managed File Transfer refreshes the pool of idle connections after the maximum number of idle connections are met and creates a new connection.

Default is 8.

Min Idle Connections

The minimum number of idle connection instances that a pool maintains. Managed File Transfer creates a new connection for the file transfer if the minimum number of idle connections is met.

Default is 0.

Disable stat Command on Server

Disable to not perform the stat operation on server.

Default is false.

Proxy Tab

Configure the following fields in the proxy tab to set up Informatica Managed File Transfer Gateway for forward proxy:

Proxy Tab field	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy, and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
Host	The host name or IP address of the proxy server. **Note:** If the Proxy Type or Host fields are blank, there is a direct connection to the target host.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use for connecting to the proxy server.
Password	The password to use for connecting to the proxy server. After you enter the password, you can optionally click the **Encrypt** button that will encrypt the password when it is stored in the Managed File Transfer database.
Is Password Encrypted	Indicates whether the password is encrypted. Choose **Yes** if you click the **Encrypt** button for the Password.

SSH Keys Tab

The SSH Keys tab contains the following fields:

Host Key

The fingerprint of the server's public key, which will be used to authenticate the server. If a fingerprint is not specified, then the server will be treated as trusted.

Private Key Alias

The private key used to authenticate the server, which is located in the "SSH Key Manager" on page 741.

If you do not know the alias name for the private key, click the  icon to select the private key.

Private Key File

The location of the file containing the SSH private key. This key file will be used for client authentication, if required by the server. You can browse for the key file by clicking the  button next to the field. The default location for SSH keys is [installdirectory]/userdata/keys/ssh where [installdirectory] is the installation directory of the Managed File Transfer product. Typically an SSH private key will have a file extension of ".pvk". A private key is only required if using SSH private key authentication or both password and SSH private key authentication.

Note: SSH Keys can be managed in Managed File Transfer's SSH Key Manager page.

Private Key File Password

The password to use for accessing the Private Key File. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database. A private key password is only required if using SSH private key authentication or both password and SSH private key authentication.

Note: If you do not wish to store the password with the server resource, this password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password for the Private Key File is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Private Key Password.

Algorithms Tab

The options on the Algorithms tab allow customization of the supported algorithms for each SSH server resource. The entries in the left column are the available algorithms and the entries in the right column are the selected algorithms. By selecting one or more algorithms, only those will be used during the communication. If no algorithms are selected for a section, the defaults for that section will be used. Refer to the Default Algorithms section below for the list of defaults.

During the handshake process, the selected options are negotiated with the server, starting with the entry at the top of the list. The first cipher and mac and compression algorithms to match an algorithm supported by the server will be used for the connection. If your company prefers certain algorithms over others, use the arrow buttons to move that cipher to the Selected column and to set the order with the most preferred algorithm at the top. Press the CTRL key while clicking to select multiple entries.

Note: If a resource consists of only unsupported algorithms before an upgrade and the resource is used in a project post-upgrade, you must save the resource before executing the project.

Default Algorithms

The following entries are set as defaults in Managed File Transfer. The entries are listed in the order of preference.

Authentication

- publickey
- password
- keyboard-interactive

Cipher

- chacha20-poly1305@openssh.com
- aes128-ctr
- aes192-ctr
- aes256-ctr
- 3des-ctr
- 3des-cbc

- blowfish-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- arcfour
- arcfour128
- arcfour256
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

After upgrading to Managed File Transfer 10.5.0 version, a warning message appears with a list of unsupported algorithms if they were selected before upgrade. You must save the configuration to proceed. Saving the configuration deletes the unsupported algorithms.

The Managed File Transfer 10.5.0 version does not support the following algorithms:

- twofish256-cbc
- serpent256-cbc
- twofish-cbc
- twofish192-cbc
- twofish128-cbc
- serpent192-cbc
- serpent128-cbc
- idea-cbc
- cast128-cbc
- des-cbc
- blowfish-ctr
- twofish128-ctr
- twofish192-ctr
- twofish256-ctr
- serpent128-ctr
- serpent192-ctr
- serpent256-ctr
- idea-ctr
- cast128-ctr

Mac

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-512-96
- hmac-sha2-512
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-256

- hmac-sha2-256-96
- hmac-sha1-etm@openssh.com
- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-etm@openssh.com
- hmac-md5-96

Compression

- none
- zlib
- zlib@openssh.com

Key Exchange

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group18-sha512
- diffie-hellman-group17-sha512
- diffie-hellman-group16-sha512
- diffie-hellman-group15-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group-exchange-sha256
- rsa2048-sha256
- ecdh-sha2-nistp521
- ecdh-sha2-nistp384
- ecdh-sha2-nistp256
- rsa1024-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1

Note: The selection of key exchange algorithm is mutually exclusive. You can either select the `curve25519@openssh.com` key-exchange algorithm in order to connect all servers that support the `curve25519@openssh.com` or select other key exchange algorithms.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

AS2 Servers Resource

The AS2 Server Resource is used to specify the settings to use when messages are sent using the *AS2* 1.2 specification. AS2 is a standard originally created to securely transfer EDI documents, but it can also be used to transmit virtually any file type. The messages are structured using the standard S/MIME format and are sent over HTTP(S) connections.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the AS2 server. This name should be descriptive enough so users can quickly identify this database server when prompted to choose from a list (for example, "AS2 Server in Atlanta"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the AS2 server. The description is optional.

URL

This is the *URL* of the server that receives the messages. The URL syntax must be a valid server and location where [hostname] can be an IP Address or a Domain name and [portnumber] is the port on which the AS2 Server listens.

AS2 From ID

The AS2 From ID is the name or ID used by the sender (most commonly you are the sender). The ID is arbitrary, but if the receiving server filters by this ID, the ID's must match. The AS2 From ID is case sensitive, can be 1 to 128 ASCII printable characters in length, and may not contain whitespaces.

AS2 To ID

The AS2 To ID is the name or ID used by the recipient. The ID is arbitrary. The AS2 To ID is case sensitive, can be 1 to 128 ASCII printable characters in length, and may not contain whitespaces.

Message Tab

Encrypt Messages

Encrypting the message itself during transmission within the encrypted tunnel is optional, but highly recommended. The default value if left blank is No.

Encryption Algorithm

The Encryption Algorithm is the algorithm used to encrypt the message. The default encryption algorithm is AES128.

Encryption Certificate Alias

The Encryption Certificate Alias is the certificate alias to use in the Default Trusted Certificate Key store.

If you do not know the alias name for the certificate, click the  icon to select the certificate.

Sign Messages

Signing the message with a digital signature to further identify yourself is optional, but highly recommended.

Signature Algorithm

The signature algorithm used to sign the messages can be SHA1, SHA224, SHA256, SHA384, SHA512, or MD5. The default is SHA1.

Signature Certificate Alias

This is the private key alias used to sign the message. The private key is located in the Default Private Key store. If you do not know the alias name for the private key, click the  icon to select the private key.

Compress Messages

Messages can be compressed to reduce bandwidth using the zlib format. The default is No.

Receipt Certificate Alias

The Receipt Certificate Alias is optional when the receipt signature contains an embedded certificate. In this scenario, Managed File Transfer will ensure that the embedded certificate is also located in the Default Trusted Certificate Key Store. To enhance security, a Receipt Certificate Alias can be specified which verifies the certificate that signed the receipt is a specific certificate in the key store.

If the receipt signature does not contain an embedded certificate, then the Receipt Certificate Alias must be specified in order to verify and trust the signature. Typically, the same certificate that is used to encrypt the outbound message can be used to verify the receipt signature. If you do not know the alias name for the certificate, click the  icon to select the certificate.

Receipt Transfer Encoding

Define the encoding of a receipt. This is useful when the receipt does not include the transfer encoding.

Connection Tab

The Connection tab contains the following fields:

User

The user name (login name) to use for connecting to the AS2 server. This is only required if the AS2 server needs the AS2 client to authenticate using either the BASIC or DIGEST authentication schemes.

Password

The password to use for connecting to the AS2 server. This is only required if the AS2 server needs the AS2 client to authenticate using either the BASIC or DIGEST authentication schemes. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the AS2 server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose **Yes** if you clicked the **Encrypt** button for the Password.

Connection Timeout

The maximum amount of time, in seconds, to wait when trying to establish a connection to the AS2 server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, the default value is 60 seconds.

Read Timeout

The maximum amount of time, in seconds, to wait for a (read) response from the AS2 server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value is 0 (zero).

Connection Retry Attempts

The number of times the AS2 Resource will attempt to connect if a connection cannot be established on the first attempt.

Connection Retry Interval

The number of seconds to wait between each connection retry attempt. If left blank, the retry interval is 0 (zero) seconds.

Follow Redirects

Specify whether or not to follow redirects. The default value is yes.

Enable Cookies

Specify whether or not to enable cookies. The default value is yes.

User Agent

The user agent is the value used in the message header to indicate what application created or sent the message. The default value is Managed File Transfer/${currentProductVersion}.

Use Chunked Encoding

Indicates if the length of the request will be pre-calculated or sent in chunks. Pre-calculating the content length may slow performance when sending large files, but not all AS2 servers support chunked encoding. The default setting is No.

Client Certificate Alias

A particular key within the default key store can be used for client authentication by indicating the key alias. The specified key will be used when required by the AS2 server. If you do not know the certificate

name, click the icon to open the default Private Key Store and select the certificate alias. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

Note: A default key store is provided in Managed File Transfer for holding client certificates and private keys. The location of this key store is **[installdirectory]/userdata/keys/x509/privateKeys.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

SSL Context Protocol

Specify the protocol to use when creating the SSLContext. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (SSL) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support SSLv3.

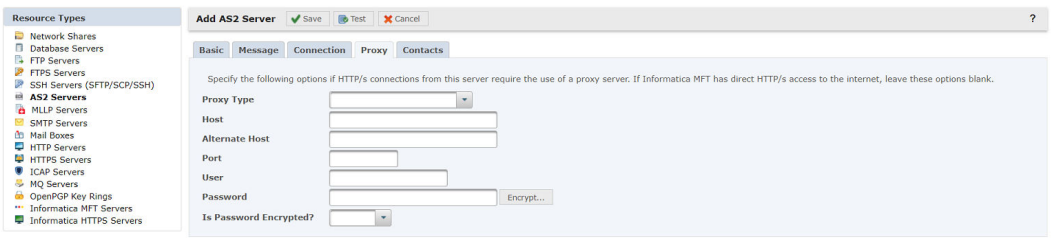
Proxy Tab

Configure the following fields in the proxy tab to set up Informatica Managed File Transfer Gateway for forward proxy:

Proxy Tab field	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy, and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.
Host	The host name or IP address of the proxy server on your network.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use for connecting to the proxy server.
Password	The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP(S) connections. After entering the password, you can optionally click the **Encrypt** button which will encrypt the password when it is stored in the Managed File Transfer database.
Is Password Encrypted	Indicates whether the password is encrypted. Choose **Yes** if you click the **Encrypt** button for the Password.

Note: The options are only needed if your system uses a proxy server to make HTTP(S) connections.

The following image shows the fields that you need to configure in the **Proxy** tab:



Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

MLLP Servers Resource

The Minimal Lower Layer Protocol (MLLP) protocol is used to transfer healthcare industry messages, such as HL7 messages. HL7 is a messaging specification for healthcare information systems.

The MLLP protocol is a minimalistic OSI-session layer framing protocol. HL7 is a messaging specification for healthcare information systems. The Managed File Transfer resource can connect to an MLLP server to send files. When defining an MLLP resource in Managed File Transfer, you need to indicate the connection properties, such as the host name or IP address, and port number.

Basic Tab

Name

A name which identifies the server. This name should be descriptive enough to quickly identify this server when prompted to choose from a list. The name cannot exceed 50 characters.

Description

A short paragraph that describes the server. The description is optional.

Host

The host name or IP address of the server.

Port

The port number to use for connecting to the server. If left blank, the default port number is 2575.

Connection Tab

Response Timeout

The number of seconds to wait when waiting for a response from the server. A timeout will occur if a response is not received in the specified amount of time. If left blank, the default timeout is 120 seconds.

Connection Timeout

The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.

Connection Retry Attempts

The number of times to retry the MLLP connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.

Connection Retry Interval

The number of seconds to wait between each connection retry attempt.

Note: For instance, if you want Managed File Transfer to retry the connection up to 10 times with a 5 second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.

Proxy Tab

Configure the following fields in the proxy tab to set up Informatica Managed File Transfer Gateway for forward proxy:

Proxy Tab field	Description
Proxy Type	Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy, and Managed File Transfer Gateway. HTTP tunneling requires that the HTTP proxy supports the CONNECT HTTP method. Not all HTTP proxy servers may support the CONNECT method and some might only allow HTTPS traffic. When using an HTTP proxy that requires authentication, Basic and Digest authentication schemes are supported. Check with the network administrator for the correct proxy type.
Host	The host name or IP address of the proxy server. **Note:** If the Proxy Type or Host fields are blank, there is a direct connection to the target host.
Alternate Host	The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.
Port	The port number to use for connecting to the proxy server. If left blank, the default port for an HTTP connection is 80 and SOCKS is 1080.
User	The user name to use for connecting to the proxy server.
Password	The password to use for connecting to the proxy server. After entering the password, you can optionally click the **Encrypt** button which will encrypt the password when it is stored in the Managed File Transfer database. **Note:** If you do not want to store the password for the proxy server in the FTP server resource, enter the password when you execute a Project.
Is Password Encrypted	Indicates whether the password is encrypted. Choose **Yes** if you click the **Encrypt** button for the Password.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

SMTP Servers Resource

Managed File Transfer can connect to SMTP mail servers for sending email messages. This is especially useful for distributing files as email attachments. When defining a SMTP resource in Managed File Transfer, you need to indicate the SMTP connection properties such as the host name (or IP address), and optionally the user and password.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the SMTP server. This name should be descriptive enough so a user can quickly identify this SMTP server when prompted to choose from a list (for example, "Corporate Mail Server"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the SMTP server. The description is optional.

Host

The host name or IP address of the SMTP server.

Connection Tab

The Connection tab contains the following fields:

Port

The port number to use for connecting to the SMTP Server. If left blank, the default port is 25.

User

The user name (login name) to use when connecting to the SMTP server. If the user name is left blank, then it is assumed that the SMTP server does not require authentication for its email clients.

Password

The password to use for connecting to the SMTP server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the SMTP server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Connection Type

The connection type to use when communicating with the SMTP Server. The following options are available:

- Normal - The connection is not encrypted.
- Explicit SSL - After initial authentication with the SMTP server, the connection is encrypted with SSL.
- Implicit SSL - The entire connection and transmission is encrypted using SSL.
- O365 - Connects to the Office365 SMTP servers.

Client ID

The ID assigned to Managed File Transfer (client). This is used as part of the topic's subscription ID.

Client Secret

Include the Client Secret if the application is a confidential client.

Is Client Encrypted

Indicates whether or not the client secret is encrypted. You should choose Yes if you clicked the **Encrypt** button for the **Client Secret**.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

Mail Boxes Resource

Managed File Transfer can connect to mail box servers for retrieving email messages. Both POP-3 and IMAP mail box server types are supported. This is especially useful for processing incoming email attachments.

When defining a mail box resource in Managed File Transfer, you need to indicate the connection properties such as the host name (or IP address), user and password.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the mail box server. This name should be descriptive enough so users can quickly identify this mail box server when prompted to choose from a list (for example, "Corporate POP3 Server"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the mail box server. The description is optional.

Server Type

Indicates if the mail box server type is **O365**, **POP-3** or **IMAP**. If this field is left blank, then the default server type of POP-3 will be used.

Host

The host name (for example, pop.example.com) or IP address (for example, 10.1.4.1) of the mail box server.

Note: The mail box host name can typically be found in your email application's account settings. For instance, in Microsoft's Outlook Express, the mail box host name would be found in the "Incoming mail server" setting for your email account.

User

The user name (login name) to use for connecting to the mail box server.

Password

The password to use for connecting to the mail box server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the mail box server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of Yes if you clicked the **Encrypt** button for the Password.

Connection Tab

The Connection tab contains the following fields:

Port

The port number to use for connecting to the mail box server. If this field is left blank, then the default port number for POP-3 servers is 110 when the Connection Type is set to Normal and 995 when set to SSL. For IMAP servers the default port number of 143 when the Connection Type is set to Normal and 993 when set to SSL.

Connection Type

The connection type to use when communicating with the server.

- Normal - The connection is not encrypted.
- SSL - The entire connection and transmission is encrypted using SSL.

Client ID

The ID assigned to Managed File Transfer (client). This is used as part of the topic's subscription ID.

Client Secret

Include the Client Secret if the application is a confidential client.

Is Client Secret Encrypted

Indicates whether or not the client secret is encrypted. You should choose Yes if you clicked the **Encrypt** button for the **Client Secret**.

Timeout

The number of seconds to wait when attempting to connect to the mail box server. A timeout error will occur if the connection cannot be established in the specified amount of time. If this field is left blank, the default timeout value of 300 seconds will be used.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

HTTP Servers Resource

Managed File Transfer can connect to HTTP servers for exchanging files. When defining a HTTP server resource in Managed File Transfer, you need to indicate the HTTP connection properties such as the host name (or IP address), and optionally the user, password and proxy information.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the HTTP server. This name should be descriptive enough so users can quickly identify this HTTP server when prompted to choose from a list (for example, "Bank HTTP Server"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the HTTP server. The description is optional.

Host

The host name or IP address of the HTTP server.

Connection Tab

The Connection tab contains the following fields:

Port

The port number to use for connecting to the HTTP server. If this field is left blank, the default port is 80.

User

The user name (login name) to use for connecting to the HTTP server. This is only needed if the HTTP server requires that the client be authenticated using either the BASIC, DIGEST, or New Technology (NT) LAN Manager (LM) (NTLM) authentication schemes.

Password

The password to use for connecting to the HTTP server. This is only needed if the HTTP server requires that the client be authenticated using either the BASIC, DIGEST, or NTLM authentication schemes. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the HTTP server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Connection Timeout

The maximum amount of time, in seconds, to wait when trying to establish a connection to the HTTP server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.

Read Timeout

The maximum amount of time, in seconds, to wait for a (read) response from the HTTP server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

Proxy Tab

These options are only needed if your system uses a proxy server to make HTTP(S) connections. The Proxy tab contains the following fields:

Proxy Type

Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.

Host

The host name (or IP address) of the proxy server on your network. This is only needed if your system uses a proxy server to make HTTP connections.

Alternate Host

The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.

Port

The port number of the proxy server on your network. This is only needed if your network uses a proxy server to make HTTP connections.

User

The user name (login name) to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP connections.

Password

The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP connections. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the proxy server, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Proxy Password.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

HTTPS Servers Resource

Managed File Transfer can connect to HTTPS servers for securely exchanging files over encrypted SSL connections. When defining a HTTPS server resource in Managed File Transfer, you need to indicate the

HTTPS connection properties such as the host name (or IP address), and optionally the SSL certificates, user, password and proxy information.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the HTTPS server. This name should be descriptive enough so users can quickly identify this HTTPS server when prompted to choose from a list (for example, "Bank HTTPS Server"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the HTTPS server. The description is optional.

Host

The host name or IP address of the HTTPS server.

Proxy Tab

These options are only needed if your system uses a proxy server to make HTTP(S) connections. The Proxy tab contains the following fields:

Proxy Type

Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.

Host

The host name (or IP address) of the proxy server on your network. This is only needed if your system uses a proxy server to make HTTPS connections.

Alternate Host

The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.

Port

The port number of the proxy server on your network. This is only needed if your network uses a proxy server to make HTTPS connections. If left blank, the default port for an HTTP connection is 80, and SOCKS is 1080.

User

The user name (login name) to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTPS connections.

Password

The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTPS connections. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the proxy server, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should select **Yes** if you clicked the **Encrypt** button for the Proxy Password.

Connection Tab

The Connection tab contains the following fields:

Port

The port number to use for connecting to the HTTPS server. If this field is left blank, then the default port number of 443 will be used.

User

The user name (login name) to use for connecting to the HTTPS server. This is only needed if the HTTPS server requires that the HTTPS client be authenticated using either the BASIC, DIGEST, or NTLM authentication schemes.

Password

The password to use for connecting to the HTTPS server. This is only needed if the HTTPS server requires that the HTTPS client be authenticated using either the BASIC, DIGEST, or NTLM authentication schemes. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the HTTPS server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates if the password is encrypted. Select **Yes** if you clicked the **Encrypt** button for the Password.

Connection Timeout

The maximum amount of time, in seconds, to wait when trying to establish a connection to the HTTPS server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.

Read Timeout

The maximum amount of time, in seconds, to wait for a (read) response from the HTTPS server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

SSL Context Protocol

Specify the protocol to use when creating the SSLContext. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (SSL) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support SSLv3.

Server Certificate Key Store Tab

The settings on the Server Certificate Key Store tab are only required when the HTTPS server requires that HTTPS connections are authenticated with a certificate. The Server Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store (which contains the trusted server certificates) for authenticating the HTTPS server. You can browse for the key store on the file system by clicking the  button next to the field. If a key store is not specified, then the HTTPS server will be treated as a trusted server. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

Note: A default key store is provided in Managed File Transfer for holding trusted server certificates. The location of this key store is **[installdirectory]/userdata/keys/x509/trustedCertificates.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Password

The password to use for accessing the trusted Server Certificate Store. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password with the HTTPS server resource, this password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password for the Server Certificate Store is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Server Certificate Store Password.

Type

Indicates if the type of the key store is **JKS** (Java Keystore) or **PKCS12** (Public Key Cryptology Standard). If this field is left blank, then the default store type of JKS will be used.

Note: The default key stores provided with the installation of Managed File Transfer are JKS type.

Client Certificate Key Store Tab

The settings on the Client Certificate Key Store tab are only required when a client requires that HTTPS connections are authenticated with a certificate. The Client Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store (which contains the trusted server certificates) for authenticating the HTTPS server. You can browse for the key store on the file system by clicking the  button next to the field. If a key store is not specified, then the HTTPS server will be treated as a trusted server. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

Note: A default key store is provided in Managed File Transfer for holding trusted server certificates. The location of this key store is **[installdirectory]/userdata/keys/x509/trustedCertificates.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Password

The password to use for accessing the trusted Server Certificate Store. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password with the HTTPS server resource, this password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password for the Server Certificate Store is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Server Certificate Store Password.

Alias

A particular key within the default key store can be used for client authentication by indicating the key alias. The specified key will be used when required by the HTTPS server.

Type

Indicates if the type of the key store is **JKS** (Java Keystore) or **PKCS12** (Public Key Cryptology Standard). If this field is left blank, then the default store type of JKS will be used.

Note: The default key stores provided with the installation of Managed File Transfer are JKS type.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

ICAP Resource

ICAP is an HTTP-like protocol that is used to send files to Data Loss Prevention (DLP) and antivirus scanning web servers. The ICAP server scans the file for viruses, inappropriate content, or restricted information. When an ICAP resource is used to scan a file used in a "Project" on page 108, success or failure responses are returned to Managed File Transfer and can be used to determine if the file is infected. When defining an ICAP resource in Managed File Transfer, you need to indicate the ICAP URL and server options.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the ICAP server. This name should be descriptive enough so a user can quickly identify this ICAP server when prompted to choose from a list (for example, "Clearswift DLP"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the ICAP server. The description is optional.

URL

The IP address of the ICAP server. The URL for the ICAP server must support Response Modification Mode (RESPMOD). The ICAP format is `[Protocol]://[IP or Hostname]:[Port Number]/[URI]` (for example, icap://10.1.1.113:1344/policy_service_resp).

Options Tab

Request Host

The ICAP server may require the host address of the request to determine which policies to use. By default, the host address is "www.example.com" and can be overridden if needed.

Client IP

The ICAP server may require the IP address of the client making the HTTP request. If needed, specify the IPv4 or IPv6 address which will be passed to the ICAP server using the X-Client-IP header.

Server IP

The ICAP server may require the IP address of the HTTP destination host. If needed, specify the IPv4 or IPv6 address which will be passed to the ICAP server using the X-Server-IP header.

Subscriber ID

The ICAP server may require the subscriber ID of the user who issued the HTTP request. If needed, specify a value that will be passed to the ICAP server using the X-Subscriber-ID header.

Authenticated User

The ICAP server may require the user who issued the HTTP request. For example, specify a value of "Local://John.Doe" or "LDAP://192.168.12.100/o=mycompany, ou=engineering, cn=John.Doe" depending on how the authentication is configured. The value will become base-64 encoded by Managed File Transfer and passed to the ICAP server using the X-Authenticated-User header.

Authenticated Groups

The ICAP servers may require the groups that the user belongs to that issued the HTTP request. For example, specify a value of "Local://Sales" or "LDAP://192.168.12.100/o=mycompany, ou=engineering" depending on how the authentication is configured. The value will become base-64 encoded by Managed File Transfer and passed to the ICAP server using the X-Authenticated-Groups header.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

MQ Servers Resource

Managed File Transfer can connect to enterprise messaging systems using JMS (Java Message Service) to send and receive messages from queues and topics. Most messaging systems are supported including Websphere MQ, SonicMQ, ActiveMQ, and SwiftMQ. Please be sure to perform the MQ server prerequisites (below) before creating the MQ server resource.

MQ Server Prerequisites

The JAR files for the MQ server need to be loaded into Managed File Transfer before connections can be made.

If using the JNDI connection type, obtain the required JAR files from your MQ server administrator. Otherwise, when using the MQ Provider Specific connection type, obtain the JAR files listed below for each MQ server. These JAR files should be copied to Managed File Transfer's class path folder of [installdirectory]/userdata/lib where [installdirectory] is the installation directory of the Managed File Transfer product. After the required files are placed in the above location, restart Managed File Transfer.

WebSphere MQ

The WebSphere MQ class JAR files are commonly located in [WebsphereMQinstalldirectory]/Java/lib

- com.ibm.mqjms.jar
- com.ibm.mq.jmqi.jar
- com.ibm.mq.commonservices.jar
- com.ibm.mq.jar
- dhbcore.jar
  SonicMQ

  The SonicMQ class JAR files are commonly located in [SonicMQinstalldirectory]/MQ<version>/lib/
- sonic_Client.jar
- sonic_Crypto.jar
  ActiveMQ

  The ActiveMQ class JAR files are commonly located in [ActiveMQinstalldirectory]/apache-activemq-<version>/
- activemq-all-<version>.jar
  SwiftMQ

  The SwiftMQ class JAR files are commonly located in [SwiftMQinstalldirectory]/jars/
- swiftmq.jar

Basic Tab

After the prerequisite JAR files have been loaded into Managed File Transfer, you can configure the MQ Server Resource in the MQ Server resource page:

Name

A user-defined name which identifies the MQ server. This name should be descriptive enough so users can quickly identify this MQ server when prompted to choose from a list. The name cannot exceed 50 characters.

Description

A short paragraph that describes the MQ server. The description is optional.

Connection Type

The connection type for the MQ server. The MQ server can use the JMS Standard (Java Message Service) or a connection type specific to the MQ Provider. When connecting to Websphere MQ, SonicMQ or ActiveMQ use the MQ Provider Specific type and use JNDI (JMS Standard) for others.

URL

The connection string to an MQ Provider Specific server uses the following syntax - providerCode:[transportProtocol:]//host[:port][?key1=value1&key2=value2]. More information on how the URL is constructed is available in the "MQ Connection URL" on page 834 section in the appendix. The connection string to a JNDI (JMS Standard) server is supplied by the MQ server administrator.

JNDI Initial Context Factory

The JNDI (Java Name and Directory Interface) context factory is the fully qualified name of the class used to look up the JMS connection factory object. For example, the class may look like com.sun.jndi.fscontext.RefFSContextFactory or com.sun.jndi.ldap.LdapCtxFactory. This is required when the connection type is set to use the JMS Standard.

JNDI Name

The name of the JMS connection factory object to use. This is required when the connection type is set to use the JMS Standard.

JNDI Properties

The optional JNDI properties are specified using key=value pairs. Each pair is placed on a separate line.

User

The user name for connecting to the MQ server.

Password

The password to use for connecting to the MQ server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the MQ server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

OpenPGP Key Rings Resource

An OpenPGP Key Ring resource can be defined in Managed File Transfer to contain the file locations of the public and secret key rings for OpenPGP. This makes it easier for a Project Designer to select the appropriate key rings, by simply choosing the key ring resource from a drop-down list when defining a Project (without having to know the exact file location of the key rings).

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the OpenPGP Key Ring resource. This name should be descriptive enough so users can quickly identify this OpenPGP Key Ring resource when prompted to choose from a list (for example, "OpenPGP Key Rings"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the OpenPGP Key Ring resource. The description is optional.

Public Key Ring

The location of the key ring which contains the public keys for OpenPGP. You can browse for the key ring on the file system by clicking the  button next to the field. OpenPGP keys can be managed in Managed File Transfer's"OpenPGP Key Manager" on page 723 page.

Note: A default key ring is provided in Managed File Transfer for holding OpenPGP public keys. The location of this key ring is **[installdirectory]/userdata/keys/pgp/pubring.pkr** where [installdirectory] is the installation directory of the Managed File Transfer product.

Secret Key Ring

The location of the key ring which contains the secret (private) keys for OpenPGP. You can browse for the key ring on the file system by clicking the  button next to the field. OpenPGP keys can be managed in Managed File Transfer's"OpenPGP Key Manager" on page 723 page.

Note: A default key ring is provided in Managed File Transfer for holding OpenPGP secret keys. The location of this key ring is **[installdirectory]/userdata/keys/pgp/secring.skr** where [installdirectory] is the installation directory of the Managed File Transfer product.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

Informatica MFT Server Resource

An Informatica MFT Server Resource stores the connection settings for connecting to a server running Managed File Transfer. When creating a "Trigger Manager" on page 206 that needs to run a Managed File Transfer Project, you can choose a pre-configured Managed File Transfer server from the drop-down list.

When this resource connects to a Managed File Transfer system that is running in a clustered environment, specify the other systems in the cluster on the Alternate Systems tab. If the primary system specified on the Basic tab is unavailable when a Trigger tries to execute a Project, it will retry the execution on the alternate systems.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the Managed File Transfer Resource. This name should be descriptive enough so users can quickly identify this Resource. The name cannot exceed 50 characters.

Description

The description is optional information to describe the Resource.

Host

The host name or IP address of the Managed File Transfer instance.

Port

The port number to use when connecting to the Managed File Transfer instance. If this field is left blank, the default port number for HTTP connection types is 8000 and 8002 for HTTPS connection types.

User

The user name (login name) to use for connecting to the Managed File Transfer instance.

Password

The password to use when connect to the Managed File Transfer instance. If encryption on the password is required, click the **Encrypt...** button.

Is Password Encrypted?

Indicates whether or not the password is encrypted. Select **Yes** if the Encrypt button was clicked above.

Connection Tab

The Connection tab contains the following fields:

Connection Type

The connection type can either be standard HTTP or secure HTTPS. If this field is left blank, the default connection type is HTTP.

Base URL

This is the base (or context) URL of the remote Managed File Transfer instance.

Connection Timeout

The maximum amount of time, in seconds, to wait when trying to establish a connection to the Managed File Transfer instance. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.

Read Timeout

The maximum amount of time, in seconds, to wait for a (read) response from the Managed File Transfer instance. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

Proxy Tab

The Proxy tab contains the following fields:

Host

The host name (or IP address) of the proxy server on your network. This is only needed if your system uses a proxy server to make HTTP(S) connections.

Port

The port number of the proxy server on your network. This is only needed if your network uses a proxy server to make HTTP(S) connections.

User

The User Name (login name) to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP(S) connections.

Password

The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTP(S) connections. After entering the password, you can optionally click the **Encrypt** button to encrypt the password.

Is Password Encrypted?

Indicates whether or not the password is encrypted. Select **Yes** if you clicked the **Encrypt** button for the Password.

SSL Tab

The SSL tab contains the following fields:

Implicit Trust

Indicates whether or not to trust the Managed File Transfer server regardless if a valid server certificate is specified. If this field is left blank, the default value is No.

Verify Host Name

Indicates whether or not the host name of the Managed File Transfer server should be verified against the server certificate. If this field is left blank, the default value is Yes.

Server Certificate Key Store Tab

The Server Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store (which contains the trusted server certificates) for authenticating the Managed File Transfer server. Type the file location in the text box or click the  icon to browse for a file. If a key store is not specified, then the Managed File Transfer server will be treated as a trusted server. Trusted certificates are managed on the "SSL Certificate Manager" on page 732 page.

Password

The password protects the Server Certificate Key Store. After entering the password, you can optionally click the **Encrypt** button to encrypt the password.

Is Password Encrypted?

Indicates whether or not the password is encrypted. Select **Yes** if the **Encrypt** button was clicked for the Server Certificate Password.

Type

Indicates if the key store is JKS (Java Keystore) or PKCS12 (Public Key Cryptology Standard). If this field is left blank, the default is JKS.

Client Certificate Key Store Tab

The Client Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store containing the client certificates and private keys. This is only required when the HTTPS server requires that HTTPS clients are authenticated with a certificate. Type the file location in the text box or click the  icon to browse for a file. Certificates and private keys are managed in the "Manage SSL Private Keys" on page 733 page.

Password

The password to use for accessing the Client Certificate Store. After entering the password, you can optionally click the **Encrypt** button to encrypt the password.

Is Password Encrypted?

If the password is encrypted, from the drop-down list, click to select **Yes**.

Type

Indicates if the key store is JKS (Java Keystore) or PKCS12 (Public Key Cryptology Standard). If this field is left blank, the default is JKS.

Alternate Systems Tab

When Managed File Transfer is running in a clustered environment, it is recommended to specify the host name or IP addresses of other systems in that cluster. If the system specified on the Basic tab does not respond, the alternate systems will be tried in the order indicated.

The Alternate Systems tab contains the following fields:

Alternate Host

The IP address or host name of a system in the Managed File Transfer cluster. The alternate Managed File Transfer system is used when the primary server is unavailable.

Alternate Port

The port number to use when connecting to the alternate Managed File Transfer system. If this field is left blank, the default port number is 8000 for HTTP and 8001 for HTTPS.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

Informatica HTTPS Server Resource

An Informatica HTTPS resource defines the connection information to the HTTPS "Service Manager" on page 516 used by Web Users. Managed File Transfer can connect to Informatica HTTPS Servers for securely exchanging files over encrypted SSL connections. When defining a Informatica HTTPS Server resource in Managed File Transfer, you need to indicate the Informatica HTTPS connection properties such as the host name (or IP address), and optionally the SSL certificates, user, password and proxy information.

Basic Tab

The Basic tab contains the following fields:

Name

A user-defined name which identifies the Informatica HTTPS Server. This name should be descriptive enough so users can quickly identify this Informatica HTTPS Server when prompted to choose from a list (for example, "Bank Informatica HTTPS Server"). The name cannot exceed 50 characters.

Description

A short paragraph that describes the Informatica HTTPS Server. The description is optional.

Host

The host name or IP address of the Informatica HTTPS Server.

Port

The port number to use for connecting to the Informatica HTTPS Server. If this field is left blank, then the default port number of 443 will be used.

User

The "Web User Management" on page 589 name (login name) to use for connecting to the Informatica HTTPS Server.

Password

The password to use for connecting to the Informatica HTTPS Server. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the Informatica HTTPS Server resource, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Password.

Connection Tab

The Connection tab contains the following fields:

Connection Timeout

The maximum amount of time, in seconds, to wait when trying to establish a connection to the Informatica HTTPS Server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.

Read Timeout

The maximum amount of time, in seconds, to wait for a (read) response from the Informatica HTTPS Server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

SSL Context Protocol

Specify the protocol to use when creating the SSLContext. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (SSL) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support SSLv3.

Proxy Tab

These options are only needed if your system uses a proxy server to make HTTP(S) connections. The Proxy tab contains the following fields:

Proxy Type

Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.

Host

The host name (or IP address) of the proxy server on your network. This is only needed if your system uses a proxy server to make HTTPS connections.

Alternate Host

The host name or IP address of an alternate proxy server. The alternate proxy server is used when the primary proxy server is unavailable.

Port

The port number of the proxy server on your network. This is only needed if your network uses a proxy server to make HTTPS connections.

User

The user name (login name) to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTPS connections.

Password

The password to use for connecting to the proxy server. This is only needed if your network uses a proxy server to make HTTPS connections. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

Note: If you do not wish to store the password for the proxy server, the password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Proxy Password.

Server Certificate Key Store Tab

The settings on the Server Certificate Key Store tab are only required when the Informatica HTTPS server requires that HTTPS connections are authenticated with a certificate. The Server Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store (which contains the trusted server certificates) for authenticating the Informatica HTTPS Server. You can browse for the key store on the file system by clicking the  button. If a key store is not specified, then the Informatica HTTPS Server will be treated as a trusted server. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

A default key store is provided in Managed File Transfer for holding trusted server certificates. The location of this key store is **[installdirectory]/userdata/keys/x509/trustedCertificates.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Password

The password to use for accessing the trusted Server Certificate Store. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

If you do not wish to store the password with the Informatica HTTPS Server resource, this password can be supplied when executing a Project.

Is Password Encrypted?

Indicates whether or not the password for the Server Certificate Store is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Server Certificate Store Password.

Type

Indicates if the type of the key store is **JKS** (Java Keystore) or **PKCS12** (Public Key Cryptology Standard). If this field is left blank, the default store type is JKS.

The default key stores provided with the installation of Managed File Transfer are JKS type.

Client Certificate Key Store Tab

The settings on the Client Certificate Key Store tab are only required when a client requires that HTTPS connections are authenticated with a certificate. The Client Certificate Key Store tab contains the following fields:

Key Store File

The location of the key store containing the client certificates and private keys. This is required only when the Informatica HTTPS Server requires that HTTPS clients are authenticated with a certificate. You can browse for the client key store on the file system by clicking the  button next to the field. Certificates can be managed in Managed File Transfer's SSL Certificate Manager page.

A default key store is provided in Managed File Transfer for holding client certificates and private keys. The location of this key store is **[installdirectory]/userdata/keys/x509/privateKeys.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Client Certificate Store Password

The password to use for accessing the Client Certificate Store. After entering the password, you can optionally click the **Encrypt** button, which will encrypt the password when it is stored in Managed File Transfer's database.

If you do not wish to store the password with the Informatica HTTPS Server resource, this password can be supplied when executing a Project.

Is Password Encrypted

Indicates whether or not the password for the Client Certificate Store is encrypted. You should choose the option of **Yes** if you clicked the **Encrypt** button for the Client Certificate Store Password.

Client Certificate Alias

A particular key within the default key store can be used for client authentication by indicating the key alias. The specified key will be used when required by the Informatica HTTPS Server. Browse for the client key store on the file system by clicking the  button next to the field.

Client Certificate Store Type

Indicates if the type of the key store is **JKS** (Java Keystore) or **PKCS12** (Public Key Cryptology Standard). If this field is left blank, then the default store type of JKS will be used.

The default key stores provided with the installation of Managed File Transfer are JKS type.

Contacts Tab

The Contacts tab allows you to store the contact information for the Resource. The Contact tab contains the following fields:

Name

The name of the contact for the resource.

Phone Number

The contact's phone number.

Email

The contact's email address.

CHAPTER 4

Workflows

Projects can be created in Managed File Transfer to automate any file transfers and business processes (workflows) for your organization. These Projects can be "Executing Projects" on page 181 immediately or "Scheduling Projects" on page 187 to run at future dates and times. A Project can also run when a certain event occurs, such as when a new file appears in a folder (defined in a "Monitors" on page 197) or when a file is uploaded from a trading partner (defined in a "Trigger Manager" on page 206).

Project Design

Projects are used to describe the work for Managed File Transfer to perform. For instance, a *Project* definition can indicate where to retrieve data from, what processes to perform on the data (for example, convert to Excel, Zip, encrypt) and where to distribute the output.

Project's are made up of Modules, Tasks and Elements.

Module

A Module is a logical grouping of one or more Tasks. For instance, a module may be defined with three Tasks to be executed in sequential order. The first Task in the Module may read (parse) data from an XML document. The second Task may insert that data into a database file. The third Task could then call a program to process that data.

Multiple modules can be defined in a Project. A Module can pass control to another Module based on certain conditions. For instance you could have a main Module to perform a series of tasks. If any errors are encountered in the main Module, you could have control passed to another module that sends an error notification to an email address or perform some other Tasks. The "Call Module Task" on page 433 task can execute another Module in a Project to perform a sub-routine of tasks based on specific criteria.

IF Condition

An IF Condition controls if a block of tasks will run if a condition is met. The "IF Condition" on page 146 is like a Yes/No decision point in a process flow chart.

Else

An "Else" on page 147 clause controls a block of tasks that will run when a preceding IF condition evaluates to false.

Loops

Loops are complex components that repeat a set of Tasks on the data or files produced in a Project. For instance, the data in a spreadsheet needs to be read into a database. A "Loops" on page 148 contains

the Tasks that will read a row of data, evaluate and process it and then iterate to the next row of data and repeat the Loop.

Task

A Task is a discrete business process to perform. For instance, a Task may write data to an XML document, send an email, import data from an Excel file, or FTP a file. Managed File Transfer includes dozens of different Chapter 5, “Task Reference” on page 227 to choose from when building a Project. There is no logical limit to the number of Tasks that can be defined in a Project.

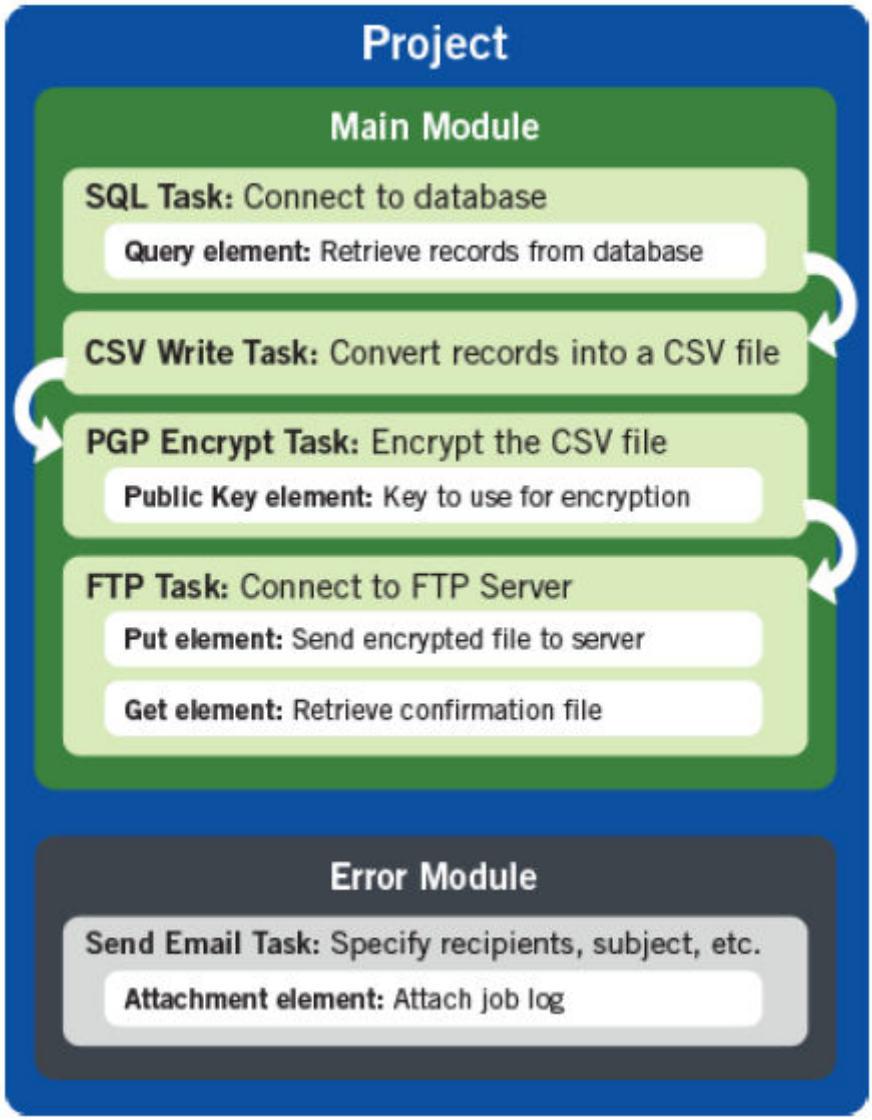
Element

A Task is made up of one or more Elements, which describes the types of work to perform within the Task. For example, the FTP task has an Element to put a file on a FTP server, an Element to get a file from a FTP server, an Element to rename a file on a FTP server, and so on. As another example, the Send Email task has an Element to indicate the attachments to send.

Example of Modules, Tasks and Elements

Listed below is an example of a Project with two modules. In the first module, named "Main", it performs four different tasks. The first task (SQL) connects to a database and retrieves records from a table. The second task (CSV Write) converts the records into a CSV file. The third task (PGP Encrypt) will encrypt the CSV file.

The fourth task (FTP) will send the encrypted CSV file to a FTP server and get back a confirmation file. In the second module, named "Error", it has a single task that sends an email with the job log attached.



Designing Projects

A Project can be created "Add Project (from scratch)" on page 167 by choosing the specific Tasks needed, or you can create a Project by using one of the included "Add Project (with template)" on page 166. Using a template is generally the fastest approach for creating a Project, since each template contains a pre-defined group of Tasks for performing commonly used business processes.

To work with Project definitions, click **Workflows** from the Main Menu, and then click **Projects**. Then drill down through the folders (on the left side of the page) to view the list of Projects within them.

Options are available to create and manage "Project Folders" on page 168 and Projects from within this page. If a user does not have read, write or execute "Folder Permissions" on page 170 for a Project folder, the folder and the "Project Explorer" on page 164 inside it are not displayed.

Predefined Projects

Informatica Managed File Transfer includes predefined projects that you can use directly or as templates to create your own customized projects.

The following predefined projects, which are used to define B2B Data Exchange endpoints, are available for use in the `DXProjects/Receive` folder:

- DX_Remote_FTP_Receive: Receive files using the FTP communications protocol.
- DX_Remote_FTPS_Receive: Receive files using the FTPS communications protocol.
- DX_Remote_HTTP_Get: Receive files using the HTTP communications protocol.
- DX_Remote_HTTPS_Get: Receive files using the HTTPS communications protocol.
- DX_Remote_SCP_Receive: Receive files using the SCP communications protocol.
- DX_Remote_SFTP_Receive: Receive files using the SFTP communications protocol.
- DX_Hosted_PGP_Decrypt: Receive the files and then decrypt the files with PGP encryption.
- DX_Hosted_Unzip: Receive and unzip the files.

The following predefined projects, which are used to define B2B Data Exchange endpoints, are available for use in the `DXProjects/Send` folder:

- DX_Remote_AS2_Send: Send files using the AS2 communications protocol.
- DX_Remote_FTP_Send: Send files using the FTP communications protocol.
- DX_Remote_FTPS_Send: Send files using the FTPS communications protocol.
- DX_Remote_HTTP_POST: Send files using the HTTP communications protocol.
- DX_Remote_HTTPS_POST: Send files using the HTTPS communications protocol.
- DX_Remote_MI_Send: Send files using the Informatica Intelligent Cloud Service mass ingestion task.
- DX_Remote_SCP_Send: Send files using the SCP communications protocol.
- DX_Remote_SFTP_Send: Send files using the SFTP communications protocol.
- DX_Hosted_PGP_Encrypt: Encrypt the files with PGP encryption and then send the files.
- DX_Hosted_Zip: Zip and then send the files.

For more information about how to use these predefined projects with B2B Data Exchange endpoints, see the "Endpoints" chapter in the *B2B Data Exchange Operator Guide*.

Custom Notifications From Projects

Applications such as that are integrated with Informatica Managed File Transfer, consume files as soon as they are downloaded or extracted.

Developers can design Managed File Transfer projects to perform actions such as copy, rename, merge, or any other custom task and when the file is ready to be consumed, developers can notify the consuming application such as Managed File Transfer by using the **Notify Consumer** task.

In order to send custom notifications to consumers, users must configure projects as follows:

1. Create a variable to stop auto-notifications.
2. Create a task to notify consumer.

Denying Auto Notifications

Create a variable to stop notifications that consumers receive as soon as the file is downloaded or extracted.

For more information about creating variables, see "Creating a Variable" on page 113.

1. Right-click the name of the project and select **Add a Variable**.

   The variable page displays.
2. Enter the name of the variable as `deny.event.auto.notifications`.
3. Set the value of the variable to `True`.
4. Enter a description of the variable.
5. Save the project.

Creating Custom Notifications

Create a custom notification task to notify consumer that the file is available for use.

For more information about adding a task, see "Notify Consumer Task" on page 452.

1. Select **Project** > **Component Library** > **Miscellaneous** and drag it to the project outline.
2. Provide the value for Source File with the full file path or the source file variable, enter other notify task field definitions, and save the project.

   For more information about Notify Task Definitions, see "Notify Consumer Task Definitions" on page 452.

Project Designer Features

Managed File Transfer's Project Designer feature allows authorized Admin Users to create, edit and debug Projects quickly without the need for programming or special skills.

Permissions Required

An Admin User must have the following permissions in order to edit a Project in the Project Designer:

- Project Designer role
- Write permission for the folder in which the Project is located
  You can access the Project Designer by following the steps below:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows**, and then click the Projects link.
3. Drill down to the folder you want to work in.
4. Select a Project to edit it. Otherwise, to create a new Project, click the  Create a Project link in the page toolbar.
5. The Project Designer page will be shown.

   The Project Designer is split into three panels. The Project Outline and Component Library are shown on the left side of the page and the Work Panel is shown on the right side of the page.

Page Toolbar

The following actions are available from the page toolbar:

- Save any changes to the Project by clicking the **Save** button.
- Exit the Project Designer by clicking the **Exit** button. You will be prompted to save any changes you made to the Project.
- Check the syntax of the Project by clicking the **Validate** button.
- Execute the Project interactively by clicking the **Execute Project** button.
- Debug the project by clicking the **Debug** button. This is helpful for finding errors in a Project or to begin executing at a particular task in the Project.
- Show the XML definition of the Project by clicking the **Show XML** button. The Project is automatically saved when the XML is displayed. It is not recommended to change the XML definition without specific instructions from Informatica.

  Note: You can change the width of the Project Outline and Component Library panes by dragging the divider lines to the left or right.

Using the Work Panel

The Work Panel (located on the right side of the page) shows the attributes for the component (Project, Module, Task, Element, Variable) that is selected from the Project Outline. It also is used to prompt for the attributes for new components that are being added to the Project. Additionally, it provides functions for working with the component and Project.

Using the Project Outline

The Project Outline provides a summary of the components and structured workflow of the Project.

Each component (node) in the Outline will have an icon which denotes its type, as described below.

- *Project*
- "Exit Project Task" on page 440
- *Module*
- "Exit Module Task" on page 439
- *Task*
- *Element*
- *IF Condition*
- "Loops" on page 148
- "Iterate Loop" on page 158
- "Exit Loop" on page 159

 - "Delay Task" on page 149

 - *Variable*

- *Comment*

 - "Sharing Common Logic between Projects (Snippets)" on page 164

Each component will also show a label (name) that was either specified by the user or the Managed File Transfer default (if a label was not specified by the user).

The Project Outline context menu can be displayed by right clicking on any component in the Outline. Components can be moved by dragging and dropping them in the Outline.

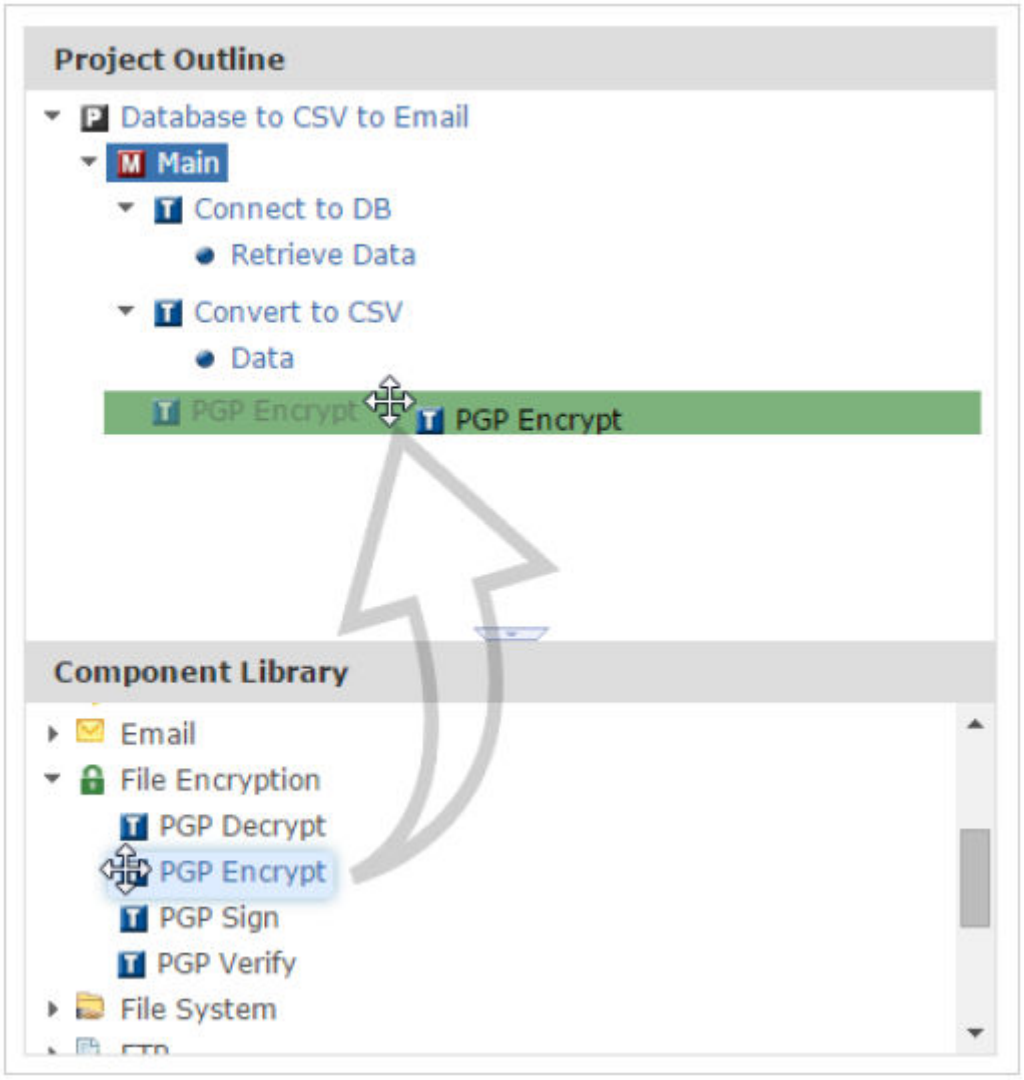
Listed below are the actions that can be performed in the Project Outline:

- Add a Module to the Project by right-clicking the Project component and selecting Add a Module.
- Add a Variable to the Project by right-clicking the Project component and selecting Add a Variable.
- Import a Project Source containing variables or code snippets by right-clicking the Project or Module component and selecting Import Project Source.
- Add an IF Condition to the Project by right-clicking the Module and selecting Add If.
- Add a Loop to a Module by right-clicking the Module component and selecting the desired Loop type.
- Add an Element to a Task by right-clicking the component and selecting the element type.
- Add a Comment to a Module, Task, Element, Variable or IF Condition by right-clicking the component and selecting Add a Comment.
- Move Up a Module, Loop, Task, Element or IF Condition in the Project Outline by right-clicking the component, pointing to Edit, and then selecting Move Up.
- Move Down a Module, Loop, Task, Element or IF Condition down in the Project Outline by right-clicking the component, pointing to Edit, and then selecting Move Down.
- Delete a Module, Loop, Task, Element or IF Condition from a Project by right-clicking the component, pointing to Edit, and then selecting Delete.
- Cut a Loop, Task, Element or IF Condition from a Project by right-clicking the component, pointing to Edit, and then selecting Cut.
- Copy a Loop, Task, Element or IF Condition from a Project by right-clicking the component, pointing to Edit, and then selecting Copy.
- Paste a Loop, Task, Element or IF Condition into a Project by right-clicking the component, pointing to Edit, and then selecting the appropriate Paste option.
- Disable a Module, Loop, Task or IF Condition by right-clicking the component, pointing to Edit, and then selecting Disable. Disabled components will appear dimmed in the Project Outline panel.
- Enable a Module, Loop, Task or IF Condition by right-clicking the component, pointing to Edit and then selecting Enable.

  Note: The right-click menu in the Project Outline pane is context sensitive to the particular component. The right-click menu will always provide the available attributes or options for the Project, Module, Task, Element or IF Condition.

Using the Component Library

The Component Library contains all the components that can be added to a Project. To add a component to the Project Outline, simply drag it from the Component Library to the desired location in the Project Outline. The component can be placed in any green highlighted area (pictured below).



After a component is placed, it can be moved at any time by dragging and dropping it to a new location in the Project Outline.

Keyboard Commands

The Project Designer supports the following keyboard commands:

Ctrl + S	Saves any changes made to the Project.
Ctrl + C	Copies the selected component to the Project Clipboard.
Ctrl + X	Cuts the selected component from the Project Outline and stores it in the Project Clipboard.

Ctrl + V	Pastes a copied or cut component from the Project Clipboard into the Project Outline.
del	Deletes the selected component.

Note: The contents of an input field will be cut, copied, pasted, or deleted when the field has focus.

Project

A Project can have its own properties to describe the Project and its behavior. Listed below are the properties (field descriptions) on each tab of the Project component.

Basic Tab

Project Name

The Project Name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores (_), periods (.) and white spaces. Maximum length is 50 characters.

Description

A short paragraph describing the Project. The Description is optional and cannot exceed 512 characters.

Main Module

The first module executed in a project is considered the Main Module and by default is given the name Main. If the first module that should start in the project is not the Main module or the Main module name was changed, modify the Main Module field accordingly.

Control Tab

Version

The version number refers to the edition of the Managed File Transfer software running the project. If improvements were made to the project handling in a future version, existing projects would not stop running as they would function based on the version in which they were created.

Project versions can differ from Task versions. Refer to the "Upgrade Project" on page 180 section to learn about upgrading Project versions or the "Outdated Tasks" on page 441 section for more information regarding versions and how to change Task versions, if available.

Log Level

Specify the level of log messages that will be generated when this Project executes. The log level impacts the amount of information that is recorded in the "Job Log and Details" on page 186.

Note: All modules and tasks within this Project will inherit the specified log level, unless the log level is overridden on the individual modules or tasks.

Silent	Logs Project-level information, such as the name of the user that ran the project, when the project started, any variables passed in and when the project stopped. It also logs any errors encountered.
Normal	Additionally logs the start and stop times of Modules, Loops and Tasks.
Verbose	Additionally logs Task-level details, such as the names of the files that were processed.
Debug	Additionally logs detailed debugging information, such as message responses from servers.

Job Queue

The Project is placed in "Job Queue Manager" on page 217 when executed in batch mode. If the Job Queue is not specified, the Project is placed in the default Job Queue. The Job Queue on the Project's Control tab is overridden by the Job Queue specified on the "Scheduling Projects" on page 187, "Execution from Administrator (with Advanced Options)" on page 184 page, "Call Project Task" on page 434 Task, "Call Remote Project Task" on page 437 Task, and the Managed File Transfer Command runProject command.

Job Name

Specify a name that identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters. Spaces are allowed. Variables are not allowed.

Thread-Safe

The Thread-Safe attribute determines whether or not it is safe to run multiple instances of the project simultaneously. The default value is false. A value of false ensures that only one instance of the project is active at any given time.

Timeout

Specify the maximum duration, in minutes, after which Managed File Transfer cancels the job. If no value is specified, the job continues to run until completion. Default is zero.

On Error Tab

On Error

The On Error option allows you to specify the action to take when any tasks error out within this Project. Valid options are:

- abort - The Project is aborted. No more tasks will be executed. This is the default setting.
- continue - Ignores the error and continues on with the next Module or task.
- call:module - Calls another Module in the Project.
- setVariable:[name]=[value] - Sets the variable in [name] to a new value in [value] and continues on with the next Module or task.

  Note: Any Modules and tasks within this Project will inherit the specified On Error option from the Project, unless the On Error option is specifically overridden on the individual Modules or tasks.

Module

A Module is a logical grouping of one or more Tasks. Multiple modules can be defined in a Project. For instance, one Module could contain the tasks to perform the data translation and the transmission of files, whereas another Module could be contain an email notification task that is called only when a problem occurs.

A Module can have its own properties to describe the Module and its behavior. Listed below are the properties (field descriptions) on each tab of the Module component.

Basic Tab

Module Name

Specify a name for this module. It must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores (_), periods (.) and white spaces.

Note: If this module name is changed (and if it was the first Module to run in the Project), then you will need to change the Main Module name on the Basic tab in the "Project" on page 108.

Description

A short paragraph describing the Module. The Description is optional and cannot exceed 512 characters.

Control Tab

Execute Only If

Specify a condition that must be satisfied before this module can be executed. This module will be skipped if the specified condition is not met. The condition is constructed using "Expressions" on page 125.

Log Level

Specify the level of log messages that will be generated when this Module executes. If not specified, then the log level will be inherited from the Project.

Note: All tasks within this Module will inherit the specified log level from the Module, unless the log level is specifically overridden on the individual tasks.

Silent	Only logs any errors that are encountered in the Module.
Normal	Additionally logs the start and stop times of the Module, as well as the times of any Loops and Tasks in the Module.
Verbose	Additionally logs task-level details, such as the names of the files that were processed.
Debug	Additionally logs detailed debugging information, such as message responses from servers.

Disabled

Modules can be disabled if needed. If a module is disabled, it will appear grayed out in the Project Outline.

On Error Tab

On Error

The On Error option allows you to specify the action to take when any tasks error out within this Module. Valid options are:

- abort - The Project is aborted. No more tasks will be executed.
- continue - Ignores the error and continues on with the next Module or task.
- call:module - Calls another Module in the Project.
- setVariable:[name]=[value] - Sets the variable in [name] to a new value in [value] and continues on with the next Module or task.
  If the On Error option is not specified, then the Module will inherit the On Error setting from the Project level.

  Note: All tasks within this Module will inherit the specified On Error option from the Module, unless the On Error option is specifically overridden on the individual tasks.

Variables

A variable is an element that acts as a reference to a particular value. Variables can be used in Projects to supply input values to their attributes. There are seven different types of variables in Managed File Transfer.

- "User Defined Variables" on page 112 - A variable that you can define in a Project with a unique name and default value. A user-defined variable can be used to supply a value to a task attribute and can be used in comparison operations.

- "System Variables" on page 114 - A pre-defined variable that is supplied in Managed File Transfer, such as the current date. System variables are similar to user-defined variables, in that they can be used to supply a value to a task attribute and can be used in comparison operations.
- "Folder Variables" on page 115 - Folder level variables can be defined at each folder level. These variables can be used by any Projects contained within that folder. User defined Project level variables override any Folder level variables.
- "File Lists and File Sets" on page 116 - A variable that contains a list of file names. A File List is generated by tasks that retrieve or process files. A file list can be used as the input for tasks that can process multiple files (such as a ZIP Task).
- "Local Files" on page 116 - These variables represent local files on the host system (where Managed File Transfer is running). These files could be the files on the local hard drive or files on the network which are accessible to Managed File Transfer's Subsystem/Service.
- "RowSet" on page 121 - A variable that contains a list of records (rows). A RowSet is generated by tasks that read the contents of a file or database (for example, SQL Task, Read CSV, Read Fixed-width, Read Excel, Read XML and Read Flat File). RowSets can be used as the input for tasks that write out to databases or files .
- "Email Lists" on page 122 - A variable that contains a list of Email Messages. An Email List is generated by the Retrieve Email task which can be used in a For Each Loop to process email attachments and message content.
- "Denying Auto Notifications" on page 104 - A variable that stops the notification that consumer receives automatically as soon as the file is downloaded or extracted. This variable can be used in a Managed File Transfer project followed by a task that creates a custom notification message when the file is ready for consumers to use.
- "AS2 Task Output" on page 124 - A variable that contains a list of attributes with information pertaining to the execution of an AS2 Task. These can be used to further process files or tasks within a Managed File Transfer project.
- "MQ Message List" on page 124 - A variable that contains a list of MQ Messages. An MQ Message List is generated by the MQ Retrieve Message Task which can be used in a For Each Loop to process message content.

Complex Variable Types

A complex variable can be defined as anything that is not a simple string or a number. For example, a Local File can be considered a complex variable with various attributes in it such as the name, path, extension, size, etc. To retrieve the attributes of a complex variable use the following variable reference syntax.

${variableName:attributeName}.

The colon (:) separates the variable from the attribute.

Note: Variables and their attributes are case sensitive. For example, ${file:lastModifiedDate} returns the name of the file and ${file:lastmodifieddate} will generate an error with the message: Variable Not Found.

User Defined Variables

You can create your own user-defined variables in a *Project*, which can be used in one or more tasks within that Project. When creating variables, you specify their names and default values. You can optionally pass the

values for these variables (which will override the default values) when the Project is executed. These variables can also be encrypted for data security purposes.

A user-defined variable can be used for two purposes within a Project:

- To supply the value for an attribute (property) in a task.
- To be used in a compare operation to determine if a Project task or module should execute.

Creating a Variable

Create a user-defined variable within a Project by following the steps below:

1. When defining a Project, right-click the Project component (the very top node in the Project outline).
2. Select the **Add a Variable** menu item.
3. You will be prompted with a page to add a new variable.
4. Specify the name and default value for the variable. You can optionally specify a description for the variable (for documentation purposes).
5. Click the **Save** button to add the variable to the Project.

Using a Variable as a Task Attribute

Follow the instructions below to use a user-defined variable within a task attribute (property):

1. When defining a task in a Project, click the `${var}` icon next to the field to insert a variable (if applicable).
2. A list of variables is displayed.
3. Click the variable to use in the attribute.
4. When using a variable within a Project task attribute, it should be formatted as ${variablename}.

   Listed below is an example of how the user-defined variable of "File_Suffix" is used to suffix (append) its value to a file name.

Note: More than one variable can be combined into a task's attribute. For instance you could have a variable containing a directory name (named "dir"), another variable containing a file name (named "file") and yet another variable containing a file extension (named "ext"). You could use all three variables for building a file path by using the syntax of ${dir}/${file}.${ext}

Using a Variable in a Condition

Follow the instructions below to use a user-defined variable within a comparison operation:

1. When defining a task or module in a Project, click the **Control** tab.
2. Specify the variable for the **Execute Only If** condition.

   Below is an example of how the user-defined variable of "FileCount" is used to determine if a task should execute. In this example, the task will execute only if the FileCount is not equal to 0.

Overriding a Variable at Runtime

The values for user-defined variables can be overridden when a Project is executed.

The first approach is to execute the Project with "Execution from Administrator (with Advanced Options)" on page 184 from within Managed File Transfer's Administrator. The advanced options page will show you the default values for the variables and will allow you to override them at execution time.

The second approach is to override the variable values by passing parameters on the supplied RUNPROJECT command, which can be run from "Execution from Windows and Unix" on page 184 platforms.

Note: Variable names are not case-sensitive. For example, a variable named "State" can also be referred to as "STATE".

System Variables

System variables are included with Managed File Transfer for use within Project tasks. A system variable can be used for two purposes within a Project:

- To supply the value for an attribute (property) in a task.
- To be used in a compare operation to determine if a Project task or module should execute.
  The system variables provided in Managed File Transfer are listed below:

System Variable Name	Description
system.caller.id	ID (or job number) of the calling project.
system.caller.project	Project location of the calling project.
system.carriageReturn	A carriage return (CR) character.
system.currentDate	The current date in ISO (yyyy-MM-dd) format. This variable is created by the Timestamp task, which should be placed before any tasks that need this variable.
system.currentTime	The current time in ISO (HH:mm:ss) format. This variable is created by the Timestamp task, which should be placed before any tasks that need this variable.
system.currentTimestamp	The current date and time in ISO (yyyy-MM-dd HH:mm:ss) format. This variable is created by the Timestamp task, which should be placed before any tasks that need this variable.
system.docroot	Documents root directory (also known as DOCROOT) as defined in the global settings.
system.emptyString	An empty string.
system.installDir	Managed File Transfer's product installation directory.
system.environment	The name of the Managed File Transfer environment as specified in the global settings. If a name is not specified, the value of this variable will be blank.
system.java.vendor	Java vendor on which Managed File Transfer is running.
system.java.version	Version of Java on which Managed File Transfer is running.
system.job.error	The last error which occurred in the job, if any.

System Variable Name	Description
system.job.id	The id (or job number) of the current job.
system.job.log	Log file location of the current log
system.job.name	The name of the Job that was specified on the Project, Monitor, Trigger, or Scheduler.
system.job.workspace	Workspace directory location of the current job. This variable is created by the Create Workspace task, which should be placed before any tasks that need this variable.
system.lineFeed	A line feed (LF) character.
system.os.arch	Operating system's architecture on which Managed File Transfer is running.
system.os.name	Name of the operating system on which Managed File Transfer is running.
system.os.version	Version of the operating system on which Managed File Transfer is running.
system.project.location	The location (folder) of the current Project.
system.project.name	The name of the current Project.
system.systemName	The name of the system that processed the Project. The system name is specified in the [installdirectory]/config/cluster.xml file.
system.tab	A tab character.
system.user.email	Email address of the user that is executing the Project.
system.user.home	Home directory of the user that is executing the Project.
system.user.name	The name of the user that is executing the Project.
system.version	Product version of Managed File Transfer.

Using a System Variable

Follow the instructions below to use a System variable within a task:

1. When defining a task in a Project, click the 

icon next to the attribute in which you want to use a System variable.
2. A list of variables will be displayed.
3. Click the System variable to use in the attribute.

   Listed below is an example of how the System variable of system.job.workspace is used to indicate the destination directory for files retrieved on a FTP task. The workspace is a system directory created for the job for storing temporary files.

Note: When using a System variable within a Project task, it should be formatted as ${systemvariablename}.

Folder Variables

Folders are used for grouping similar Projects together and for controlling which users have access to those Projects. Folders can also be used to define variables that all Projects in the folder and its subfolders can

access. For example, a variable containing administrator email addresses defined on the root folder would be accessible by every Project in Managed File Transfer. If the list of administrators needs updated, the variable could be modified which will automatically be reflected in all Projects.

Variables can be defined on each folder level in the folder tree. Subfolders can override a parent folder's variable value by defining a variable with the same name. For example, if the root folder contained a variable named 'admins', a subfolder could also contain a variable named 'admins' and override the value just for that folder. If a Project has a variable defined with the same name as a folder variable, the variable value in the Project will take precedence.

Variables are administered using the "Add Folder" on page 168 and "Edit Folder" on page 169 folder links on the "Project Explorer" on page 164 page.

File Lists and File Sets

A **File List** references a set of "Local Files" on page 116 or "Remote Files" on page 120 objects that were retrieved or processed by a task. The File List element defines the variable name for the File List, and uses the File Set element to define the target directory where the files are located. A File List can have one or more File Sets, which allows you to create a single File List that contains files from multiple directories.

The File Set element also allows you to add optional file filters that let you search for files with specific attributes. The files to select can be included and excluded based on various filter criteria:

- Wildcards (for example, *.* or *.txt or pay??.xls)
- Regular expressions
- Date/time ranges
- Size ranges
  For instance, you could add a File Set to a Zip task that compresses any files that end with an .xls extension which were created after 2010-12-15 with a size of 100 kb or greater.

  You can iterate through each file in a File List variable using a "Loops" on page 148.

Local Files

The Local File variable specifies the absolute path and file name of a single file (for example, C:\mydir \myfile.txt on a Windows system, and /mydir/myfile on a UNIX system). The Local File variable is created by a Task that outputs a single "File Paths" on page 161 (for example, Write CSV or Merge File), or Tasks that output multiple Local Files as part of a "File Lists and File Sets" on page 116.

Each Local File variable contains the following attributes:

Attribute Name	Description
name	The name of the file, including the extension if one exists. If the Local File's path is /orders/company/20150304.txt, then the value of this attribute would be 20150304.txt
exists	This returns a true or false value on whether the file exists.
extension	The extension of the file if one exists. If the Local File variable is a directory, then the value of this attribute will be an empty string. If the Local File variable is a data file and the file has an extension, the extension will be returned. If the file does not have any extension, an empty string is returned.

Attribute Name	Description
lastModifiedDate	The last modified date and time of the file in ISO format, yyyy-MM-dd HH:mm:ss.SSS. Refer to the date and time format symbols for more information.
lastModifiedMillis	The last modification date and time of the file in milliseconds since the Unix timestamp (January 1, 1970).
size	The size of the file in bytes, which is a whole number.
parentFile	The path or folder location containing the file. For example, C:\temp\ or /tmp/. The path and path separators are dependent on the host operating system.
path	The absolute path of the file. For example, C:\temp\myfile.txt or /documents/myfile.txt. The path and path separators are dependent on the host operating system.
nameWithoutExtension	The name of the file excluding the extension.

Note: All attribute names are case sensitive.

Creating a File List

In the example below, a File List variable will be created that references XML files from a local directory.

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
2. On the Basic tab of the Create File List task, specify the File List Variable value:
   File List Variable

   The name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists, then it will be overwritten.
3. Click the **Add** button in the sub-menu and select the **File Set** option from the sub-menu.
4. Within the File Set page, specify the directory containing the files.
5. Click the **Add** button in the sub-menu and choose the **Add a Wildcard Filter** option from the sub-menu.
6. Click the **Add** button (since the Wildcard Filter element does not have any attributes) and choose the **Include Files** option from the sub-menu.
7. From the next page, specify the pattern of the files to include. Specify a ? to match a single character. Specify an * to match zero or more characters. For example, specify the pattern of *.xml to include all files that end with “xml”. As another example, specify the pattern of *.* to include all files that in the directory.
8. Click the **Save** button when done specifying the pattern.

Creating a File List from Multiple Directories

In the example below, a File List variable will be created that references XML files contained in two different local directories.

1. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the Call Module task to the Project Outline.

2. On the Basic tab of the Create File List Task, specify the File List Variable value:
   File List Variable

   The name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists, then it will be overwritten.
3. Click the **Add** button in the sub-menu and select the **File Set** option from the sub-menu.
4. Within the File Set page, specify the directory containing the files.
5. Click the **Add** button and choose the **Add a Wildcard Filter** option from the sub-menu.
6. Click the **Add** button (since the Wildcard Filter element does not have any attributes) and choose the **Include Files** option from the sub-menu.
7. From the next page, specify the pattern of the files to include. Specify a ? to match a single character. Specify an * to match zero or more characters. For example, specify the pattern of *.xml to include all files that end with “xml”. As another example, specify the pattern of *.* to include all files that in the directory.
8. From the Project outline, select the Create File List task you created.
9. Repeat steps 3 through 7 to add another File Set that references a different directory to the File List.
10. Click the **Save** button when done specifying the pattern.

Using a File List

In the example below, the variable called "archiveList" will be used as the input into the Zip Task. When the task is executed, the files referenced in the archiveList variable will be compressed into the ArchivedFiles.Zip output file.

Note: When using an input variable within a Project task, it should be formatted as ${variablename}

File Set Field Definitions

Add a File Set

The Add a File Set element allows you to specify a directory of files that will be processed by the task.

Field	Definition
Basic Tab	
Base Directory	Specify the starting directory or file location for the File Set. The directory or file location must be accessible to the user who runs the MFT application. If no filters are defined, all files in this directory will be included. **Note:** If the admin user enables the **Restrict to Home Directory** property, the restriction doesn't apply to the base directory.
Recursive	Specify whether or not to process files from all sub-folders within the base directory. Default is false.
Sort By	Specify whether to sort files by the last modified date. Default is none.

Sort Ascending	Specify the order to sort files. Select **true** to sort files in the ascending order. Select **false** to sort files in the descending order. Default is true.
Advanced Tab	
Stability Time	Time in seconds that Managed File Transfer waits to check the file stability. For example, if stability time is 10 seconds, Managed File Transfer verifies after every 10 seconds whether the file is in the process of transferring or is transferred completely. Default is 5 seconds.
Stability Failure File List Variable	Variable where Managed File Transfer captures the files it found to be unstable.

Wildcard Filter

The Wildcard Filter element allows you to specify a "Wildcards and Regular Expressions" on page 837 to include or exclude files that contain specific characters. The Wildcard Filter element does not contain any fields. You must add an Include or Exclude element.

Field	Definition
Include & Exclude Element Basic Tab	
Pattern	Specify the pattern to match. An asterisk (*) matches any number of characters and a question mark (?) matches a single character.
Case Sensitive	Specify whether or not the pattern is case sensitive. Default Value: false

Regular Expression Filter

The Regular Expression Filter element allows you to specify a "Wildcards and Regular Expressions" on page 837 to include or exclude files that contain specific characters. The Regular Expression Filter element does not contain any fields. You must add an Include or Exclude element.

Field	Definition
Include & Exclude Element Basic Tab	
Pattern	Specify the pattern to match. An asterisk (*) matches any number of characters and a question mark (?) matches a single character.
Case Sensitive	Specify whether or not the pattern is case sensitive. Default Value: false

Add a Date

The Date Filter element allows you to specify files that were created or modified in a specified time frame. The Date Filter element does not contain any fields. You must add an Include or Exclude element.

Field	Definition
Include & Exclude Element Basic Tab	
From Date	Specify a Start Date. The date must be entered in yyyy-MM-dd format. If a start time other than midnight is desired, then the format is yyyy-MM-dd HH:mm:ss. Leaving this value blank will match all files that are modified before the specified To Date.
To Date	Specify an End Date. The date must be entered in yyyy-MM-dd format. If an end time other than midnight is desired, then the format is yyyy-MM-dd HH:mm:ss. Leaving this value blank will match all files that were modified after the specified From Date.

Add a Size

The Size Filter element allows you to specify file of a certain size. The Size Filter element does not contain any fields. You must add an Include or Exclude element.

Field	Definition
Include & Exclude Element Basic Tab	
From	Specify the minimum file size. This must be a number and may optionally be followed by KB, MB or GB to denote Kilo Bytes, Mega Bytes and Giga Bytes.
To	Specify the maximum file size. This must be a number and may optionally be followed by KB, MB or GB to denote Kilo Bytes, Mega Bytes and Giga Bytes.

Remote Files

The Remote File variable refers to files on a remote system such as an FTP, FTPS, SFTP or Informatica HTTPS Server. The Remote File contains information about the file like name, extension and size. The path is relative to the remote system (for example, /home/user/myfile.txt).

Each Remote File variable contains the following attributes:

Attribute Name	**Description**
name	The name of the file, including the extension if one exists. If the Remote File's path is /orders/company/20150101.txt, then the value of this attribute would be 20150101.txt
extension	The extension of the file if one exists. If the Remote File variable is a directory, then the value of this attribute will be an empty string. If the Remote File variable is a data file and the file has an extension, the extension will be returned. If the file does not have any extension, an empty string is returned.

Attribute Name	Description
lastModifiedDate	The last modified date and time of the file in ISO format, yyyy-MM-dd HH:mm:ss.SSS. Refer to the date and time format symbols for more information. This attribute may only exist when using the Create a File List sub-task.
lastModifiedMillis	The last modification date and time of the file in milliseconds since the Unix timestamp (January 1, 1970). This attribute may only exist when using the Create a File List sub-task.
size	The size of the file in bytes, which is a whole number. This attribute may only exist when using the Create a File List sub-task.
path	The relative path of the file. For example, /home/user/myfile.txt.
nameWithoutExtension	The name of the file excluding the extension.

Note: All attribute names are case sensitive.

RowSet

A **RowSet** variable contains a list of records (rows) that were read from a file or database.

For instance, you may want to read data from an Excel file and then import that data into a database. In the example below, a variable named 'myData' will be created to hold the records read from an Excel file.

The RowSet 'myData' can then be used in a task (for example, SQL Task) that needs to read those records.

Note: When using an input variable within a Project task, it should be formatted as ${variablename}.

The following table illustrates data that is contained in the RowSet variable named 'myData':

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
Employee ID	First Name	Last Name	Hire Date	Dept. Code	Salary
34594	Heather	Banks	1998-01-19	BB001	72000
34593	Tina	Young	2010-04-01	BB001	65000
34590	Kathy	Harris	2007-09-30	KH001	105000
34592	Mark	Walker	2012-11-15	KH001	87500
34591	John	Davis	2001-06-15	KH001	85000

Informatica Managed File Transfer stores metadata information within the RowSet variable when it is created from a data translation task such as a SQL or Read CSV. The metadata includes:

Column Indexes

Columns in a RowSet variable can be accessed by notating the Index number of the column on the variable name within brackets "[]". All Indexes in RowSet variables begin at Index 1. For example: The variable ${myData[1]} refers to the data from the column at Index 1.

Column Header Names

Columns in a RowSet variable can also be accessed by notating the column's Header name on the variable, also within brackets "[]". For example: The variable ${myData[Salary]} refers to the data from the column at Index 6.

Data Type

When a RowSet is created, each column defaults to the data type VARCHAR. The data type of a column can be later specified using a Column Element of a Data Translation Task. For example: The Salary data type can be updated from VARCHAR (72000) to DECIMAL (72000.00).

Email Lists

An Email List contains a list of Email Message variables returned by the "Retrieve Email Task" on page 346. Email Lists can be used inside of a loop to process each message individually. For example, by using the "For-Each Loop" on page 152 capability, you can process each message conditionally based on attributes like from address, subject, file names, and more.

Email Message Variable

The Email Message variable contains the attributes of an email. Referring to the subject attribute in a Project will return the subject line of the email message. Referring to the attachments attribute in a Project will return a list of Email Attachment variables. For more information on each attribute, refer to the following table:

Attribute Name	Description
id	The ID of the message.
subject	The subject of the email message. If the subject is not present, an empty string is returned.
sentDate	The date and time the message was sent, in ISO format.
receivedDate	The date and time the message was sent, in ISO format.
sentDateMillis	The date and time the message was sent, in milliseconds since the Unix timestamp (January 1, 1970).
receivedDateMillis	The date and time the message was received, in milliseconds since the Unix timestamp (January 1, 1970).
from	A list of Email Address variables containing the "from" email addresses. In most cases, there will be only one Email Address in this list, which is the sender.
to	A list of Email Address variables containing the "to" email addresses.
cc	A list of Email Address variables containing the "cc" email addresses.
replyTo	A list of Email Address variables containing the "reply-to" email addresses.
allRecipients	The list of Email Address variables containing all recipients of this email ("to" and "cc")
attachments	A list of Email Attachment variables representing each attachment in this Email Message.
messageBodies	A list of Email Body variables representing the body parts in the email message.

Email Address Variable

The Email Address variable contains an email address and an optional name. If you specify the Email Address variable in a Project, both the name and the email address will be returned. To access the address or name separately, use the following attributes:

Attribute	Name Description
address	The email address
name	The name of the person/entity. Will be empty string if the name is not present.

Email Attachment Variable

Variables of this type represent the attachments that were saved to the local file system when processing incoming emails using the Retrieve Email task. If you specify the Email Attachment variable in a Project the absolute path to the local file in which the attachment was saved will be returned. The Email Attachment variable inherits all attributes of the "Local Files" on page 116 variable type and provides the following additional attributes:

Attribute	Name Description
originalName	The name of the attachment sent in the email. If two messages have an attachment with the same name, the second file will be renamed.
contentType	The content type of the attachment. For example, if the attachment was a PDF the contentType would be application/pdf.

Email Body Variable

Variables of this type represent an Email Body that was saved to the local file system when processing incoming emails using the Retrieve Email task. If you specify the Email Body variable in a Project, the absolute path to the local file in which the Email Body was saved will be returned. The Email Body variable inherits all attributes of the "Local Files" on page 116 variable type and provides the following additional attributes:

Attribute	Name Description
contentType	The content type of the body part. For example, if the Email Body was plain text, the contentType would be text/plain.

Denying Auto Notifications

Create a variable to stop notifications that consumers receive as soon as the file is downloaded or extracted.

For more information about creating variables, see "Creating a Variable" on page 113.

1. Right-click the name of the project and select **Add a Variable**.

   The variable page displays.
2. Enter the name of the variable as `deny.event.auto.notifications`.
3. Set the value of the variable to `True`.

4. Enter a description of the variable.
5. Save the project.

AS2 Task Output

The following attributes are populated during the execution of an *AS2* task. These attributes contain a wide range of useful information like the status code of the receipt, the number of files sent and more. Subsequent tasks can access this information using the ${variableName:attributeName} syntax.

For example, to get a "File Lists and File Sets" on page 116 variable with the files sent to the AS2 server you would specify ${variableName:processedSourceFiles} where variableName is the identifier you specified in the Output Variable attribute on the "AS2 Task" on page 488. By referencing the main variable, ${variableName}, all attributes will be printed and can be useful when sending an email notification or printing the summary of all attributes to the job log.

Attribute Name	Description
messageId	The unique ID for the AS2 message.
httpStatusCode	The returned HTTP status code, which is a whole number.
httpStatusMessage	The message text associated to the HTTP status code.
numFilesSent	The number of files sent in the message, which is a whole number.
processedSourceFiles	A "File Lists and File Sets" on page 116 containing a list of files processed.
receiptMessage	The text of the receipt returned by the AS2 server. If a receipt was not requested, an empty string will be returned.
receiptStatusCode	The disposition type and disposition modifier found in the receipt, if one exists. The receipt status will contain values like 'processed', 'failed', 'processed/error' and more.
receiptStatusMessage	The disposition modifier extension provided in the receipt, if one exists. This value may contain additional information about the status of the receipt. For example, 'insufficient-message-security'.
receiptFile	A "Local Files" on page 116 variable referring to the receipt that was written when the Receipt Destination is set to "file".
sentMic	The calculated message integrity code (MIC) of the sent message.
returnedMic	The message integrity code (MIC) returned in the receipt. If the receipt content MIC is not present, an empty string is returned.
receiptSignatureAlias	The alias of the certificate in the Trusted Certificate Key Store that was used to verify the authenticity of the receipt signature. If a signature isn't present or the signature is not trusted, an empty string is returned.

MQ Message List

An MQ Message List contains a list of MQ Message variables returned by the MQ Retrieve Task. MQ Message Lists can be used inside of a loop to process each message individually. For example, by using the "For-Each Loop" on page 152 capability, you can process each message conditionally based on attributes like the correlation ID, priority, properties and more.

MQ Message Variable

The MQ Message variable contains the attribute of an MQ message. Referring to the correlationId in a Project will return the JMSCorrelationID of the message. Referring to the file attribute in a project will return the path of the file where the message contents were stored. For more information on each attribute refer to the following table:

Attribute	Description
id	The ID of the message.
file	The path of the file where the message contents were stored.
correlationId	The correlation ID of the message, if any.
destination	The full destination path. For example, queue:///queueName
queueName	The queue name if the destination was a queue.
topicName	The topic name if the destination was a topic.
deliveryMode	The delivery mode.
expiration	The date/timestamp when the message will expire.
priority	The priority of the message. Possible values are 0 through 9, with 0 being the lowest priority, and 9 being the highest.
redelivered	Whether the message was redelivered.
replyTo	The queue or topic to reply to, if any.
timestamp	The date/timestamp when the message was sent.
type	The type of message.
properties[propertyName]	The JMS and user-defined message properties can be retrieved by using the properties[propertyName] syntax. Replacing propertyName with the appropriate JMS or user-defined property will return the respective value.

Expressions

Expressions in Managed File Transfer can be used to manipulate and calculate values, as well as to condition components in Projects. Expressions must be enclosed inside ${ } and can be composed of strings, variables, functions, mathematical equations and logical operators.

Expressions can be entered manually or constructed using the "Expression Wizard" on page 130 by clicking the ${var} icon next to an attribute in a Project.

When using an expression as a condition (for example, on an IF statement), the result of the expression must return a true or false. For example, ${fileCount > 0} would return true if the variable fileCount is greater than 0.

Note: Project definitions at version 2.0 use the following Expression Syntax. Projects at version 1.0 will continue to run, but are limited to using the "Expression Syntax 1.0" on page 142.

Expression Syntax

Below is a list of items that are allowed in expressions.

Item	Usage	Example
Variables	A variable refers to a value which may be a number, string or object. Multiple variables can be contained within one expression or function.	${x} - Returns the value of variable "x" ${x + y} - Returns the result of variable "x" added to variable "y". Both variables must contain a numeric value. ${x + 2} - Returns the result of variable "x" added to 2 ${concat(x,y)} - Returns the combined string values from variables x and y
RowSet Values	RowSet values can be accessed by placing the column name or column number inside of [ ] (square brackets). Column names must be placed inside double or single quotes. Additional functions, equations and other expressions can be placed in the square brackets.	${data[1]} - Returns the value of the first column ${data[x]} - Returns the value of the column with a name contained in the variable "x" ${data['columnName']} - Returns the value of the column with a name of "columnName" ${data[length(x)]} - Returns the value of the column with an index that is the length of variable "x"
Keywords	The following keywords are reserved for use by expressions and cannot be used as variable names in Managed File Transfer: - true - false - and - or - ne - eq - gt - lt - le - ge - not - null - if - else - elseif - break - continue - do - while - dowhile - for - foreach - try - catch	${contains('x','x',false)} - False does not need quotes and will not be interpreted as a variable since it is a reserved keyword representing a boolean value. ${x == true} - Returns if the variable "x" is equal to true. The keyword true does not need quotes and will not be interpreted as a variable. ${data[1] == null} - Returns true if the first column in the RowSet is null.

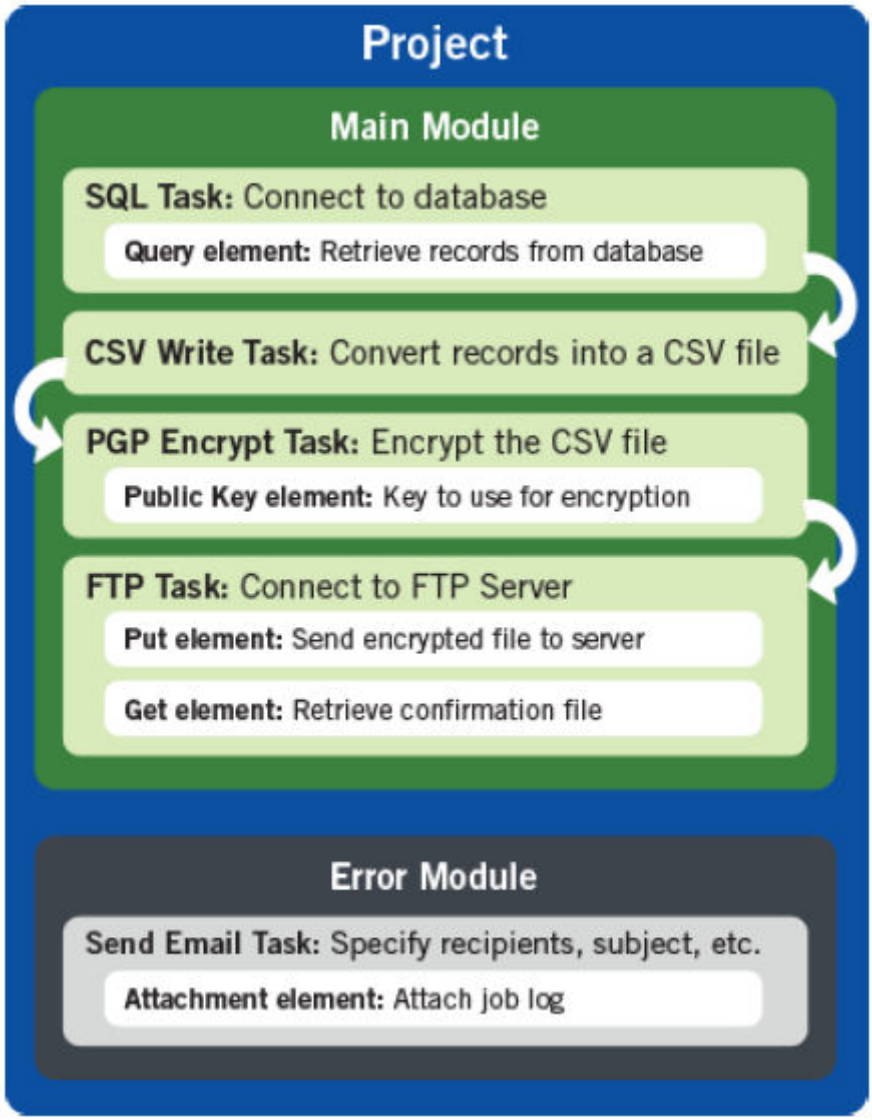
Item	Usage	Example
Method Calls	Method Calls are way to retrieve additional METADATA for a variable. To call a method, insert a colon and the method name immediately after the variable name. Each variable type (File List, Local File, Email List, etc) provides a different set of methods that are available. Refer to the "Variables" on page 111 topic for a complete list of methods that are available for each variable type.	${FileInfo("C:\file.txt"):size} - The FileInfo function returns the size of the specified file.
Grouping	Parentheses can be placed in expressions to determine the order of precedence.	${x+(2-1)} - Calculates the equation in parentheses first before adding it to the variable "x" ${(x >= 0 || y >= 0) && z == 'enabled'} - Returns true if "x" or "y" are greater than zero and "z" is equal to "enabled"
Functions	A "Functions" on page 131 is declared by placing parentheses after the function name. If parameters are needed, they should be placed inside the parentheses and must be separated by commas. Each parameter can contain additional functions, equations, strings, variables and any other expression value.	${Substring('text', 3)} - Returns the value "xt" from the Substring function ${Concat('x','y','z')} - Returns the value "xyz" from the Concat function ${Length(Concat('x', 'y', 'z'))} - Returns the value 3 as the Concat function passed in "xyz" to the Length function
Strings	Any text that is enclosed in single or double quotes is treated as a string value. If a string is enclosed with double quotes and a double quote is needed in the string value, it must be escaped by another double quote. If the string is enclosed in single quotes and a single quote is needed in the string value, it must be escaped by another single quote.	${x == 'enabled'} - Returns true if the variable "x" equals the string value 'enabled' ${x == "enabled"} - Returns true if the variable "x" equals the string value "enabled" ${length("x""x")} - Returns the value 3 since the double quote in the middle is escaped and resolves to one double quote. ${length('x''x')} - Returns the value 3 since the single quote in the middle is escaped and resolves to one single quote. ${length('x""x')} - Returns the value 4 as the double quotes in the middle are not escaped since the string is enclosed with single quotes. ${length("x''x")} - Returns the value 4 as the single quotes in the middle are not escaped since the string is enclosed with double quotes.
Numbers	An expression may contain whole numbers, decimals or numbers written in scientific notation. Numbers can optionally be formatted with "Number Patterns" on page 797 by using the FormatNumber(number, pattern) function.	${10.00} - Represents the value 10.00 ${2e2} - Represents the value 200 ${3.820954E6} - Represents the value 3820954 ${FormatNumber(3820, '#,###')} - Returns the value 3,820 as a string

Item	Usage	Example
Math Operators	Valid math operators are: **+** Addition **-** Subtraction ***** Multiplication **/** Division - When dividing numbers that result in a decimal value, the maximum number of digits to the right of the decimal point is 16. **%** Returns the remainder after the first operand is divided by the second operand. **^** Raises the first operand to the power of the second operand. Expressions containing more than one mathematical step will calculate exponents, multiplication and division before addition and subtraction.	${1+5-3*4/2} - Returns the value 0 ${2^3} - Returns the value of 2 taken to the power of 3 ${10%3} - Returns the value 1

Item	Usage	Example
Logical Operators	Multiple conditions can be separated with the logical operators AND (&&) and OR (||). The AND operator requires both sides to evaluate to true. If the first operand evaluates to false the second operand is not evaluated. The OR operator requires that either side evaluates to true. If the first operand evaluates to true the second operand is not evaluated.	${(x == y) || (1+1 eq 2)} - Returns true as the second parameter is true ${true || EndsWith(x,'csv')} - The EndsWith function is not called because the first operand is evaluated to true and meets the condition. ${(x+y==y+x) && (1+1 eq 2)} - Returns true as both sides evaluate to true
Comparison Operators	Both string and symbolic operators are supported. **== or eq** Equals **<> or ne** Not Equal **< or lt** Less Than **>or gt** Greater Than **<= or le** Less Than or Equal to **>= or ge** Greater Than or Equal to	${x == x} - Returns "true" as the left operand equals the operand on the right ${1+1 eq 2} - Returns "true" as the result of the left operand equals the value of the right operand

Expression Wizard

The Expression Wizard is available for Projects that are version 2.0. The wizard is accessible by clicking the `${var}` icon next to an attribute in the Project. The Expression Wizard displays all the available items for building an "Expressions" on page 125 to place in a field.



Using the Expression Wizard

Hover over any item in the wizard to view a description of it. Click an item to insert it into the Field Value at the current cursor position. Highlighting text in the Field Value and then clicking ${...}, "..." or (...) in the Other column will place the desired brackets or quotes around the selected item.

Buttons Available

Done

Copies the expression into the Project.

Reset

Resets the expression in the Field Value box to the original field value.

Clear

Clears the expression in the Field Value box and returns it to the default.

Cancel

Closes the Expression Wizard without placing an expression in the Project.

Functions

Functions can be used within "Expressions" on page 125 and "Email Templates" on page 810 to perform various operations on variables, strings and data.

Absolute

Returns an absolute value of the specified numeric parameter, which is the number without positive or negative indication.

Definition

${Absolute(number)}

number - Any number or variable containing a number.

Examples

${Absolute(-10.5)} - Returns the value 10.5

${Absolute(3-8)} - Returns the value 5

Concat

Concatenates all parameters and returns a single string. At minimum two parameters are required, but multiple parameters are accepted.

Definition

$Concat(text, text[, text...])

text - The text or variable that will be concatenated with the other parameters.

text - The text or variable that will be concatenated with the other parameters.

[, text...] - The optional text or variables that will be concatenated with the other parameters.

Examples

${Concat('te', 'xt')} - Returns "text"

${Concat('Production', ' ' , 'Server')} - Returns "Production Server"

Contains

Searches the text in the first parameter for the value in the second parameter. An optional third parameter can indicate if the search is case sensitive.

Definition

${Contains(haystack, needle[, case Sensitive])}

haystack - The text or variable that will be searched.

needle - The search string.

caseSensitive - Determines whether the search is case sensitive. Valid values are true and false. The default is true.

Examples

${Contains('example', 'mp')} - Returns "true" since 'mp' is contained in 'example'

${Contains(x, 'xlsx', false)} - Returns "true" since the variable x contains FILE.XLSX and case sensitivity was turned off

CurrentDate

Returns the current date. If a pattern is not specified, the date is formatted according to the ISO standard for date and time patterns.

Definition

${CurrentDate([pattern])}

pattern - A string or variable containing a date pattern.

Examples

${CurrentDate()} - Returns the value "yyyy-MM-dd" (for example, 2011-12-31)

${CurrentDate('MM/dd/yy')} - Returns the example value 12/31/11

CurrentTime

Returns the current time. If a time pattern is not specified, the time is formatted using the ISO 24-hour standard.

Definition

${CurrentTime([pattern])}

pattern - A string or variable containing a time pattern.

Examples

${CurrentTime()} - Returns the value "HH:mm:ss" (for example, 13:30:24)

${CurrentTime('hh:mm a')} - Returns the example value 1:30 PM

CurrentTimeMillis

Returns the current time in milliseconds.

Definition

${CurrentTimeMillis()}

Example

${CurrentTimeMillis()} - Returns a numerical value

CurrentTimestamp

Returns the current timestamp. If a pattern is not specified, the time is formatted using the ISO standard for date and time patterns.

Definition

${CurrentTimestamp([pattern])}

pattern - A string or variable containing a timestamp pattern.

Examples

${CurrentTimestamp()} - Returns "yyyy-MM-dd HH:mm:ss.SSS" (for example, 2011-12-31 13:30:24.785)

${CurrentTimestamp('MM/dd/yyyy HH:mm')} - Returns the example value 12/31/2011 13:30

Decimal

Returns the numeric value contained within the parameter. Useful for converting strings to numbers.

Definition

${Decimal(text)}

text - Any string, variable or function that returns a string value.

Example

${Decimal('10.00')} - Returns 10.00.

EncryptPassword

Encrypts the value by using the Managed File Transfer encryption logic for passwords (same as clicking the Encrypt button). This is useful for encrypting passwords that are stored externally for future use in Managed File Transfer Projects.

Note: The Encrypt Password function cannot be used in Email Templates.

Definition

${Encrypt(text)}

Parameter

text - Any string, variable or function that returns a string value.

Example

${Encrypt('password')} - Returns the encrypted value "JSTs0doxdervqMm0HHUz7Q=="

EndsWith

Checks if the text in the first parameter ends with the value of the second parameter. An optional third parameter can indicate if the search is case sensitive.

Definition

${EndsWith(haystack, needle[, case Sensitive])}

haystack - The text or variable that will be searched.

needle - The search string.

caseSensitive - Determines whether the search is case sensitive. Valid values are true and false. The default is true.

Examples

${EndsWith('example', 'le')} - Returns "true" since 'example' ends with 'le'

${EndsWith(x, 'xlsx', false)} - Returns "true" since the variable x contains FILE.XLSX, and case sensitivity was turned off

FileInfo

Returns information on the "Local Files" on page 116 specified, such as size, last modified date, file directory, etc.

Definition

${FileInfo(filePath)}

filePath - Any string, variable or function that returns a file path.

Examples

${FileInfo("C:\example.txt"):exists} - Returns true or false indicating whether or not the file exists.

${FileInfo("resource:smb://resourceName/file.txt"):size} - Returns the file size of the specified file in a Network Shares resource.

FormatNumber

Returns a string value for the number in the first parameter formatted with the "Number Patterns" on page 797 specified in the second parameter.

Definition

${FormatNumber(number, pattern)}

number - Any number or variable.

pattern - A string or variable containing a number pattern.

Examples

${FormatNumber(10, '#.00')} - Returns the value 10.00

${FormatNumber(9110.997,'$#,##0.00')} - Returns the value $9,111.00

FormatTimestamp

Converts the time in milliseconds to the format defined in the date and time pattern.

Definition

${FormatTimestamp(timeInMillis, pattern)}

timeInMillis - Any millisecond value or variable.

pattern - A string or variable containing a timestamp pattern.

Examples

${FormatTimestamp(1325342402619, "yyyy-MM-dd")} - Returns the value 2011-12-31

${FormatTimestamp(file:lastModifiedMillis, "yyyy-MM-dd")} - Returns the last modified date of a file in year-month-day format

If

Determines the value to use based on the result of the provided condition. All three parameters are required.

Definition

If(condition, resultOfTrue, resultOfFalse)

condition - Any function or variable that returns a boolean value (true or false).

resultOfTrue - Any string, variable, or function that is used if the condition returns "true."

resultOfFalse - Any string, variable, or function that is used if the condition returns "false."

Examples

${if(IsEmpty(text), "Value is empty","Value is not empty")} - Returns "Value is empty" if the variable 'text' is empty, or "Value is not empty" if the variable 'text' contains a value.

${if((numFiles >10), "Greater than 10","Less than 10")} - Returns "Greater than 10" if the value of 'numFiles' is larger than 10, or "Less than 10" if the value of 'numFiles' is less than 10.

IsEmpty

Returns "false" if there are any non-blank characters. Otherwise, returns "true" if the parameter is empty after trimming all leading and trailing whitespaces.

Definition

${IsEmpty(text)}

text - Any string, variable or function that returns a string value.

Examples

${IsEmpty(x)} - If the variable "x" contains a value then the function returns "false"

${IsEmpty(' ')} - Returns the value "true"

IsNotEmpty

Returns "true" if there are any non-blank characters. Otherwise, returns "false" if the parameter is empty after trimming all leading and trailing whitespaces.

Definition

${IsNotEmpty(text)}

text - Any string, variable or function that returns a string value.

Examples

${IsNotEmpty(x)} - If the variable "x" contains a value then the function returns "true"

${IsNotEmpty(' ')} - Returns the value "false"

IsNotNull

Returns "true" if the value of the parameter is not null. Otherwise, it will return "false".

Definition

${IsNotNull(value)}

value - Any string, variable or function.

Examples

${IsNotNull(null)} - Returns the value "false"

${IsNotNull('0')} - Returns the value "true"

${IsNotNull(data[1])} - Returns "true" or "false" based on the value in a RowSet column

IsNull

Returns "true" if the value of the parameter is null. Otherwise, it will return "false".

Definition

${IsNull(value)}

value - Any string, variable or function.

Examples

${IsNull(null)} - Returns the value "true"

${IsNull('0')} - Returns the value "false"

${IsNull(data[1])} - Returns "true" or "false" based on the value in a RowSet column

LastPositionOf

Returns the last position where the value of the second parameter is found in the first parameter. If there is no match, a value of -1 is returned. An optional third parameter can indicate if the search is case sensitive.

Definition

${LastPositionOf(haystack, needle[, case Sensitive])}

haystack - The text or variable that will be searched.

needle - The text search string.

caseSensitive - Determines whether the search is case sensitive. Valid values are true and false. The default is true.

Examples

${LastPositionOf('SELECT', 'S')} - Returns a value of 1 since the first character is the letter "S".

${LastPositionOf('SELECT', 'e')} - Returns a value of -1 since there is no case sensitive match.

${LastPositionOf('SELECT', 'E')} - Returns a value of 4 since the last position the letter "E" appears is the fourth position.

${LastPositionOf('SELECT', x, false)} - Returns a value of 5 since the variable contains to 'c' and case sensitivity is turned off.

Length

Returns the length of the characters contained in the parameter.

Definition

${Length(text)}

text - Any string, variable or function that returns a string value.

Examples

${Length('SELECT')} - Returns the value 6.

${Length(x)} - Returns the character length of the variable "x"

Lower

Returns the parameter in lowercase format.

Definition

${Lower(text)}

text - Any string, variable or function that returns a string value.

Example

${Lower('EXAMPLE')} - Returns the value "example"

LTrim

Trims all leading whitespaces.

Definition

${LTrim(text)}

text - Any string, variable or function that returns a string value.

Example

${LTrim('   example')} - Returns the value "example"

NotContains

Searches the text in the first parameter checking to see if it does not contain the value in the second parameter. An optional third parameter can indicate if the search is case sensitive (defaults to true).

Definition

${NotContains(haystack, needle[, case Sensitive])}

haystack - The text or variable that will be searched.

needle - The search string.

caseSensitive - Determines whether the search is case sensitive. Valid values are true and false. The default is true.

Examples

${NotContains('example', 'mp')} - Returns "false" since 'mp' is contained in 'example'

${NotContains(x, 'xlsx', false)} - Returns "false" since the variable x contains FILE.XLSX and case sensitivity was turned off

PositionOf

Returns the position where the value in the second parameter is found in the first parameter. The optional third parameter can indicate the starting position of the search. An optional fourth parameter can indicate if the search is case sensitive. The result returns -1 if the text is not found.

Definition

${PositionOf(haystack, needle[, startPos][, caseSensitive])}

haystack - The text or variable that will be searched.

needle - The search string.

startPos - The position to start the search. If not specified, the search will start in position 1.

caseSensitive - Determines whether the search is case sensitive. Valid values are true and false. The default is true.

Examples

${PositionOf('example', 'e')} - Returns a value of 1 since the first character is the letter "e"

${PositionOf('example', 'e', 2)} - Returns a value of 7 since the search started at position 2

${PositionOf('example', 'x', 3)} - Returns a value of -1 since "x" was not found after position 3

${PositionOf('example', 'A', 2, false)} - Returns a value of 3 since the letter "a" was within the search scope and the search was not case sensitive.

RandomNumber

Generates a random number between the lower limit specified by the first parameter and the upper limit specified by the second parameter. If only one parameter is specified, then the minimum value is 0. When no parameters are specified, the minimum is 0 and the maximum is 2,147,483,647.

Definition

${RandomNumber([min][, max])}

min - Any positive or negative whole number.

max - Any positive or negative whole number greater than the 'min' value.

Examples

${RandomNumber(1,100)} - Returns a value between 1 and 100

${RandomNumber(-20, -10) - Returns a value between -20 and -10

${RandomNumber(25)} - Returns a value between 0 and 25

${RandomNumber()} - Returns a value between 0 and 2,147,483,647

Replace

Searches the text in the first parameter for the "Wildcards and Regular Expressions" on page 837 in the second parameter and replaces it with the value in the third parameter.

Definition

${Replace(text, regex, replacement)}

text - Any string, variable or function that returns a string value.

regex - Any text or a regular expression.

replacement - Any text, a variable containing text or a regular expression.

Examples

${Replace('example', 'ex', 's')} - Returns the value "sample"

${Replace('abc.txt', '(.*)\.txt', '$1.csv')} - Returns the value "abc.csv"

RTrim

Trims all trailing whitespaces.

Definition

${RTrim(text)}

text - Any string, variable or function that returns a string value.

Example

${RTrim('example ')} - Returns the value "example"

StartsWith

Checks if the text in the first parameter starts with the value of the second parameter. An optional third parameter can indicate if the search is case sensitive.

Definition

${StartsWith(haystack, needle[, caseSensitive])}

haystack - The text or variable that will be searched.

needle - The search string.

caseSensitive - Determines whether the search is case sensitive. Valid values are true and false. The default is true.

Examples

${StartsWith('example', 'ex')} - Returns "true" since 'example' starts with 'ex'

${StartsWith('Text', 't', false)} - Returns "true" since case sensitivity is turned off and 'Text' starts with 't'

String

Returns the value as a string. This is useful for converting numbers to strings.

Definition

${String(value)}

value - Any variable or function that can be returned as a string value.

Example

${String(3 + 3)} - Returns the string value "6"

Substring

Returns the portion of the first parameter starting at the position specified in the second parameter. The optional third parameter specifies how many characters to return. If the third parameter is not specified, the entire value from the start position is returned.

Definition

${Substring(text, startPos[, length])}

text - Any string, variable or function that returns a string value.

startPos - The character position from which to start. If not specified, the starting position is 1.

length - The number of characters to return starting from the 'startPos'.

Examples

${Substring('example', 3, 3)} - Returns the value "amp"

${Substring('example', 3)} - Returns the value "ample"

Trim

Removes any leading or trailing white spaces from the parameter.

Definition

${Trim(text)}

text - Any string, variable or function that returns a string value.

Example

${Trim(' example ')} - Returns the value "example"

Unescape

Returns the parameter after all the escaped characters are processed. All special escape characters like \n (new line), \r (carriage return), \t (tab), hex (\xXX) and Unicode (\uXXXX) values are converted to their corresponding values.

Definition

${Unescape(text)}

text - Any string, variable or function that returns a string value.

Example

${Unescape('\texample')} - Returns the value "	example"

Upper

Returns the parameter in uppercase format.

Definition

${Upper(text)}

text - Any string, variable or function that returns a string value.

Example

${Upper('example')} - Returns the value EXAMPLE

WholeNumber

Returns the whole number of a parameter. This is useful for converting strings to whole numbers.

Definition

${WholeNumber(text)}

text - Any string, variable or function that returns a string value.

Example

${WholeNumber('10')} - Returns the value 10

Expression Syntax 1.0

Note: The following expression syntax is for version 1.0 of Project definitions. You can "Upgrade Project" on page 180 a Project to the 2.0 version to take advantage of "Functions" on page 131 and advanced expressions. Various components in Managed File Transfer Projects optionally accept a condition which is used to determine if the component should be executed or not. These components include:

- Modules

- Tasks
- While Loops
- Do-While Loops
- Exit Loops
- Iterate Loops

Simple Conditions

A simple condition compares two values using the specified comparison operator.

The syntax is: <value1> <condition> <value2>

<Value1> and <Value2> Parameters

- Can be constant values or variable references. Variable references are denoted using the standard variable reference syntax ${variableName}.
- Can be enclosed in single quotes to indicate that they are character (or string) values. By omitting single quotes, a numeric comparison is performed. It is not legal to have one value enclosed in single quotes, but not the other.
  <Condition> Parameters

Condition	Syntax	Description
Equals	eq	Checks for equality of the given values. The condition evaluates to true if and only if both values are exactly the same. When comparing string values, the comparison is performed in a case-sensitive manner. So the condition 'a' eq 'A' evaluates to false.
Not Equals	ne	Checks for un-equality of the given values. The condition evaluates to true if and only if both values are not equal. When comparing string values, the comparison is performed in a case-sensitive manner. So the condition 'a' ne 'A' evaluates to true.
Less Than	lt	Checks to see if <value1> is less than <value2>. If so, it evaluates to true.
Less Than or Equal to	le	Checks to see if <value1> is less than or equal to <value2>. If so, it evaluates to true.
Greater Than	gt	Checks to see if <value1> is greater than <value2>. If so, it evaluates to true.
Greater Than or Equal to	ge	Checks to see if <value1> is greater than or equal to <value2>. If so, it evaluates to true.

Examples

1 eq 1 – always evaluates to true as both values are numeric constants, 1.

1 eq ${fileCount} – Evaluates to true if the value of variable fileCount at the time of evaluation is 1.

${fileCount} lt 10 – Evaluates to true if the value of variable fileCount at the time of evaluation is less than 10.

${n1} ge ${n2} – Evaluates to true if the value of variable n1 is greater than or equal to the value of variable n2.

'MFT' eq 'mft' – Always evaluates to false as both values are character constants and the case is different.

'NE' eq '${state}' – Evaluates to true if the value of the variable ${state} at the time of evaluation is NE.

'${state}' lt 'M' – Evaluates to true if the value of variable ${state} begins with a upper case letter A through N.

'${x}' le '${y}' – Evaluates to true if the character comparison of variable x is less than variable y.

Complex Conditions

Complex Conditions support two or more simple conditions joined together using a logical operator. The following logical operators are supported:

- and
- or
  The syntax is: <condition1> <logical operator> <condition2>

  Example

  (${fileCount} eq 5) or (${fileCount} eq 10) – Evaluates to true if and only if the value of the variable fileCount is either 5 or 10.

Condition Grouping

A complex condition can have condition groups to dictate how the simple conditions in the complex condition should be evaluated.

In this example, the expression contains more than one logical operator. Managed File Transfer marks the condition as invalid and raises a compilation error when the project is compiled.

Example of Incorrect Grouping Expression

${a} eq ${b} and ${c} eq ${d} or ${e} eq ${f} and ${g} eq {h}

In order to properly group conditions and to guarantee a consistent result, manually group the conditions. This is done with the use of open and close parenthesis. The condition below will evaluate to true if a = b and c = d or e = f and g = h.

Example of Correct Grouping Expression

(${a} eq ${b} and ${c} eq ${d}) or (${e} eq ${f} and ${g} eq {h})

Condition groups can also be nested. Meaning a condition group can have one or more groups inside them. The condition below will evaluate to true if a = 2 and either b ≠ 4 or state = NE.

Example

(${a} eq 2 and (${b} ne 4 or '${state}' eq 'NE'))

Dates, Times and Timestamps

Variables can be initialized to the current date, time or timestamp within a Project. These variables can then be used as attributes within tasks in Projects. Listed below are some examples on where these date/time/timestamp variables could be utilized within a Project:

- To suffix the names of any files sent to a FTP server with a timestamp, so each file name is unique on the server.
- To prefix the names of any daily files retrieved from a SFTP server with the current date, so existing files will not be overwritten on your system.

- When inserting records into a database, to populate one of the columns (fields) with the current time. A “Timestamp” task is provided in Managed File Transfer, which must be executed to initialize the date/time/timestamp variables. This Timestamp task needs to be placed in a Project above any tasks that need to utilize those variables.

  Note: The date/time/timestamp variables are only as current as the last time the Timestamp task was executed.

Example

The following steps illustrate how to include the Timestamp task in a Project, and then use the date variable to prefix files retrieved from a FTP server:

1. Create a new Project or edit an existing Project.
2. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Timestamp task to the Project Outline.
3. The Timestamp task opens. You can optionally specify a Label, which would be shown in the Project outline.
1. By default, the Timestamp task will initialize the system variables of system.currentDate, system.currentTime and system.currentTimestamp, which will all be in *ISO format*. However, instead of using the system variables in ISO format, you can create your own variable(s) with a custom format by following the instructions below.

   Click the **Add** button within the Timestamp task.

   Choose the **Format** option from the sub-menu.

   Specify the name of the variable to store the date, time or timestamp.

   Specify the pattern. The pattern rules are documented in the appendix.
2. Click the **Save** button to save the Timestamp task.
3. The TimeStamp task must be placed above any tasks that need to use the date/time/timestamp variables. If needed, you can move the TimeStamp task up in the Project outline by right-clicking the Timestamp task, point to Edit and then click the **Move Up** menu item.
4. After adding the Timestamp task, the date/time/timestamp variable(s) can be utilized in the remaining tasks (in this example FTP Get), within the Project. If you performed step 4 above (to create your own custom formatted variable), then you can use that variable in a task. Otherwise, you will need to use one of the system variables (which are in *ISO format*). In the example below, the system variable of system.currentDate is used to prefix the file name with the current date.

   Note: Be sure to format the variable using the syntax of ${variablename}
5. For this FTP example, the Project outline will appear similar to the image below. Notice that the TimeStamp task (which was labeled as “Current Date and Time” is above the FTP task.

Adding or Subtracting units from a Date, Time or Timestamp

When defining your own variable to contain a date, time or timestamp (as described in step 4 above), you can optionally add or subtract units from that variable. For instance, you could create a date variable that is one year older than today's date. Or you could create a time variable that is 2 hours newer than the current time.

To add or subtract units from a date, time or timestamp variable, click the **Date Manipulation** tab while defining the Format in a Timestamp task. If you want to add a units, enter the value as +X, where X is the

number of units to add. If you want to subtract units, enter the value as -X, where X is the number of units to subtract. Listed below is an example of subtracting 1 year from the current date.

Note: For Projects at version 2.0, you can also use "Functions" on page 131 to get the current date, time and timestamp within fields. These functions do not require the Timestamp task to be run first.

IF Condition

While a Managed File Transfer Project is running, additional tasks or loops can be executed if a condition evaluates to true. The IF Condition can be placed at any point in a Project. Tasks, Loops and additional IF Conditions can be placed inside an IF Condition. An "Else" on page 147 clause can be added after an IF condition to execute a set of tasks when the IF condition evaluates to false.

Example: IF Condition

One file is expected in a location for processing. When more than one file is present a different process should take place.

1. Generate a File List.
   a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
   b. On the Create File List page, specify the Number of Files Found Variable value.
   c. Click the **Add** button to specify the file location for the File Set.
2. The IF Condition can check for the presence of more than one file.
   a. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the If task to the Project Outline.
   b. On the IF page, type the condition statement. Condition statements are based on "Expressions" on page 125.
3. To add a task under the IF condition, expand the appropriate folder in the Component Library, drag a task to the Project Outline, and then place it within the IF condition.

IF Field Definitions

The IF Condition reads an expression and then executes Tasks if the expression evaluates to true.

Field	Definition
Basic Tab	
Label	Specify a label for this if block.
Condition	Specify the conditional expression used to determine if the if block should run. The if block will run as long as the specified condition evaluates to true.
Control Tab	

<table>
<tr><td>Log Level</td><td>Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug.
Default Value: Inherited from parent Module
<table><tr><td>Silent</td><td>Only logs any errors that are encountered.</td></tr><tr><td>Normal</td><td>Additionally logs the start and stop times of the IF Condition, as well as the times of any Loops and Tasks contained in the IF Condition.</td></tr><tr><td>Verbose</td><td>Additionally logs task-level details, such as the names of the files that were processed.</td></tr><tr><td>Debug</td><td>Additionally logs detailed debugging information, such as message responses from servers.</td></tr></table></td></tr>
<tr><td>Disabled</td><td>Whether or not this task is disabled.
Default Value: false</td></tr>
</table>

Else

An Else clause can be added after an "IF Condition" on page 146 to execute a set of tasks when the IF condition evaluates to false.

Example: Else Condition

In the example below, a module will be called if one or more files are found in a folder. Otherwise (else) an email will be sent if no files are found.

1. Generate a File List.
   a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
   b. On the Create File List page, specify the Number of Files Found Variable value.
   c. Click the **Add** button to specify the file location for the File Set.
2. The IF Condition can check for the presence of more than one file.
   a. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the If task to the Project Outline.

b. On the IF page, type the condition statement. Condition statements are based on "Expressions" on page 125.

1. To add a task under the IF condition, drag another task from the Component Library to the Project Outline .
2. To add an Else clause under the IF condition, right-click the IF condition in the Project outline and choose Add Else. After choosing the Else clause, it will appear in the outline after the IF Condition.
3. To add a task under the Else clause, drag another task from the Component Library to the Project Outline .

Else Field Definitions

An Else clause can be added after an "IF Condition" on page 146 to execute a set of tasks when the IF condition evaluates to false.

Field	Definition
Basic Tab	
Label	Specify a label for this else block.

Loops

Loops within Managed File Transfer Projects are used to repeat one or more tasks. A Loop can be placed inside a Module, an IF Condition, or another Loop. The following Loops are supported in Managed File Transfer:

- "For Loop" on page 150 - Executes one or more tasks a predetermined number of times.
- "For-Each Loop" on page 152 - Iterates over a collection of items (File Lists, RowSets, Email Lists, etc.).
- "While Loop" on page 155 - Executes one or more tasks repeatedly while the Loop condition evaluates to true.
- "Do-While Loop" on page 156 - Similar to the While Loop, except the Do While Loop will evaluate the condition after each iteration. This Loop is guaranteed to run at least once.

Sub-elements of Loops

Loops can have the following Project components:

 Chapter 5, "Task Reference" on page 227 - Any task can be added to a Loop.

 Loops - Loops can be nested.

 "Exit Loop" on page 159 - Allows exiting a Loop based on a condition.

 "Iterate Loop" on page 158 - Skips subsequent tasks in the current iteration of the Loop based on a condition.

 "IF Condition" on page 146 - Advanced logic to execute additional tasks or Loops if a condition evaluates to true.

 "Else" on page 147 - Executes additional tasks or Loops when an IF condition evaluates to false.

Error Handling within Loops

If a Loop contains multiple tasks and the first task errors out for any reason, by default the remaining tasks in the Loop will not execute. However, if the first task's On Error attribute was set to 'continue', then the second task in the Loop would execute. If the task's On Error attribute was set to 'setVariable:errorvariable=true', then the next task in the loop could check the value of the error variable to conditionally execute.

Session Persistence within Loops

By default, when a file transfer task (FTP, FTPS, SFTP or SCP) is finished, the connection with the server (session) will be disconnected and closed. When using a file transfer task in a Loop or as part of a multi-step workflow, the session can be kept open and reused rather than closing and reopening the session for each file transfer task to the same server. To keep a session open or to hand off the open session to the next file transfer task in a Project, use the Input Session ID and Output Session ID variables on the Advanced tab of the file transfer task. If this is the first file transfer session in the Project and other tasks will use this connection, only specify the Output Session ID (for example, FTPSession). The next task that uses the session would specify ${FTPSession} in the Input Session ID field. When no additional tasks in the Project need the open session, it should be closed using the "Close Session Task" on page 432 (using the Session ID value of ${FTPSession}).

Delay Task

The Delay task can be used to pause a Project for a specified amount of time. This is especially useful in file scanning loops.

Example 1: Delay Task

You may want to scan for files on a FTP server every 15 minutes. A Loop could be coded in a Project to first perform a FTP task (which scans for the files), followed by a Delay task to wait 15 minutes before trying again.

1. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the Delay task to the Project Outline.
2. On the Basic tab of the Delay task, specify values for the following attributes:
   Time

   The length of time to wait.

   Time Unit

   What measurement of time to use
3. Click the **Save** button.

Field Definitions

Delay Task

The Delay task can be used to pause a Project for a specified amount of time.

Field	Definition
Basic Tab	

Label	Specify a label for this task.
Time	Specify the time to delay the project's execution.
Time Unit	Specify the time unit to use. Default Value: seconds
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

For Loop

A For Loop executes one or more tasks for a specified number of times. A For Loop could contain a FTP task that scans for files in a directory, followed by a Delay task that waits a couple minutes before reiterating the loop. The For Loop could continue to repeat up to a maximum number of iterations you specify.

Example: For Loop

For instance, you may want to check a POP-3 server every 5 minutes for new emails to process. These emails may contain attachments to save to a specified folder.

1. Create the For Loop that will repeat the Retrieve Email task:
    a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For Loop task to the Project Outline.
    b. On the For Loop page, specify the Begin Index value, the End Index value, and the Step. In this example the Loop will run 20 times and increment by one step each time.
2. Create the Retrieve Email Task to retrieve the Email:
    a. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Retreive Email task to the Project Outline.
    b. In the Retrieve Email page, specify the Mail Box and attachment options.

        Note: Other Tasks could be inserted here to further process the saved attachments if needed.

3. Create a Delay Task to add a pause in the Loop:
    a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the Delay task to the Project Outline.
    b. Specify the length of time to wait before checking for new emails.
4. Click the **Save** button.

For Loop Field Definitions

A For Loop executes one or more tasks for a specified number of times.

Field	Definition
Basic Tab	
Label	Specify a label for this loop.
Begin Index	Specify the begin index of the loop. The value can be any positive or negative whole number. The value must be less than or equal to End Index when Step is a positive number and must be greater than or equal to End Index when Step is a negative number.
End Index	Specify the end index of the loop. The value can be any positive or negative whole number. The value must be greater than or equal to Begin Index when Step is a positive number and must be less than or equal to Begin Index when Step is a negative number.
Step	Specify the amount by which the current index of the loop should be incremented or decremented. The value can be any positive or negative whole number except 0 (zero). If not specified, this value defaults to 1.
Advanced Tab	
ID	Specify an ID for this loop. IDs are not required, but are used to conditionally exit or iterate a loop when there are nested loops. The value must be a valid identifier. The ID must be unique in a given loop hierarchy.
Current Iteration Variable	If needed, specify a variable name to hold the current iteration count. The value of this variable is a whole number that starts at 1 and is incremented every time the loop advances.
Current Index Variable	Specify the variable name to which the current index of the iteration be exported. The value must be an identifier. For example, index. The value of this variable will be a positive or negative whole number that represents the current index of the loop and the value is updated every time the loop advances. For example, if the loop is defined with begin=10, end=100 and step=10, then the code inside the loop will be executed 10 times. The first time, the value of this variable will be 10, then 20 and the last time, it will be 100.
Control Tab	

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module **Silent** Only logs any errors that are encountered in the Loop. **Normal** Additionally logs the start and stop times of the Loop, as well as the times of any Loops and Tasks contained in the Loop. **Verbose** Additionally logs task-level details, such as the names of the files that were processed. **Debug** Additionally logs detailed debugging information, such as message responses from servers.
Disabled	Whether or not this task is disabled. Default Value: false

For-Each Loop

For-Each Loops are used to iterate over a collection of items such as a list of files contained in a "File Lists and File Sets" on page 116 or a collection of data in a "RowSet" on page 121. The For Each Loop will perform the same set of Tasks on each item in the collection.

Example Uses:

- Loop through a set of rows (records) retrieved from a database table (which is contained in a RowSet variable). For each row in the loop, call a program to process the data.
- Loop through a set of files that were retrieved from a FTP server, which would be contained in a File List variable. For each file in the loop, decrypt the file and send it to another internal server.
- Loop through a list of file attachments that were retrieved from an email server. For each file attachment in the loop, encrypt the file and forward to another email address.
  When looping through a RowSet (a collection of Rows), a row is exported to the Current Item Variable specified on the For Each Loop. To access the value of a specific column in the row, use the following syntax in a task under the For Each Loop:

  ${rowVar[columnNumber]} or ${rowVar[columnName]}

  When looping through a File List (a collection of files), the file information is exported to the Current Item Variable specified on the For Each Loop. For instance, to access the full path of the file, use the following syntax in a task under the For Each Loop:

  ${file}

  To access specific file attributes, use the following syntax:

  ${file:size}

  For a complete list of attributes, refer to the "Variables" on page 111 reference.

Example: For-Each Loop

A particular FTP Server may not accept multiple files at a time from a client. In order to send multiple files to that FTP Server, you could instead use a For Each Loop on the File List to perform a Manual Put one file at a time. In this scenario, only files ending with "txt" need to be sent to the FTP server.

1. Create a File List of files to send to the FTP Server:
   a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
   b. On the Create File List page, specify the File List Variable.
   Specify the File Set that contains the files to transfer.
   c. Click the **Add** button in the page toolbar and select the File Set menu item.
   d. In the File Set page, type the complete directory path to the Base Directory that contains the files or click the  icon to browse for the directory.
2. Create a Wildcard filter to find files ending with "txt" and include them in the File Set:
   a. Click the **Add** button in the page toolbar and select the Add Wildcard Filter menu item.
   b. On the Wildcard Filter page, click the **Add** button in the page toolbar and then select the Include Files menu item.
   c. In the Wildcard Pattern page, type the filter pattern.
3. Create the For-Each Loop:
   a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For-Each Loop task to the Project Outline.
   b. Specify the Items Variable and the Current Item Variable for the For Each Loop.
4. Create the FTP Task to put the files on the FTP Server:
   a. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
   b. Specify the FTP Server.
5. Under the FTP Task, create the Manual Put element to put each file individually on the server without additional file path information:
   a. On the FTP Task page, click the **Add** button in the sub-menu and select the Put a File Manually menu item.
   b. Specify the Source File variable and the Destination File variable.
6. Click the **Save** button.

For-Each Loop Field Definitions

For-Each Loops are used to iterate over a collection of items such as a list of files contained in a "File Lists and File Sets" on page 116 or a collection of data in a "RowSet" on page 121.

Field	Definition
Basic Tab	
Label	Specify a label for this loop.

Items Variable	Specify a variable that contains the items to iterate over. The value of this attribute must be a variable reference (e.g. ${rowset} or ${filelist}). Currently Collection and RowSet object types are supported, meaning, the value of the referenced variable must be a Collection or a RowSet.
Current Items Variable	Specify a variable name which will be populated with the item at the current index. The variable can then be used in the tasks inside the loop or anywhere in the project. The value must be a valid identifier (e.g. myItem).
Advanced Tab	
ID	Specify an ID for this loop. IDs are not required, but are used to conditionally exit or iterate a loop when there are nested loops. The value must be a valid identifier. The ID must be unique in a given loop hierarchy.
Current Iteration Variable	If needed, specify a variable name to hold the current iteration count. The value of this variable is a whole number that starts at 1 and is incremented every time the loop advances.
Current Index Variable	Specify a variable name which will be populated with the index of the current item. The value must be a valid identifier (e.g. index).
Begin Index	Specify the index of the item at which the processing should start. All items before the specified value will be skipped. The value must be a whole number and should be greater than zero. It must also be less than or equal to the End Index. If not specified, this value defaults to 1, which means processing starts with the first item in the Items Variable.
End Index	Specify the index of the item after which the processing should end. All items after the specified value will be skipped. If not specified, this value defaults to the size of items in the specified Items Variable.
Step	Specify the amount by which the current index should be incremented. For example, when Step is set to 2, every other item in the specified Items Variable is processed. If not specified, this value defaults to 1, meaning every item in the specified Items Variable will be processed.
Control Tab	
Log Level	Specify the level of logging to be used while executing this loop and the tasks in this loop. Valid options are - silent, normal, verbose and debug. All tasks within this loop will inherit the specified log level, which may be overridden on the individual tasks. **Note:** All tasks within this Loop will inherit the specified log level from the Loop, unless the log level is specifically overridden on the individual tasks. Default Value: Inherited from parent Module **Silent** Only logs any errors that are encountered in the Loop. **Normal** Additionally logs the start and stop times of the Loop, as well as the times of any Loops and Tasks contained in the Loop. **Verbose** Additionally logs task-level details, such as the names of the files that were processed. **Debug** Additionally logs detailed debugging information, such as message responses from servers.
Disabled	Whether or not this task is disabled. Default Value: false

While Loop

The While Loop checks a specified condition before executing the tasks contained within the loop. If the condition is met, the tasks within the Loop will execute one iteration. If the condition is not met, the tasks within the Loop are skipped and the Loop will stop processing.

Example: While Loop

A company expects to retrieve four files each day from a trading partner's FTP server. The four files can appear at any time during the day. All four files must be processed at the same time. In the example below, the loop verifies there are exactly four files, then it processes those files and exits.

1. Create a Variable that counts the number of files.
    a. From within the Project Designer page, expand the Project folder in the Component Library, and then drag the Variable task to the Project Outline.
    b. Provide the variable name and default value.
2. Create the While Loop using the "fileCount" variable:
    a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the While Loop task to the Project Outline.
    b. Specify the Condition for the While Loop.
3. Add the FTP Task to monitor the file count:
    a. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
    b. On the FTP Task page, specify the FTP Server.
4. Add the File List variable:
    a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
5. Add the FTP File Set where the files will be located:
    a. Click the **Add** button in the sub-menu and select the Add a File Set menu item.
    b. On the FTP File Set page, specify the Base Directory where the files will be located.
6. Create a Delay Task to wait before rechecking for the file count:
    a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the Delay task to the Project Outline..
    b. On the **Basic** tab, set the duration and the time units.
    c. Click the Control tab to set the condition so the Delay Task only executes if needed. In this example the Delay Task will only execute if there are not 4 files in the specified location. If the condition is met, then the Loop will continue with the remaining Tasks.
7. Add additional Tasks (after the Delay task) to process the files when the file count is satisfied. For instance, you could add a FTP task with a Get to retrieve the files and then add another task to process those retrieved files.
8. Click Save.

While Loop Field Definitions

The While Loop checks a specified condition before executing the tasks contained within the loop.

Field	Definition
Basic Tab	
Label	Specify a label for this loop.
Condition	Specify the conditional expression used to determine if the loop should be terminated. The loop will continue to run as long as the specified condition evaluates to true.
Advanced Tab	
ID	Specify an ID for this loop. IDs are not required, but are used to conditionally exit or iterate a loop when there are nested loops. The value must be a valid identifier. The ID must be unique in a given loop hierarchy.
Current Iteration Variable	If needed, specify a variable name to hold the current iteration count. The value of this variable is a whole number that starts at 1 and is incremented every time the loop advances.
Control Tab	
Log Level	Default Value: Inherited from parent Module. **Silent** Only logs any errors that are encountered in the Loop. **Normal** Additionally logs the start and stop times of the Loop, as well as the times of any Loops and Tasks contained in the Loop. **Verbose** Additionally logs task-level details, such as the names of the files that were processed. **Debug** Additionally logs detailed debugging information, such as message responses from servers.
Disabled	Whether or not this task is disabled. Default Value: false

Do-While Loop

A Do-While loop is similar to a "While Loop" on page 155, however a Do-While loop checks the condition at the end of the loop. Therefore the tasks in a Do-While loop will execute at least once.

Example: Do-While Loop

In the example below, the Do While Loop contains a task that gets a file count on an FTP server. It will continue looping until the file count is equal to 4.

1. Create the Do-While Loop:
   a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the Do-While task to the Project Outline.
   b. Specify the Condition value for the While Loop.
2. Create the FTP process to retrieve the file count:
   a. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
   b. On the FTP Task page, specify the FTP Server.
3. Create the File List variable:
   a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
   b. In the Create File List page, type in the name of the variable to store the file count.
4. Add a File Set to specify the folder (on the FTP server), in which to check for the files:
   a. Click the **Add** button in the sub-menu and select the Add a File Set menu item.
   b. On the FTP File Set page, specify the Base Directory where the files are located.
5. Create a Delay Task to wait before rechecking the availability of the files:
   a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the Delay task to the Project Outline.
   b. On the **Basic** tab, set the duration and the time units.
   c. Click the Control tab to set the condition so the Delay Task only executes if needed. In this example, the Delay Task will only execute if there are not 4 files in the specified location. If the condition is met, then the Loop will continue with the remaining Tasks.
6. Create one or more tasks (after the Delay task) to process the files when the count is satisfied. For instance, you could add a task to get the files from the FTP server and other tasks to import or translate those files.
7. Click Save.

Do-While Loop Field Definitions

A Do-While Loop will execute the tasks located within the loop one time, test the condition at the end of the loop, and iterate through the loop until the condition is met.

Field	Definition
Basic Tab	
Label	Specify a label for this loop.
Condition	Specify the conditional expression used to determine if the loop should be terminated. The loop will continue to run as long as the specified condition evaluates to true. The tasks inside the loop are executed at least once and then the condition is evaluated for subsequent iterations.

Advanced Tab	
ID	Specify an ID for this loop. IDs are not required, but are used to conditionally exit or iterate a loop when there are nested loops. The value must be a valid identifier. The ID must be unique in a given loop hierarchy.
Current Iteration Variable	If needed, specify a variable name to hold the current iteration count. The value of this variable is a whole number that starts at 1 and is incremented every time the loop advances.
Control Tab	
Log Level	Specify the level of logging to be used while executing this loop and the tasks in this loop. Valid options are - silent, normal, verbose and debug. All tasks within this loop will inherit the specified log level, which may be overridden on the individual tasks. Default Value: Inherited from parent Module **Silent** Only logs any errors that are encountered in the Loop. **Normal** Additionally logs the start and stop times of the Loop, as well as the times of any Loops and Tasks contained in the Loop. **Verbose** Additionally logs task-level details, such as the names of the files that were processed. **Debug** Additionally logs detailed debugging information, such as message responses from servers.
Disabled	Whether or not this loop is disabled. Default Value: false

Iterate Loop

The Iterate Loop is a special component for advancing the loop to the next iteration without running the remaining items in the loop. For example, a Loop may contain multiple Tasks, but the condition for the loop might be met before all the Tasks execute. Therefore, the Iterate Loop could be used to return control immediately back to the top of the loop and perform another iteration.

Example: Iterate Loop

A shared folder location is used by several people. You want to process the files at this location, but ignore any files that contain the word 'Payroll' in the file name. In order to ignore files that contain specific text in the file name, you can use a For Each Loop on the File List to iterate through a list of files, and then use the Iterate Loop to skip files that contain the specified text.

1. Create a File List:
    a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.

b. On the Create File List page, specify the File List Variable, and then specify the File Set that contains the files to process.

c. Click the **Add** button in the page toolbar and select the File Set menu item.

d. In the File Set page, type the complete directory path to the Base Directory that contains the files or click the icon to browse for the directory.

2. Create the For Each Loop:

a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For-Each task to the Project Outline.

b. Specify the Items Variable and the Current Item Variable for the For Each Loop.

3. Create the Iterate Loop:

a. On the For-Each Loop page, click the **Add** button in the sub-menu and select the Add Iterate Loop menu item.

b. On the Iterate Loop page, specify a Condition. If the Condition is met, tasks that follow the Iterate Loop will not be executed, and Managed File Transfer will iterate to the next file in the loop.

4. Add additional Tasks (after the Iterate Loop) to continue to process the files that don't meet the Iterate Loop Condition. For instance, files that do not contain the word 'Payroll' in the file name.

5. Click Save.

Iterate Loop Field Definitions

The Iterate Loop allows you to test a condition inside a Loop. If the condition is met, the rest of the tasks in the loop are skipped, and the next iteration of the loop will begin.

Field	Definition
Basic Tab	
Condition	Specify the condition that should evaluate to true for the parent loop or the specified Loop ID to continue on with the next iteration.
Loop ID	Specify the ID of the loop that should be continued with the next iteration. If left blank, the immediate parent loop is continued.

Exit Loop

The Exit Loop is a special component used to exit (or leave) the loop when a certain condition is met.

Example: Exit Loop

The Payroll department sends biweekly statements to their insurance and employee investment trading partners. The department prefers to send statements in batches of at least 10 files. If less than 10 files are found in the File Set, the loop is exited and no file processing occurs.

1. Create a File List:

a. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.

b. On the Create File List page, specify the File List Variable.

c. Specify a Variable for the Number of Files Found.
Specify the File Set that contains the files to process.

d. Click the **Add** button in the page toolbar and select the File Set menu item.

e. In the File Set page, type the complete directory path to the Base Directory that contains the files or click the  icon to browse for the directory.

2. Create the For-Each Loop:

   a. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For-Each task to the Project Outline.

   b. Specify the Items Variable and the Current Item Variable for the For Each Loop.

3. Create the Exit Loop:

   a. On the For-Each Loop page, click the **Add** button in the sub-menu and select the Add Exit Loop menu item.

   b. On the Exit Loop page, specify a Condition. If the Condition is met, the loop is exited and no other tasks within the loop are performed.

4. Add additional Tasks (after the Exit Loop) to continue to process the files if the Exit Loop Condition is not met. For instance, if there are less than 10 files in the File Set.

5. Click Save.

Exit Loop Field Definitions

The Exit Loop allows you to exit a loop if a test condition is met.

Field	Definition
Basic Tab	
Condition	Specify the condition that should evaluate to true for the parent loop or the specified Loop ID to exit.
Loop ID	Specify the ID of the loop that needs to be exited. If left blank, the immediate parent loop will be exited.

Workspaces

Managed File Transfer can create a workspace directory for temporarily storing files while executing a Project. You can define tasks which place files into the workspace, as well as tasks which retrieve files from the workspace.

For instance, you may want to retrieve files from a FTP server and temporarily store them on disk before importing their contents into a database table. A workspace could be used to temporarily store those retrieved files. After importing the file contents into a table, you could then delete the workspace (the retrieved files) using the “Delete Workspace” task.

Outline Example

Listed below is an outline example of a Project that creates a temporary workspace, generates an Excel file (which is placed in the workspace), sends the file over FTP, and then deletes the workspace.

Creating a Workspace

Create a workspace within a Project by following the steps below:

1. Create a new Project or edit an existing Project.
2. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Create Workspace task to the Project Outline.
3. The Create Workspace task page opens. You can optionally specify a Label, which shows in the Project outline.
4. Click the **Save** button to save the “Create Workspace” task.
5. The Create Workspace task must be placed above any tasks that need to use the workspace. If needed, you can move the Create Workspace task up in the Project outline from the right-click menu by pointing to Edit and then clicking the **Move Up** menu item.

Using a Workspace

After a workspace is created, you can read and write files from/to the workspace by NOT specifying a directory name for a file name within a Task. For example, if you specify "Employees.xls" (without specifying a directory name) for the “Output File” attribute in the Write Excel Task, the file will be stored in the Workspace.

Deleting a Workspace

In order to minimize disk space usage, you should delete a workspace when it is no longer needed. To delete a workspace, add the Delete Workspace task to the end of your Project. This task will delete the Project’s workspace directory and any files contained within it.

Note: A workspace is not automatically deleted when the job ends. You need to purposely remove the workspace using the "Delete Workspace" task in a Project.

File Paths

Many tasks in Managed File Transfer can refer to files and folders on the local system, on network shares and in workspaces. The following file path constructs can be used to refer to these locations:

Local Files

A file is considered local by Managed File Transfer when it can be accessed directly by the operating system on the host server without additional drivers or resources.

Platform	Syntax	Example
Windows	driveletter:\[folder]\[filename]	C:\My Documents\readme.txt
Linux	/[folder]/[file]	/usr/readme.txt
IBM i IFS	/[folder]/[file]	/usr/readme.txt

Network Files

The path to a file could be in a network location. Creating a Network Share defines a path on the network where files can be accessed directly by a task in a project. After defining the path location using a Network Share resource, a file can be referenced using the syntax - resource:smb://[ResourceName]/[AdditionalPath]. For example, if the Network Share resource is MyShare, the file is accessed from this share using the syntax - resource:smb://MyShare/subfolder/myfile.txt.

Workspaces

"Workspaces" on page 160 provide a temporary folder location for Projects allowing files to be referenced without specifying the full path to the file. To reference a file in the workspace from within a task, only the file name needs to be supplied with no additional path information (for example, "FileName.txt"). To reference the workspace folder in an output or destination directory field, use the period (.) symbol.

Static and Variable Values

Path references can be made using static text, variable values or a combination of both.

Static: /files/orders.txt

Variable: ${pathToFile}

Combination: /files/${filename}

File Chooser

The File Chooser tool is available on file path related fields to assist in browsing for and selecting files or file paths. Clicking the  icon next to the field will open the File Chooser. The File Chooser can browse the entire local file system (on the server where Managed File Transfer is installed) as well as network shares. When browsing network shares, the File Chooser automatically builds the URL path required to access a network file and places that path in the appropriate field.

Debug Project

When running a Project in Debug mode, users can interactively execute tasks one step at a time. The job log and variable values can be monitored during each step while debugging. At each stopping point, the values for the variables can be changed before the next task is executed.

Executing a Project in Debug Mode

1. Log in as a user that has both the Project Executor and Project Designer roles.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder containing the Project to execute.
4. Click the  icon next to the Project to edit it.
5. Click the  **Debug** option to start the Project in Debug mode.
6. When a user first enters Debug mode, Project variables are initialized and displayed on the Variables tab.

   The values can be edited by clicking  next to the variable name.

Breadcrumbs

A navigation aid that displays the next task to be executed in relation to where the task exists within the Project Outline.

Previous Task

Displays the task that was previously executed.

Next Task

Displays the next task to be executed.

Functions Available

Next

Click the  **Next** button to execute the next task. The results of the executed task are displayed in the Job Log tab, and variable values are displayed on the Variables tab.

Skip

Click the  **Skip** button to skip over the next task. If the skipped task has an output variable specified, the Skipping Task - Required Output Variables page appears.

New Value

Enter a value for the skipped variable(s).

Set Variables

Sets the value of the variable(s) for the skipped task and closes the Skipping Task - Required Output Variables page. This ensures the variable is available for subsequent tasks that require a value to be set.

Ignore Variables

Closes the Skipping Task - Required Output Variables page without assigning a value to the variables in the skipped task.

Cancel

Closes the Skipping Task - Required Output Variables page and returns the user to the current task.

Resume

Click the  **Resume** button to execute all remaining tasks in the Project.

Stop

Click the **Stop** button to cancel the execution of the Project Debugger and writes an ERROR to the Log.

Done

Click the **Done** button to closes the Project Debugger after the Project completes execution.

Sharing Common Logic between Projects (Snippets)

In Managed File Transfer, you can create common logic and definitions (aka Snippets) which can be shared with one or more Projects. This will save time and ensure quality by not having to duplicate the same logic into multiple Projects. Snippets may contain just a few lines of logic or can be much more complex (depending on your requirements) with definitions for modules, loops, tasks and variables.

The logic for a Snippet can be built using the Project Designer or can be hand-coded using Managed File Transfer's XML language. Once you build the Snippet logic, you should save it as an XML file on the server where Managed File Transfer is installed. Snippets can be imported into Projects using the **Import Project Source** option.

The Snippets are not actually copied into Projects where the Import Project Source option is specified. The Snippet XML file is only "referred to" by these Projects, so it is dynamically loaded when the Project executes. This allows you to change the Snippet logic in the future without having to re-import the Snippet into the Project.

Import Project Source - Example

You may want to use the same error handling logic in several different Projects. Rather than configuring the same error handling logic in each of those Projects, you can instead create the logic in a single Snippet XML file and import that file into any Projects which need it.

1. Create the Snippet XML file with the custom error-handling logic and save it into a folder on the server running Managed File Transfer. You are not required to "hand-code" the XML logic. Instead, you could use the Project Designer to build the logic and then copy/paste the portions that you need from the Show XML page.
2. Import the Snippet XML file into any Projects which need that error handling logic:
   a. From within the Project Designer page, right-click the Project or Module where the logic is needed.
   b. On the drop-down list, select the **Import Project Source** option.
   c. In the File Location attribute, type the full path and file name or click the icon to browse for the file.

Project Explorer

For an introduction to *Project* concepts and design, please refer to the "Project Design" on page 100 section. If a user does not have read, write or execute "Folder Permissions" on page 170 for a Project folder, the folder and the Projects inside it are not displayed.

On the Projects page, click a column name to sort the list based on that column. A sort direction arrow shows the sorted column. Click the column name again to toggle the sort direction.

To work with Projects, click **Workflows** from the main menu, and then click **Projects**.

Page Toolbar

The following actions are available from the page toolbar:

- "Add Project (from scratch)" on page 167 a Project by clicking the  Create a Project link in the page toolbar.
- "Search Projects" on page 179 Projects by clicking the  Search Projects link in the page toolbar.
  - Import a Project by selecting the Import Projects link and clicking either the "Import Project from ZIP" on page 178 or "Import Project from XML" on page 178 import method.
  - Access the Folder options by selecting the Folder link and clicking an available option:
  - "Add Folder" on page 168 by clicking the  Add link.
  - "Edit Folder" on page 169 by clicking the  Edit link.
  - "Deleting a Folder" on page 170 by clicking the  Delete link.
  - "Export Folder" on page 177 a Folder by clicking the  Export link
  - Set Folder "Folder Permissions" on page 170 by clicking the  Permissions link.
  - Search for Projects in the current folder by typing a Project name into the Filter By field.

Project Actions

The following actions are available by selecting the  Actions icon:

- "Edit Project" on page 172 a Project by clicking the  icon.
- "Copy Projects" on page 173 the Project to another folder or location by clicking the  icon.
- "Move Projects" on page 174 the Project to another folder or location by clicking the  icon.
  - Delete the selected Project by clicking the icon.
  - View the Project Definition and Error Logging by clicking the  icon.
  - View Creation and Modification details for the Project by clicking the  icon.
  - View "Work with Scheduled Jobs" on page 188 for the Project by clicking the  icon.
- "Export Project" on page 176 a copy of the Project Definition to a local file by clicking the  Export link.
- "Promote Projects" on page 175 a Project from one Managed File Transfer instance to another by clicking the  Promote link.

- "Execution from Administrator (with Advanced Options)" on page 184 the Project with the ability to change Run and Queue Priorities or run with interactive options by clicking the Execute Advanced... icon.
  - Execute a Project Interactively by clicking the icon.
  - Submit the selected Project to "Execution from Administrator" on page 183 by clicking the Submit to Batch icon.
  - View the "Project Execution History" on page 185 for a Project by clicking the icon.

Footer Actions

The following actions are available when one or more items are selected from the table:

- "Copy Projects" on page 173 the selected Projects to another folder.
- "Move Projects" on page 174 the selected Projects to another folder .
- "Promote Projects" on page 175 a Project from one Managed File Transfer instance to another.
- "Export Project" on page 176 a single Project Definition to an XML file by clicking the Project checkbox and then click the **Export** button, or export multiple Project Definitions to a ZIP file by clicking two or more Project checkboxes and then clicking the **Export** button.
  - Submit the selected Projects to "Execution from Administrator" on page 183.
  - Delete the selected Projects.

Add Project (with template)

If you want to use a pre-defined template for creating a new Project, which is normally the fastest method, then follow the steps below:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows**, and then click the Projects link.
3. Drill-down to the folder to create the new Project under.
4. Click the **Create a Project** link in the sub-menu.
5. The Managed File Transfer **Project Designer** page will open.
6. Display a list of available templates by expanding drop down Template field. Select the template to use for your Project.
7. After selecting a template, specify a Project name and optional description.

Template

Click the drop down Template Selection window. Select a template for this project.

Project Name

Specify a name for this project. The Project Name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores (_), periods(.), and white spaces. Maximum length is 50 characters.

Description

Type a Description for the Project. The description cannot exceed 512 characters.

Folder

If needed, type the name of the folder in the Folder box.

1. Click the **Save** button to add the Project.
2. A Project outline is generated, based on the selected template.
3. For each component (task or element) in the Project outline:
   Click the component to change.

   Enter the values for the component's attributes. If a value is left blank in a non-required attribute, then the attribute's default value will be used.

   Click the **Save** button to save the changes for the Project.
4. If needed, you can remove a component from the outline by right-clicking the component and selecting the **Delete** menu item.
5. When done making changes to the Project, click the  **Validate** link in the sub-menu to validate the syntax of the Project.
6. If the validation was successful, then click the **Save & Finish** button to save the Project and return to the folder.
7. "Executing Projects" on page 181 the Project.

   Note: You can learn more about how to edit Projects by referring to the "Project Designer Features" on page 104 section.

Add Project (from scratch)

If you want to choose the specific tasks needed for a Project (without using a template), you can build the Project by following the steps below:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows**, and then click the Projects link.
3. Navigate to the folder in which to create the new Project.
4. Click the  Create a Project link in the sub-menu.
5. The Managed File Transfer Project Designer will open.
6. Type in the new Project name and description.

Template

Click the  icon to open the Template Selection window. Select a template for this project.

Project Name

The Project Name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores (_), periods(.), and white spaces. Maximum length is 50 characters.

Description

The Project Description is optional and cannot exceed 512 characters.

Folder

The folder in which the project will be saved.

1. Click the **Save** button to add the Project.
2. The Project Outline and Component Library will appear.
3. To add a component to the Project Outline, expand the appropriate folder in the Component Library and drag the component to the desired location in the Project Outline. Learn more about the available tasks in the Chapter 5, "Task Reference" on page 227 section.
4. Enter the values for the attributes. If a value is left blank in a non-required attribute, then the attribute's default value will be used.
5. After entering the attributes for the task, click the **Save** button.
6. When complete, click the  Validate link in the sub-menu to validate the syntax of the Project.
7. If the validation was successful, click the **Save & Finish** button to save the Project and return to the folder.
8. "Executing Projects" on page 181 the Project.

   Note: You can learn more about how to edit Projects by referring to the section named "Project Designer Features" on page 104.

Project Folders

Projects can be stored within user-defined folders in Managed File Transfer. Folders are very useful for organizing Projects, which will become important as you create more and more Projects. For instance, you may want to have a folder called "Payroll Functions" to contain any Projects related to payroll and another for Projects that exchange data with your bank.

Permissions can be set on folders so only certain Users can have access to the Projects within those folders. For instance, you may only want certain Users in the finance department to be able to run sensitive Projects in the "Bank Transactions" folder.

Variables can also be set at the "Folder Variables" on page 115 that can be used by the Projects contained within that folder.

Note: A default folder is included with Managed File Transfer named Root (/). Although you can place Projects directly in the default Root folder, it is recommended to create your own folders under Root to organize your Projects.

Add Folder

Follow the instructions below to add a new folder:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder to add the new folder under.
4. Click the Folder drop-down link in the page toolbar, and then select **Add**.
5. Key in the name and optional description for the new folder.

6. Click the **Save** button to add the folder.

Folder Variables

Folder level variables are be used to provide the same constant values to any Projects within the folder. For each folder variable, you can assign the variable name, its constant value and a description. For example, you could define a folder variable named “CompanyCode” with a constant value of 99. Any projects in that folder referring to CompanyCode would receive the value of 99.

When adding a folder, the page displays any “Folder Variables” on page 115 that are inherited from its parent folders. Click the Add Variable link to add a new variable entry and click a cell to type the variable information. A red flag on an entry simply indicates that it is a new entry.

Click the **Save** button to save the folder and folder level variables.

Note: Sub-folders can override a parent folder's variable value by defining a variable with the same name. For example, if the root folder contained a variable named 'AgencyNbr', a subfolder could also contain a variable named 'AgencyNbr' and override the value just for that folder. If a Project has a variable defined with the same name as a folder variable, the variable value in the Project will take precedence.A user must have “Write” permission for the Parent folder before adding a sub-folder.

Edit Folder

Follow the instructions below to change the name or description for a folder:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder that you wish to change.
4. Click the Folder drop-down link in the page toolbar, and then select  **Edit**.
5. Change the name and description for the folder.
6. Click the **Save** button to apply the changes.

Folder Variables

Folder level variables are be used to provide the same constant values to any Projects within the folder. For each folder variable, you can assign the variable name, its constant value and a description. For example, you could define a folder variable named “CompanyCode” with a constant value of 99. Any projects in that folder referring to CompanyCode would receive the value of 99.

When editing a folder, the page displays any “Folder Variables” on page 115 inherited from its parent folders. Click the Add Variable link to add a new variable entry and click a cell to type the variable information. A red flag on an entry simply indicates that it is a new entry.

Click the **Save** button to save the folder and folder level variables.

Note: Sub-folders can override a parent folder's variable value by defining a variable with the same name. For example, if the root folder contained a variable named 'AgencyNbr', a subfolder could also contain a variable named 'AgencyNbr' and override the value just for that folder. If a Project has a variable defined with the same name as a folder variable, the variable value in the Project will take precedence. A user must have “Write” permission for the folder in order to change its properties.

Deleting a Folder

Follow the instructions below to delete a folder:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder that you wish to delete.
4. Make sure there are no Projects in the folder. A folder cannot be deleted if it contains Projects.
5. Click the Folder drop-down link in the page toolbar, and then select **Delete**.
6. Click the **Confirm** button in the confirmation dialog.

   Note: An Admin User must have "Write" permission for the folder in order to delete it.

Folder Permissions

Permissions (authorities) for a folder can be granted to individual Admin Users and Groups of Admin Users. There are three different types of folder permissions that can be granted: Read, Write and Execute.

Permission	Description
Read	Allows Project Designers to view, copy and promote Projects contained within the folder.
Write	Allows Project Designers to change and delete the folder, as well as create, change and delete Projects contained within the folder.
Execute	Allows Admin Users to execute Projects contained within the folder.

For instance, you may have Projects in a folder that only certain Admin Users should be able to execute. Additionally, if you do not want these Admin Users to change the Projects in the folder, then you would only give the Admin Users the folder permission of **Execute**.

By default, a new folder will be granted the same permissions as the parent folder (the folder containing the new folder).

Note: If an Admin User does not have read, write or execute permission for a Project folder, the folder and the "Project Explorer" on page 164 inside it are not displayed. However, if an Admin User has permissions to a subfolder, but not its parent folder, then the user will still be able to drill down through the parent folder to gain access to the subfolder.Add Folder Permissions

Follow the instructions below to add permissions to a folder:

1. Permissions can be added to a folder using the **Add Permissions** page. To access this page:
   a. Log in as an Admin User with the Security Officer role.
   b. From the main menu, select **Workflows** and then click the Projects link.
   c. Drill down to the folder for which you wish to change the permissions.
   d. Click the Folder drop-down link in the page toolbar, and then select **Permissions**.
   e. On the Folder Permissions page, click the **Add Permissions** link in the page toolbar.

2. To authorize Admin Users to the folder:
    a. On the left side of the page, select (highlight) the Admin Users to assign to the folder. Multiple entries can be selected by holding down the Ctrl or Shift key while clicking the mouse.
    b. Click the → arrow.
3. To authorize Admin Groups to the folder:
    a. On the left side of the page, select (highlight) the Admin Groups to assign to the folder. Multiple entries can be selected by holding down the Ctrl or Shift key while clicking the mouse.
    b. Click the → arrow.
4. Select the permissions for the Admin Users and Admin Groups by checking on the **Read**, **Write** and/or **Execute** boxes.
5. Click the **Save** button to apply the changes.
6. Click the **Cancel** button to leave the permissions page.

    Edit Folder Permissions

    Follow the instructions below to change the permissions for a folder:
7. Permissions can be edited for a folder using the **Folder Permissions** page. To access this page:
    a. Log in as an Admin User with the Security Officer role.
    b. From the main menu, select **Workflows** and then click the Projects link.
    c. Drill down to the folder for which you wish to change the permissions.
    d. Click the Folder drop-down link in the page toolbar, and then select  **Permissions**.
8. Select or deselect the permissions for the Admin Users and Admin Groups by checking on or off the boxes next to those Users and Groups.
9. If desired, click the Add Permissionson page 0 link (located towards the top of the page) to grant permissions to additional Admin Users or Admin User Groups.
10. Click the **Save** button to apply the changes.
11. Click the **Done** button to close the permissions page.

Add Folder Permissions

Follow the instructions below to add permissions to a folder:

1. Permissions can be added to a folder using the Add Permissions page. To access this page:
    a. Log in as an Admin User with the Security Officer role.
    b. From the main menu, select Workflows and then click the Projects link.
    c. Drill down to the folder for which you wish to change the permissions.
    d. Click the Folder drop-down link in the page toolbar, and then select  Permissions.
    e. On the Folder Permissions page, click the  Add Permissions link in the page toolbar.
2. To authorize Admin Users to the folder:
    a. On the left side of the page, select (highlight) the Admin Users to assign to the folder. Multiple entries can be selected by holding down the Ctrl or Shift key while clicking the mouse.
    b. Click the → arrow.

3. To authorize Admin Groups to the folder:
    a. On the left side of the page, select (highlight) the Admin Groups to assign to the folder. Multiple entries can be selected by holding down the Ctrl or Shift key while clicking the mouse.
    b. Click the arrow.
4. Select the permissions for the Admin Users and Admin Groups by checking on the Read, Write and/or Execute boxes.
5. Click the Save button to apply the changes.
6. Click the Cancel button to leave the permissions page.

Edit Folder Permissions

Follow the instructions below to change the permissions for a folder:

1. Permissions can be edited for a folder using the Folder Permissions. To access this page:
    a. Log in as an Admin User with the Security Officer role.
    b. From the main menu, select Workflows and then click the Projects link.
    c. Drill down to the folder for which you wish to change the permissions.
    d. Click the Folder drop-down link in the page toolbar, and then select  Permissions.
    e. On the Folder Permissions page, click the  Add Permissions link in the page toolbar.
2. Select the permissions for the Admin Users and Admin Groups by checking on the Read, Write and/or Execute boxes.
3. If desired, click the "Add Folder Permissions" on page 171 link in the page toolbar to grant permissions to additional Users or Groups.
4. Click the Save button to apply the changes.
5. Click the Done button to close the permissions page.

Page Toolbar

The Page Toolbar contains the following elements:

 "Add Folder Permissions" on page 171 to the folder.

 Save and Apply to Sub Folders - Saves the permissions for the current folder and applies those permissions to all of the sub folders under the current folder.

 Save - Apply the changes made to the folder Permissions.

 Remove All Permissions - Removes all User and Group permissions from the folder.

 Done - Return to the previous page.

Edit Project

Change an existing Project definition by following the steps below:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.

3. Drill down to the folder containing the Project.
4. Select the Project you want to change.
5. The Project outline displays on the left side of the page.
6. Click the component within the Project outline to change.
7. The current settings for the component will be displayed.
8. Make any desired changes to the attributes for the Project component.
9. Click the **Save** button to save the changes.

Permissions Required

An Admin User must have the following permissions in order to change a Project:

- Project Designer role.
- Write permission for the folder in which the Project is located.

  Note: You can learn more about how to edit Projects by referring to the section named "Project Designer Features" on page 104.

Copy Projects

Authorized users can make a copy of one or more Projects. This is useful for creating a new Project that is similar to an existing Project or to make a backup of a Project before making changes to it. When making a copy of a Project, you can keep the current name or give the copied Project a new name.

Follow the steps below to Copy one or more Projects:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. In the Folders column, drill-down to the folder containing the Projects to copy.
4. Click the checkboxes of the Projects to copy.
5. Click the **Copy** button that appears in the page footer.
6. In the Copy Project(s) page, select the destination folder and specify what should happen when a Project with the same name already exists in the destination folder.
7. If needed, type a new name for each Project.
8. Click the **Copy** button to copy the Projects.

Destination Folder

This is the folder to which Projects will be copied. Click the  icon to browse for a folder. By default, the destination folder is the same as the source folder.

When Project Exists

The action taken when a Project already exists in the destination folder. The default value is Rename.

- **Rename**

  If Projects exist in the destination folder, it will copy the Projects and append sequential numbers to the Project Names.

- **Overwrite**

  The Projects being copied will overwrite any existing Projects in the destination folder.

- **Skip**

  If the Projects already exist in the destination folder, it will only copy the Projects that are not already present.

- **Error**

  If the Projects already exist in the destination, an error is displayed.

New Name

The new names to give the copied Projects in the destination folder.

Permissions Required

An Admin User must have the following permissions to copy a Project:

- Project Designer role.
- Read permission for the folder containing the source Projects.
- Write permission for the folder where the Projects are being copied.

Move Projects

Authorized users can move one or more Projects to another folder. When moving Projects, you can keep the current names or give them new names.

Follow the steps below to move one or more Projects:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. In the Folders column, drill-down to the folder containing the Projects to move.
4. Click the checkboxes of the Projects to move.
5. Click the **Move** button that appears in the page footer.
6. In the Move Project page, select the destination folder and specify what should happen when a Project with the same name already exists in the destination folder.
7. If needed, type a new name for each Project.
8. Click the **Move** button to move the Projects.

Destination Folder

This is the folder to which Projects will be moved. Click the  icon to browse for a folder.

When Project Exists

The action taken when a Project already exists in the destination folder. The default value is Rename.

- **Rename**

  If Projects exist in the destination folder, it will move the Projects and append sequential numbers to the Project Names.

- **Overwrite**

  The Project being moved will overwrite any existing Project in the destination folder.

- **Skip**

  If the Projects already exist in the destination folder, it only moves the Projects that are not already present.

- **Error**

  If the Projects already exist in the destination, an error is displayed.

New Name

The new names to give the moved Projects in the destination folder.

Permissions Required

An Admin User must have the following permissions to move a Project:

- Project Designer role
- Write permission for the folder containing the source Projects
- Write permission for the folder where the Projects are moving

Promote Projects

Authorized users can promote Project(s) from one Managed File Transfer installation to another. This will copy the definition of the Project(s) to the targeted installation. For example, after a Project is tested, the Project could be promoted from that test installation to a production installation of Managed File Transfer.

Promote Project(s) by following the steps below:

1. Projects can be promoted using the **Promote Project(s)** page. Follow the steps below to access this page:
   a. Log in as an Admin User with the Project Designer role.
   b. From the main menu, select **Workflows** and then click the Projects link.
   c. Drill-down to the folder containing the Project(s) to promote.
   d. Click the checkboxes of the Project(s) to promote.
   e. Click the **Promote** button that appears in the page footer.
2. Enter values for the following fields:

Target Server

The host name (or IP address) of the Managed File Transfer installation on which to copy the Project(s). The value specified must be a URL of the form `http://[host]:[port]/informaticamft`, where [host] is the host name or IP address of the target Managed File Transfer installation, and [port] is the port number on which Managed File Transfer server is running, which by default is 8000. An example value would be http://10.1.4.1:8000/informaticamft

User Name

The user name to login to the target Managed File Transfer installation.

Password

The password for the user to login with. The password is case sensitive.

Target Folder

The folder on the target installation in which to copy the Project(s).

Create Target Folder

Indicate if the target folder should be created if it does not already exist.

Replace Target Project(s)?

Indicate if the Project(s) should be replaced on the target Managed File Transfer installation if they already exist with the same name in the target folder.

3. Click the **Promote** button to copy the Project(s) to the target installation.

Permissions Required

An Admin user must have the following permissions in order to promote a Project:

- Project Designer role on both the source and target Managed File Transfer installations.
- Read permission for the Project folder on the source Managed File Transfer installation.
- Write permission for the Project folder on the target Managed File Transfer installation.

Export Project

Authorized users can export one or more Project definitions into an XML or ZIP file on their local computer. This is useful for sharing Project definitions with another installation of Managed File Transfer.

Export a Project definition into an XML file

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder containing the Project to export.
4. Click the  icon beside the Project to export and from the drop-down menu, click **Export**.
5. The name of the exported file will be constructed using the Project name with an .xml extension.
6. The XML file can be imported into another installation of Managed File Transfer using the "Import Project from XML" on page 178 page.

Export multiple Project definitions into a ZIP file

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder containing the Project(s) to export.
4. Click the checkboxes next to the Projects to export, and then click **Export.**
5. The ZIP file can be imported into another installation of Managed File Transfer using the "Import Project from ZIP" on page 178 page.

Permissions Required

An Admin User must have the following permissions in order to export a Project:

- Project Designer role.
- Read permission for the folder containing the Project to export.

  Note: The "Promote Projects" on page 175 function performs the equivalent of an export and import.

Export Folder

Authorized users can export a Project folder and all of its Project definitions and Variables into a ZIP file on their local computer. This is useful for sharing Project definitions with another installation of Managed File Transfer.

Project folders can be exported using the Export Folder page. Follow the steps below to access this page.

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the desired folder.
4. Click the Folder link, and then select  **Export**.
5. Specify values for the following fields:

   Export File Name

   Specify the ZIP file name.

   Include Folder Level Variables

   Includes variables defined on this folder and any subfolders when exporting this folder.

   Include Folder Description

   Includes the folder description of this folder and any subfolders when exporting the folder.

   Include Subfolders

   Include Subfolders
6. Click the **Export** button to export the folder to a ZIP file.

Permissions Required

An Admin User must have the following permissions in order to export a Project folder:

- Project Designer role.

- Read permission for the folder containing the Projects to export.

Import Project from XML

Authorized users can import a Project definition from an XML file. This is useful for importing a Project definition that was "Export Project" on page 176 from another installation of Managed File Transfer.

Projects can be imported using the **Import Project** from XML page. Follow the steps below to access this page:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder to import the Project into.
4. Click the **Import Project** link and then choose Import from XML.
5. The Import Project from XML page will be displayed.
6. Enter values for the following fields:
   - Import From - Choose Workstation to select a file from your local system or Server to select a file from your Managed File Transfer server.
   - XML File - Navigate to the XML file that will be imported into Managed File Transfer.
   - Ignore Compile Errors - Specify whether to ignore compiler errors when importing a Project. When checked, the Project will be imported even if it contains compile errors.
   - Replace Target Project - Specify whether or not to replace a Project if it already exists in the target folder.
7. Click the **Import** button to import the Project.

Permissions Required

An Admin user must have the following permissions in order to import a Project:

- Project Designer role.
- Write permission for the folder to import the new Project into.

Import Project from ZIP

Authorized users can import Project definitions from a ZIP file. This is useful for importing multiple Project definitions that were "Export Project" on page 176 from another installation of Managed File Transfer or entire "Export Folder" on page 177 that were exported to a ZIP File.

Projects can be imported using the **Import Projects from ZIP** page. Follow the steps below to access this page:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder to import the Project into.
4. Click the **Import Project** link and then choose Import from ZIP.
5. Specify values for the following fields on the Import Project From Zip page:

- Import From - Choose Workstation to select a file from your local system or Server to select a file from your Managed File Transfer server.
- ZIP File - Navigate to the ZIP file that will be imported into Managed File Transfer.
- Ignore Compile Errors - Specify whether to ignore compiler errors when importing a Project. When checked, the Project will be imported even if it contains compile errors.
- Replace Target Project - Specify whether or not to replace a Project if it already exists in the target folder.
- Maintain Directory Structure - Specify whether or not you wish to keep the directory structure of the Projects or to put all Projects in the target folder.
- Overwrite Folder Description - Specify whether to overwrite existing folder descriptions with descriptions from the imported file.
- Overwrite Duplicate Folder Variables - Specify whether to overwrite folder level variables if they already exist.

6. Click the **Import** button to import the Projects from the Zip File.

Permissions Required

An Admin User must have the following permissions in order to import a Project:

- Project Designer role.
- Write permission for the folder to import the new Project into.

Search Projects

The Search Projects page will show which Projects in the specified folder match the search term. The search is performed against the text located in the Project XML files. Projects can be found that refer to a particular file, Resource, Task and more. For example, searching for the term "user@example.com" will return all Projects that refer to this email address.

Follow the instructions below to search the contents of Projects:

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. On the Projects page, click the  Search Projects link in the page toolbar.
4. In the Search Projects page, type a search term and click the  icon to select a Project folder.
5. Select optional features such as recursively searching sub-folders or whether the search term should be case sensitive.
6. Click the **Search** button.

   The following details are shown for each Project on the page:

   - Project - The folder path and Project name
   - References - The number of times the Search Term appears in the Project
   - Project Description - The description of the Project
   - Last Modified On - The last time the Project was modified
   - Last Executed On - The last time the Project was run

Search Projects Actions

The following actions are available by selecting the  Actions icon:

- Click the  icon to edit the "Project" on page 108.
- Click the  icon to view the Project.
- Click the  icon to view creation and modification details about the Project.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Delete Projects

Follow the steps below to delete one or more Project(s):

1. Log in as an Admin User with the Project Designer role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder containing the Project(s) to delete.
4. Select the Project(s) by clicking their checkboxes.
5. Click the **Delete** button that appears in the page footer.

Permissions Required

An Admin User must have the following permissions in order to delete a Project:

- Project Designer role.
- Write permission for the folder in which the Project is located.

  Note: The Projects will be permanently deleted and cannot be recovered. It is recommended to first "Copy Projects" on page 173 the Projects into an "archive" folder before deleting them.

Upgrade Project

The Upgrade Project process converts an existing Project from version 1.0 to the new Project version 2.0. Project version 2.0 provides additional functions for manipulating values, flexible expressions and enhanced job controls. Projects created in this version of Managed File Transfer and later are automatically set at version 2.0.

The Project upgrade process is comprised of a few different steps. First, the Project is validated and then the user can select whether to make a backup of the Project before upgrading. It is highly recommended to make a backup of a Project to restore it later if the upgraded version produces undesirable results. Secondly, the upgrade process is performed and the user can choose to save the upgraded Project or cancel the upgrade.

During the upgrade, the following components will be modified in the Project:

- Any Module with a "Depends On" setting will be updated with one or more "Call Module Task" on page 433 Tasks. For example, if the Project's Main module depends on modules A and B, then the "Depends On" will be removed from the Main module and two Call Module tasks would be inserted to the beginning of the Main module (one to call module A and another to call module B).
- Any expression used for conditioning, such as the "Execute Only If" statement, will be updated to use the new "Expressions" on page 125 syntax. For example, the previous syntax ${var1} ge ${var2} will be converted to the new expression of ${var1 ge var2}.
- "RowSet" on page 121 using the column name, instead of the column index, will be converted in the upgrade process to place quotes around the column name (for example, ${data[columnName]} becomes ${data["columnName"]}).

- Variables, module names and resource names will no longer be case sensitive.

When the upgrade is complete, an Upgrade Log is displayed. The Upgrade Log displays any issues encountered while upgrading the Project and provides options to Download the upgrade log in text format, Save and Finish the Project upgrade process, or Cancel the upgrade.

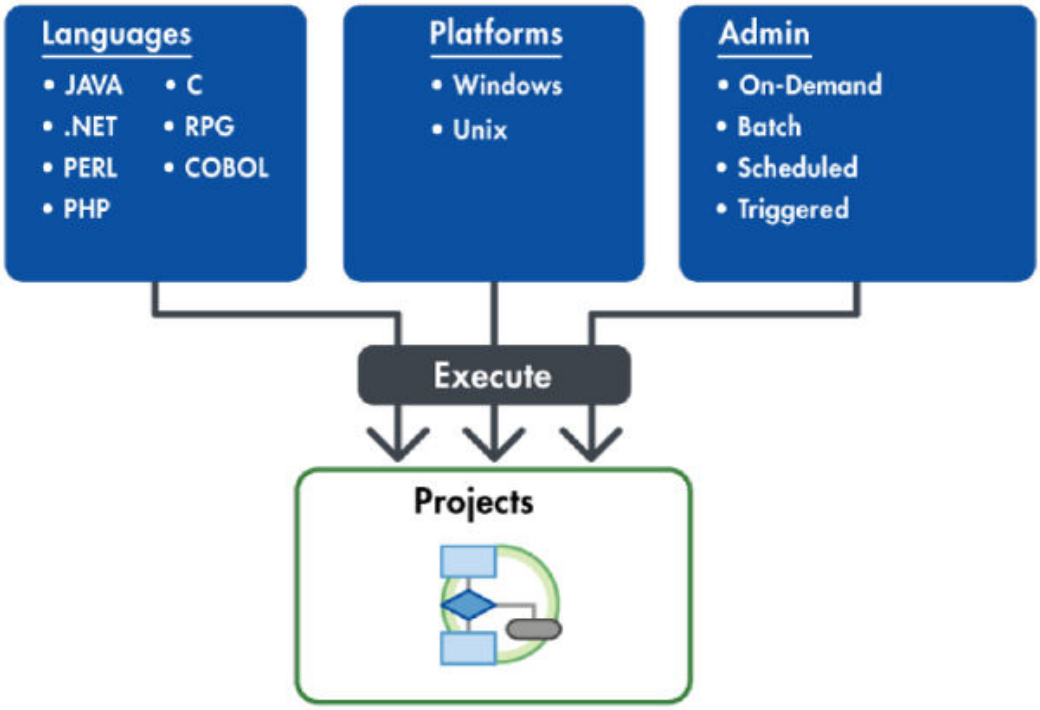
Follow the steps below to upgrade a Project:

1. Log in as an Admin User with the Project Manager role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Click the  Action icon and then click  **Edit** icon.
4. In the Project page, click the  Upgrade Project link in the page toolbar.
5. On the Upgrade page, complete the required fields and then click the **Upgrade** button.
6. The Upgrade Project process starts and when complete, an Upgrade Log is displayed.
7. It is strongly recommended that you test the upgraded Project to ensure it behaves as expected.

Executing Projects

Several methods are available for executing Projects within Managed File Transfer. Users can execute Projects "Execution from Administrator" on page 183 from within Managed File Transfer's browser-based administrator. Projects can also be executed by the integrated "Scheduling Projects" on page 187 and "Monitors" on page 197 processes.

External applications can additionally launch Projects from other systems ("Execution from Windows and Unix" on page 184) by using Managed File Transfer's commands and APIs, or by making HTTP(S) requests to the Managed File Transfer server.



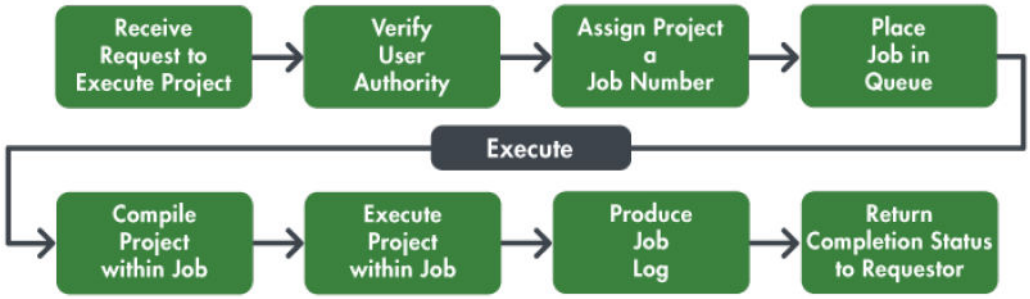
Managed File Transfer provides enterprise features for executing Projects including a "Work with Queued Jobs" on page 220, multi-threading (to allow the concurrent execution of multiple Projects), priority settings, real-time "Active Jobs" on page 221 and detailed "Completed Jobs" on page 223.

Every execution of a Project is considered a **Job**. Listed below are the primary steps performed as jobs flow through Managed File Transfer.

1. After an authorized request is received to execute a Project, a Job will be created and assigned a unique job number.
2. A batch job initially starts in the Managed File Transfer "Work with Queued Jobs" on page 220.
3. When Managed File Transfer is ready to run the job, it will advance the job from the job queue into the "Active Jobs" on page 221 subsystem to execute.
4. The job's Project will then be compiled and executed by Managed File Transfer.
5. When the job finishes, a "Completed Jobs" on page 223 will be generated.
6. The completion status (along with any error messages) will be returned to the user or requesting application.

Job Execution Flowchart

The following image shows the job execution flowchart:



Execution from Administrator

Admin Users can run Projects through the Managed File Transfer Administrator, which is useful for running Projects on an as-needed basis or for testing purposes.

Projects can be executed either in interactive or batch mode (explained below). "Execution from Administrator (with Advanced Options)" on page 184 options can be specified by a user to override "User Defined Variables" on page 112, the *job queue priority* and *run priority*.

Executing a Project Interactively

When an Admin User executes a Project interactively, the Admin User's browser will wait until the Project completes. Perform the following steps to execute a Project interactively:

1. Log in as an Admin User with the Project Executor role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder containing the Project to execute.
4. Click the icon next to the Project to execute.
5. The Project will execute and will return the completion status and error messages, if any.

Executing a Project in Batch

When an Admin User executes (submits) a Project in batch, the Admin User will be able to perform other functions in Managed File Transfer while the Project is executing. Multiple Projects can be submitted to batch at one time. Perform the following steps to execute Project(s) in batch:

1. Log in as an Admin User with the Project Executor role.
2. From the main menu, select **Workflows** and then click the Projects link.
3. Drill down to the folder containing the Project(s) to execute.
4. Select the Project(s) to execute by clicking their checkboxes.
5. Click the **Submit to Batch** button (that appears at the bottom of the page) to execute the Project(s).

Execution from Administrator (with Advanced Options)

Managed File Transfer allows an Admin User to specify advanced options when executing a Project. These options allow the Admin User to override the values of any Project "User Defined Variables" on page 112 (parameters) and specify the *job queue priority* and *run priority*.

Perform the following steps to execute a Project with advanced options:

1. Log in as an Admin User with the Project Executor role.
2. From the main menu, select **Workflows**, and then click the Projects link.
3. Drill down to the folder containing the Project to execute.
4. Click the  Action icon on the project to execute and from the drop-down list and click **Execute Advanced…**.
5. A page will prompt for the advanced options for running the Project.
6. If needed, override the job's run priority.
7. Specify an optional Job Name. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list.
8. Select one of the following Execution Mode options:

   Interactive

   Executes the Project interactively, in which your browser will wait until the Project completes.

   Batch

   Executes the Project in batch mode, allowing you to specify a Queue Priority and "Job Queue Manager" on page 217. While the Project is executing, you can perform other functions in Managed File Transfer .
9. If variables exist in the Project, you can override any values for those variables. Encrypted variables appear with a  icon.

Execution from Windows and Unix

Informatica Managed File Transfer Projects can be executed from the command line of Windows and Unix using Managed File Transfer Command (GACmd). When the command is run, the Command Line Utility performs an HTTP(S) request to the specified Managed File Transfer server and executes the specified function. With the Command Line Utility, it is possible to execute Managed File Transfer functions from custom programs, scripts and scheduler software.

Executing a Command

The Command Line Utility command can execute Projects and call functions on an Managed File Transfer installation that resides on the local system or a remote server on the network. All parameter names are case-insensitive. Values containing spaces must be enclosed in "double-quotes." For example, the following command executes a project in Managed File Transfer:

Example:

infamftcmd.bat -server http://10.1.4.1:8000/informaticamft -user Administrator -password Administrator -command runProject -project/Test

For more information on available commands, see the *Managed File Transfer Command Line Reference*.

APIs are also available for JAVA and .NET for calling Managed File Transfer functions.

Project Execution History

To view the Project Execution History page in Managed File Transfer, log in as an Admin User that has both the Project Designer and Job Manager roles or the Project Executor role.

From the main menu, click **Workflows**, and then click **Projects**. In the list of Projects, click the Action icon beside a Project and then click the Execution History icon to open the Project Execution History page.

The Project Execution History page provides a wide variety of search criteria. You can also specify the **Results Per Page** displayed on the page. After specifying the criteria, click the **Search** button.

The following details will be shown for each Job on the page:

- Job Number - A unique job number given to each project at runtime
- Project Name - Name of the Project
- Project Folder - The folder location of the Project
- Status - The outcome of the job (= Successful, = Failed or = Canceled)
- User - The user who submitted the Job
- Start Time - When the Job started executing
- End Time - When the Job completed
- Time - Execution time (in seconds)

Page Toolbar

The following actions are available from the page toolbar:

- Click the **Done** button to return to the Projects page.

Project Execution Actions

The following actions are available by selecting the Actions icon:

- "Job Log and Details" on page 186 the Job Details by clicking the icon.
- "Job Log and Details" on page 186 the Job Log by clicking the icon.

  - Edit the selected Project by clicking the Edit Project link.

  - View the folder where the Project is located by clicking the View Project Folder link.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages to a .CSV file on your local computer.

  Note: The default saved Job Log file name is "JobLogsYYYYMMDD.csv" (where YYYYMMDD is the current year, month, and day).

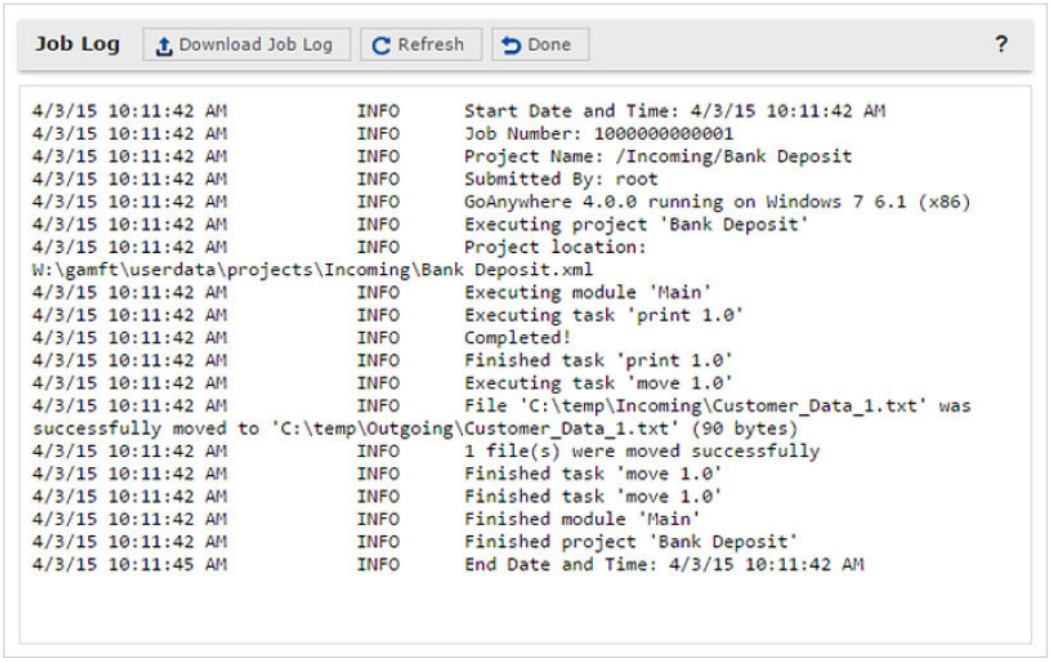
Job Log and Details

Each time a job is executed a log is created that captures the activity related to the job/project. The amount of information captured in the job log is defined by the Log Level set on the Control tab in the "Project" on page 108. The Job Details page provides an overview of a job.

Job Log

View the job log for a job by clicking the icon next to the job you wish to view.

The following image shows the job log:



Job Details

View the details for a job by clicking the icon next to the job you wish to display.

Scheduling Projects

Managed File Transfer includes a built-in scheduler for executing Projects (Jobs) at future dates and times. Jobs can be executed on a one-time or recurring basis.

Holiday Calendars

Holiday Calendars define the dates of the holidays and other non-working days in your organization. "Work with Scheduled Jobs" on page 188 can use a holiday calendar to determine what should happen to the job when the execution falls on a holiday (for example, skip this run, execute the day before or execute the day after). Multiple holiday calendars can be created to provide scheduling flexibility.

To access Holiday Calendars:

1. Log in as an Admin User with the Job Manager role.
2. From the main menu, select **Workflows** and then click the Scheduler link.
3. From the Scheduler page toolbar, click the Holiday Calendars link.

Page Toolbar

The following actions are available from the page toolbar:

- "Add or Edit a Calendar" on page 188 a calendar by clicking the **Add a New Calendar** button.
  - Return to the Schedules page by clicking the **Done** button.

Manage Calendars Actions

The following actions are available by selecting the Actions icon:

- "Add or Edit a Calendar" on page 188 a calendar by clicking the icon.
  - Copy a calendar by clicking the icon.
  - Delete the calendar by clicking the icon.
- "View Calendar" on page 188 the calendar information by clicking the icon.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Add or Edit a Calendar

A calendar can be created or edited using the **Manage Calendar** page. To create a new calendar, click the Add a New Calendar link in the page toolbar. To edit an existing calendar, click the icon next to the calendar.

Name

A name for the calendar.

Description

The description provides additional information about the holiday calendar.

Non-Business Days

Days of the week when the company is closed and when processing should not occur.

Holidays

There are two ways to add dates to the holiday calendar.

1. Click the **Add Date** option to add a new holiday entry.
2. In the Name column, type a name for the holiday.
3. Click the Date field or the icon to open the calendar pop-up to select a date.

   Note: Dates are automatically sorted in ascending order when saved. The Holiday Suggestions page offers a quick way to select the most common holidays in the United States.

   To select any holiday, click its corresponding checkbox. When finished, click the **Add Selected Holidays** button to add the dates to the Calendar. If a holiday falls on a weekend, the observed date is used instead.

   Dates already part of a holiday calendar appear grayed out on the Holiday Suggestions page.

View Calendar

The View Calendar page displays general information about the calendar (when it was created, the user that last modified it, etc.), as well as a list for each holiday entry. When finished viewing the calendar details, click the **Done** button.

Note: Holiday Dates are the observed date.

Work with Scheduled Jobs

To work with Scheduled Jobs, log in as an Admin User with the Job Manager role. Select **Workflows** from the main menu, and then click the Scheduler link.

This page allows you to search for Scheduled Jobs using a variety of criteria such as Run Times, Project or Job Name, User, Status and Schedule (trigger type). After typing the criteria, click the **Search** button to perform the search. If a column below is not shown, click the Show/Hide Columns link for a complete list.

Note: When searching for a Scheduled Job, the search results found on the Basic Search tab will return exact matches for the search term. Use the Advanced Search tab to search additional fields and control the search term logic (for example, Equals, Begins With, Ends With and Contains). Search terms are not case sensitive.

Page Toolbar

The following actions are available from the page toolbar:

- "Adding or Editing a Scheduled Job" on page 190 a Scheduled Job by clicking the **Schedule a New Job** button in the page toolbar.
- "Holiday Calendars" on page 187 a Holiday Calendar by clicking the **Holiday Calendars** button in the page toolbar.
- "Work with Repeating Scheduled Jobs" on page 194 the Repeating Jobs Queue by clicking the View Repeating Jobs Queue link in the page toolbar.
  - Disable all Scheduled Jobs from running by clicking the Disable Scheduler link in the page toolbar. When the Disable Scheduler link is clicked, all active jobs will finish. Jobs that are scheduled to run will be suspended until the Enable Scheduler link in the page toolbar is clicked (even if Managed File Transfer is restarted).

Scheduled Jobs Actions

The following actions are available by selecting the Actions icon:

- "View Scheduled Job" on page 194 a Scheduled Job by clicking the View icon.
- "Adding or Editing a Scheduled Job" on page 190 a Scheduled Job by clicking the icon.
  - Copy a Scheduled Job by clicking the Copy icon. This option will prompt you to "Adding or Editing a Scheduled Job" on page 190 a new Scheduled Job.
  - Delete a Scheduled Job by clicking the Delete icon.
- "Promote Schedules" on page 195 a Schedule to another Managed File Transfer server by clicking the Promote icon.
  - Execute a Scheduled Job immediately by clicking the Run Now icon.
  - View the "Completed Jobs" on page 223 for the Scheduled Job by clicking the Show history icon.
  - Deactivate or Activate a Scheduled job by clicking the Deactivate or Activate icon.
  - Reset the Misfire count by clicking the Reset Misfires link.
- "Show Schedule" on page 197 the future schedule of the Scheduled Job by clicking the Show Schedule link.
  - Edit the selected Project by clicking the Edit Project link.
  - View the folder where the Project is located by clicking the View Project Folder link.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete the selected Scheduled Jobs.
- Promote the selected Schedules.
- Execute the selected Scheduled Jobs by clicking the **Run Now** button.
- Activate or Deactivate the selected Scheduled Jobs.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Columns** button to select which Scheduled Job properties are displayed in the table.

Scheduled Job Columns

- Name - The name of the Scheduled Job.
- Description - The description of the Scheduled Job.
- Project - The location and name of the Project run by the Scheduled Job.
- User - The user account that will run the Scheduled Job.
- Job Name - The Job Name specified from the properties of the Project or Scheduled Job.
- Job Queue - The assigned Job Queue the Scheduled Job runs under.
- Queue Priority - The assigned Queue Priority of the Scheduled Job.
- Run Priority - The amount of processing priority the job receives from the processor.
- Schedule - The frequency for the Scheduled Job. Hover the pointer over the Schedule column to view the Schedule settings.
- Status - Whether the job is active or inactive.
- Last Run Time - The date/time of when the Scheduled Job last ran.
- Next Run Time - The date/time of when the Scheduled Job will run again.
- Run Count - The number of times the Scheduled Job has run.
- Misfires - The number of times that the Scheduled Job did not run (due to any downtime of the Managed File Transfer server).
- Created By - The user who created the Scheduled Job.
- Created On - The date and time the Schedule Job was created.
- Last Modified By - The user who last modified the Scheduled Job.
- Last Modified On - The date and time the Schedule Job was last modified.

Adding or Editing a Scheduled Job

A Scheduled Job can be created or edited using the **Scheduled Job** page. To access this page, log in as an Admin User with the **Job Manager** role. Select **Workflows** from the main menu, and then click the Scheduler link. To create a new Scheduled Job, click the Add a Scheduled Job link in the page toolbar. To edit an existing Scheduled Job, click the icon.

Listed below are the field descriptions within each tab of the Scheduler.

Project Tab

The Project tab contains the following settings:

Name

A user-defined name which identifies the Scheduled Job. The Job Name cannot exceed 50 characters. Spaces are allowed.

Description

A short paragraph that describes the Scheduled Job. The Description is optional and cannot exceed 512 characters.

Project

The name of the Project to execute. You can browse for the Project by clicking the button next to the field.

Login As

The user name (Login as) to use for running the Scheduled Job.

Password

The password to use for authenticating the specified user (Login as).

Job Queue

The Job Queue that this Job will be placed into. If the Job Queue is not specified on the Scheduled Job, the Job Queue on the Control tab of the Project will be used. If both are not specified, the Project will be placed in the default Job Queue.

Status

The status indicates if the Scheduled Job is active or inactive. An inactive Scheduled Job will not be executed.

Queue Priority

The queue priority indicates the order in which the job will leave the "Work with Queued Jobs" on page 220 and execute. The queue priority can be a value from 1 to 10, in which jobs with a higher queue priority will be executed before jobs with a lower queue priority. For instance a job with a queue priority of 6 will be executed before a job with a queue priority of 5.

Run Priority

The run priority indicates how much attention (CPU) the job will receive from Managed File Transfer when it executes. The run priority can be a value from 1 to 10, in which jobs with a higher run priority will receive more attention than jobs with a lower run priority. For instance a job with a run priority of 6 will receive more attention (CPU) than a job with a run priority of 5.

Job Name

Specify a name which identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters. Spaces are allowed.

Schedule Tab

The Schedule tab contains the following settings:

Trigger Type

The type of schedule this job should use. The trigger types are explained below:

- One time - The job will run once at the indicated start date and time.
- Startup - The job will run once whenever the Managed File Transfer application is started.

- Minutely - The job will run every X minutes.
- Hourly - The job will run every X hours.
- Daily - The job will run every X days.
- Weekly - The job will run every X weeks, in which additional settings can be specified.
- Monthly-The job will run once a month, in which the day of month can be specified.

Start date

The date that the Scheduled Job should first run.

Start Time

For trigger types of One Time, Minutely, Hourly and Daily. The time that the Scheduled Job should first run.

Run Every

For trigger types of Minutely, Hourly, Daily and Weekly. The number of units to wait between each execution of the Scheduled Job. The valid range is 1 to 999. The unit type (weeks, days, hours or minutes) depends on the trigger type selected.

End Date

For trigger types of Minutely, Hourly, Daily, Weekly and Monthly. Optional: The date/time that the Scheduled Job should stop running. Leave this option unchecked to schedule a job that does not have an end date.

Days to Run

For trigger type of Weekly. The days of the week (Sun, Mon, Tue, etc.) this Scheduled Job should run.

Run At

F or trigger types of Weekly and Monthly. The time of day this Scheduled Job should run.

Day of Month

For trigger type of Monthly. The day of the month (1st, 2nd, 3rd, etc.) which this Scheduled Job should run.

Day of Week

For trigger type of Monthly. The week of the month (first, second, etc.) and day of the week (Sun, Mon, etc.) this Scheduled Job should run.

Holiday Calendar

For trigger types of Daily, Weekly, Monthly. The drop-down list provides a list of available holiday calendars that were created on the "Holiday Calendars" on page 187 page.

Holiday Rule

For trigger types of Daily, Weekly, Monthly. The action taken by the scheduled job when the next runtime falls on a holiday.

- Skip - The scheduled job cycle is skipped and runs as scheduled after the holiday.
- Previous Business Day - The scheduled job cycle will run a day before the holiday.
- Next Business Day - The scheduled job cycle will run a day after the holiday.

Advanced Options

After the Scheduled Job runs, indicate if it should repeat itself for a period of time. This advanced option is like having a schedule within a schedule. This could be used for repeatedly calling Projects that only

need to run during certain periods of the day. If the scheduled job uses a holiday calendar and executes the day before a holiday, the repeat options can cause the job to continue executing into the holiday.

The valid repeat options are:

- Do not repeat
- Repeat Always

  Note: The next execution time of a repeating job will be based on when the current execution finishes (not when it started). For instance, if a job execution finishes at 9:02am, and if the Run Every parameter is set to 5 minutes, then the next execution time for the job will be 9:07am
- Repeat only when the project fails
- Repeat only when the project succeeds
- Repeat only if the specified condition evaluates to true

  Note: When specifying the condition that would evaluate to true, the value can be composed of another variable. If using a variable, type the name of the variable and not the variable syntax (for example, variableName instead of ${variableName}). If a Repeat option is selected, you can indicate how long the Scheduled Job should repeat and how long the delay should be between repeats.

  Example #1: You could set up a scheduled job that runs every day by specifying the Daily trigger type. Lets say the Start Time is set for 9:00 am and the advanced option is set to Repeat Always for 2 hours with a 5 minute delay between executions. With this example, the Scheduled Job will first run at 9:00am. If the job takes 2 minutes to run, then it will repeat again at 9:07am, then again at 9:14am, and so on, until 11am (when the 2 hours expires). This entire sequence would be repeated each day of the week.

  Example #2: You could set up a scheduled job that runs every Monday using the **Weekly** trigger type. Lets say the **Start Time** is set for 1 pm and the advanced option is set to **Repeat only when the project fails** for 3 hours with a 10 minute delay between executions. With this example, on Monday, the Scheduled Job will first run at 1 pm. If the Project takes 1 minute to run and if it fails, then the Scheduled Job will repeat again at 1:11 pm. If it fails again, then it will repeat again at 1:22pm, and so on until 4 pm (when the 3 hours expire). This entire sequence would be repeated the next Monday.

Email Notification Tab

The Email Notification tab contains the following settings:

When Job Completes Normally

The list of email addresses (comma delimited) to notify when the Scheduled Job completes normally. You can optionally indicate whether or not the job log should be attached to the email. The email that is sent uses the SuccessfulScheduledJob.xml "Project Email Templates" on page 826.

When Job Fails

The list of email addresses (comma delimited) to notify when the Scheduled Job fails. You can optionally indicate whether or not the job log should be attached to the email. The email that is sent uses the FailedScheduledJob.xml "Project Email Templates" on page 826.

Project Variables

If "Variables" on page 111 exist in the Project being called, you can override the values for those variables within the Scheduled Job.

The Project Variables contain the following settings:

Variable Name

The name of the variable in the Project.

Description

The description for the variable.

Original Value

The value of the variable as it is currently defined in the Project.

New Value

The value to pass from the Scheduled Job to the Project for the variable.

Work with Repeating Scheduled Jobs

The Repeating Scheduled Jobs queue is only applicable for jobs that have repeating options specified under the Schedule tab's Advanced Options. To learn more about these advanced options please refer to the Schedule tab in "Adding or Editing a Scheduled Job" on page 190.

After a scheduled job first executes, the repeating options are evaluated to determine whether the job should schedule itself to repeat. If the job should repeat it will be placed into the Repeating Scheduled Jobs queue.

Note: If the job is currently repeating, disabling the scheduled job will not end its repeating jobs. You can stop a repeating job from rescheduling itself by canceling the job that is next in the queue.

For each job in the Scheduler Job Queue, this page will show the assigned job number, the system that will execute the job, the name of the Project, the User that submitted the job, when the job is scheduled to run, the Job Queue, the queue priority and the run priority.

The System column displays which system in the cluster will run the scheduled job. This column is only displayed when Managed File Transfer is running in a clustered environment.

The Job Queue indicates the Job Queue in which the jobs will be executed in.

The Job Name indicates the Job Name specified in the properties of the Project or Scheduled Job.

The **Queue Priority** (shown for each job on the page) indicates the order in which the jobs will leave the queue and execute. The queue priority will be a value from 1 to 10, in which jobs with a higher queue priority will be executed before jobs with a lower queue priority. For instance a job with a queue priority of 6 will be executed before a job with a queue priority of 5. Jobs with the same queue priority will be processed on a first in/first out basis.

The **Run Priority** indicates how much attention (CPU) the job will receive from Managed File Transfer when it executes. The run priority is a value from 1 to 10, in which jobs with a higher run priority will receive more attention than jobs with a lower run priority. For instance a job with a run priority of 6 will receive more attention than a job with a run priority of 5.

Functions Available

- Refresh the Scheduler Job Queue page by clicking the **Refresh** button.
- Delete a repeating scheduled job by clicking the  icon.

View Scheduled Job

Follow the instructions below to view the properties for a Scheduled Job:

1. Log in as an Admin User with the Job Manager role.

2. The properties can be viewed using the View Scheduled Job page. To open this page, first open the "Work with Scheduled Jobs" on page 188 page and then click the View  icon next to the entry to view.
3. This page displays the properties for the Scheduled Job, along with the User/date/time of when the Scheduled Job was created and when it was last modified.
4. Click the **Done** button when finished viewing the Scheduled Job details.

Promote Schedules

Authorized users can promote Schedules from one Managed File Transfer installation to another. This will copy the definition of the Schedule to the targeted installation. For example, after a Schedule is tested, the Schedule could be promoted from that test installation to a production installation of Managed File Transfer.

Promote Schedule(s) by following the steps below:

1. Schedules can be promoted using the **Promote Schedules** page. Follow the steps below to access this page:
   a. Log in as an Admin User with the Job Manager role.
   b. From the main menu, select **Workflows** and then click the Scheduler link.
   c. Click the checkboxes of the Schedule(s) to promote.
   d. Click the **Promote** button that appears in the page footer.
2. Enter values for the following fields:

Target Server

The host name (or IP address) of the Managed File Transfer installation on which to copy the Schedule(s). The value specified must be a URL of the form `http://[host]:[port]/informaticamft`, where [host] is the host name or IP address of the target Managed File Transfer installation, and [port] is the port number on which Managed File Transfer server is running, which by default is 8000. An example value would be http://10.1.4.1:8000/informaticamft

User Name

The user name to login to the target Managed File Transfer installation.

Password

The password for the user to login with. The password is case sensitive.

Replace Existing Schedules

Indicate if the Schedule(s) should be replaced on the target Managed File Transfer installation if they already exist with the same name.

1. Click the **Promote** button to copy the Schedule(s) to the target installation.

Permissions Required

An Admin User must have the following permissions in order to promote a Schedule:

- Job Manager role on both the source and target Managed File Transfer installations.

Scheduled Job History

To view the Scheduled Job History page in Managed File Transfer, login as a user that has the Job Manager role.

Select **Workflows** from the main menu, and then click the Scheduler link. In the list of Scheduled Jobs, click the icon beside a Scheduled Job to open its Scheduled Job History.

The Scheduled Job History page provides a wide variety of search criteria. You can also specify the Results Per Page displayed on the page. After specifying the criteria, click the **Search** button

The following details will be shown for each Job on the page:

- Job Number - A unique Job number given to each project at runtime
- Project Name - Name of the Project
- Folder - The folder location of the Project
- Status - The outcome of the job (= failed, = success)
- User - The User who submitted the Job
- Start Time - When the Job started executing
- End Time - When the Job completed
- Time - Execution time (in seconds)

Page Toolbar

The following actions are available from the page toolbar:

- Click the **Done** button to return to the Schedules page.

Scheduled Job History Actions

The following actions are available by selecting the Actions icon:

- "Job Log and Details" on page 186 the Job Details by clicking the icon.
- "Job Log and Details" on page 186 the Job Log by clicking the icon.

  - Edit the selected Project by clicking the Edit Project link.

  - View the folder where the Project is located by clicking the View Project Folder link.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file.
- Click the **Export Results** button to save the results from all pages to a .CSV file on your local computer.

  Note: The default saved Job Log file name is "JobLogsYYYYMMDD.csv" (where YYYYMMDD is the current year, month, and day).

Show Schedule

The Schedule page displays the next scheduled dates and times a scheduled job will run. Scheduled times affected by a holiday rule are displayed in red with the adjusted date shown in the Adjusted Schedule column.

Click on the Calendar radio button to view the scheduled dates and times in a calendar format. Click the  **Edit** button to "Adding or Editing a Scheduled Job" on page 190 the Schedule. Click the  **Done** button to return to the Scheduled Jobs page.

Monitors

The File Monitor function in Managed File Transfer provides the ability to repeatedly scan for new, changed or deleted files in a folder. When the scan condition is met, the Monitor can call a pre-defined *Project* to process the file(s).

How Monitors Work

When a new Monitor is created, an initial snapshot of the folder is taken and the next run time is calculated. Taking a snapshot requires the Monitor to scan the folder (and optionally subfolders), looking for files that match the file name pattern. The result is an XML-based snapshot file that will be stored in the [monitorsdirectory]/[monitor type] folder. The location of the Monitors Directory can be configured in the Global Settings.

The Monitor function will check every 15 seconds for any Monitors that need to run, which is based on their calculated next run times. When an individual Monitor runs, it will load the last recorded snapshot file and will also take a current snapshot. Based on the Monitor settings, it then compares the files for one of the following events:

- Files Created: When scanning for files that were created, the Monitor compares the new snapshot against the last one. If a file was not in the last snapshot, it is considered new. The Monitor will then determine if the file is still being written to by another application using the File Availability settings on the Monitor's "Adding or Editing Monitors" on page 200 tab. If successful, meaning no other process is currently writing to it, the Monitor will add the file to the monitor.fileList output variable (which can be sent onto the Project). If the file is in use, it is removed from the current snapshot and ignored. The next time the Monitor compares snapshots, it will treat the file (that was in use) as new and will, once again, determine if the file is in use, and add the file to the monitor.fileList output variable if the file is not being written to.
- Files Modified: When scanning for modified files, the Monitor compares the new snapshot against the last one. If the file is located in both snapshots and the last modified date has been updated, then the Monitor will determine if the file is in use using the File Availability settings on the Monitor's "Adding or Editing Monitors" on page 200 tab. If successful, the modified file is added to the monitor.fileList output variable. If the file is in use, the file will be ignored and checked the next time the Monitor runs.

- Files Deleted: When scanning for deleted files, the Monitor compares the new snapshot against the last one. If a file is in the last snapshot but is not in the new one, the file is added to the monitor.fileList output variable.
  After the snapshot comparison completes, the Monitor will overwrite the snapshot file with the current snapshot.

  If any files were found which meet the event criteria that was monitored for, then the Project (specified on the Monitor's Action tab) will be called with the list of files (from the monitor.fileList variable).

  Note: Email notifications can be sent when a Project completes successfully, when a Project fails or if an error occurs. A notification email can also be sent if no files were found by the end of the day (that met the selection criteria). These emails are sent using the SMTP settings located in the Global Settings and the email messages can be customized using "Project Email Templates" on page 826.

Editing or Enabling Monitors

Under certain conditions, a new snapshot is created when a Monitor is edited. This occurs when a previously disabled Monitor becomes enabled, or when the following Monitor settings have been changed:

- Monitor Type (FTP, FTPS. SFTP, Local/Network Share)
- Folder Location
- Recursive
  Event Type (Files Created, Files Modified, Files Deleted)

  File Name Pattern

  Pattern Type

  When a new snapshot is created, any file activity that occurred since the last time the Monitor ran will be ignored.

Performance Considerations

Each time a Monitor runs, system resources are utilized to scan folders and compare snapshots. Scanning a folder with a couple files only takes a few milliseconds and minimal system resources. On the other hand, if hundreds of Monitors are set to run every 15 seconds with thousands of files in each folder, the performance impact on the server should be taken into consideration.

The number of active Monitors can be limited by changing the Maximum Concurrent Monitors (located on the Runtime tab in the Global Settings). When a Monitor starts a Project, the Monitor remains active while the Project is running. Setting the Maximum Concurrent Monitors to 1 only allows one Monitor to run at a time. If the Project being executed takes a long time to process, this may undesirably delay the execution of the other Monitors. The default Maximum Concurrent Monitors is 20.

To determine which monitors are actively running and how long they are processing, set the Global Log Level to Debug (located on the Global Log tab in the Log Settings). In Debug mode, a log record is written each time a Monitor is submitted and when a Monitor completes along with the time taken.

Work with Monitors

To work with Monitors, log in as an Admin User with a Job Manager role. From the menu bar, point to Workflows, and then click **Monitors**.

This page allows you to search for Monitors using a variety of criteria. After typing the criteria, click the **Search** button to perform the search. If a column below is not shown, click the Show/Hide Columns link for a complete list.

Note: When searching for a Monitor, the search results found on the Basic tab will return exact matches for the search term. Use the Advanced Search tab to search additional fields and control the search term logic (for example, Equals, Begins With, Ends With and Contains). Search terms are not case sensitive.

Page Toolbar

The following actions are available from the page toolbar:

- "Adding or Editing Monitors" on page 200 a Monitor by clicking the  Add Monitor link in the page toolbar.
  - Disable all Monitors from running by clicking the  Disable Monitors link in the page toolbar. When the Disable Monitors link is clicked, all active Monitors will finish. Monitors that are scheduled to run will be suspended until the  Enable Monitors link in the page toolbar is clicked (even if Managed File Transfer is restarted).
- "Active Monitors" on page 205 all active Monitors by clicking the  Active Monitors link in the page toolbar.
- "Queued Monitors" on page 204 all queued Monitors by clicking the  Queued Monitors link in the page toolbar.

Monitor Actions

The following actions are available by selecting the  Actions icon:

- "Adding or Editing Monitors" on page 200 a Monitor by clicking the  icon next to the entry.
  - Copy the Monitor by clicking the  icon. The monitor is copied, automatically renamed and opened for editing.
  - Delete the selected Monitor by clicking the  icon.
- "Promote Monitors" on page 204 a Monitor to another Managed File Transfer installation by clicking the  Promote icon.
- "View Monitor" on page 206 a summary of the Monitor by clicking the  icon.
  - Deactivate or Activate a Monitor by clicking the  Deactivate or  Activate icon.
  - Reset the Misfire count by clicking the  Reset Misfires link.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Monitors.
- Promote one or more selected Monitors to another Managed File Transfer server.
- Activate the Monitor.
- Deactivate the Monitor.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Columns** button to select which Monitor properties are displayed in the table.

Monitor Columns

- Monitor Name - The name of the Monitor. Hover the pointer over the Monitor Name to view when the Monitor is scheduled to run.
- Description - A description of what the Monitor does.
- Status - Whether the Monitor is active or inactive.
- Monitor Location - The type of resource being monitored.
- Schedule - The frequency of the Monitor.
- Last Run Time - The date/time of when the Monitor last ran.
- Next Run Time - The date/time of when the Monitor will run again.
- Run Count - The number of times the Monitor has run.
- Misfires - The number of times that the Monitor did not run (due to any downtime of the Managed File Transfer server).
- Created By - The user who created the Monitor.
- Created On - The date and time the Monitor was created.
- Last Modified By - The user who last modified the Monitor.
- Last Modified On - The date and time the Monitor was last modified.
- Action Last Run Time - The last date/time the action ran.
- Actions Fired - The number of times the action (Project) has run.

Adding or Editing Monitors

To create or modify a Monitor, log in as an Admin User with the **Job Manager** role. From the menu bar, point to Workflows, and then click **Monitors**. To create a new Monitor, click the Add Monitor link in the page toolbar. To edit an existing Monitor, click the icon.

Listed below are the field descriptions within each tab of the Monitor.

General Tab

The General tab contain the following settings:

Monitor Name

A user-defined name which identifies the Monitor. This name should be descriptive enough so users can quickly identify this Monitor from the list. The Monitor Name cannot exceed 50 characters. Spaces are allowed.

Description

A short paragraph that describes the Monitor. The Description is optional and cannot exceed 512 characters.

Status

The status indicates if the Monitor is active or inactive. An inactive Monitor will not execute. If a Monitor is set to inactive, it will appear grayed out on the Monitors page.

Monitor Location

The type of folder or resource to monitor. Valid values are Local/Network Share, "FTP Servers Resource" on page 55, "FTPS Servers Resource" on page 59, or "SFTP Servers Resource" on page 66. When an FTP, FTPS, or SFTP location is selected, the FTP Resource field appears. Select an existing resource, or click the Create button to add a new one.

Folder

The folder location that is monitored for events. A Monitor can search files on the local file system, a network share, or an FTP, FTPS, or SFTP resource. Type the folder location or click the icon to browse for the location.Note: When monitoring files on a network share, the Network Shares resource cannot be set to authenticate using the logged in user credentials.

Recursive

The recursive option will include the files in the sub-folder(s) of the folder selected for monitoring.

Event Type

The type of file event for which to monitor. Valid values are File Created, File Modified and File Deleted.

File Name Pattern

The Monitor will search for (filter) files based on the specified pattern. By default, an * indicates to search for any files in the folder. The File Name Pattern can either be a "Wildcards and Regular Expressions" on page 837. The file name pattern cannot exceed 100 characters.

Pattern Type

The pattern type can be Wildcard or Regular Expression and must indicate the type of pattern used in the File Name Pattern field.

Schedule Tab

The Schedule tab contain the following settings:

Start At

The time of day when the Monitor will start monitoring for file events.

Check Until

The time of day when the Monitor will stop monitoring for file events.

Check Every

rhe duration between each execution of the Monitor. The shortest time period between monitor cycles is 15 seconds.

Days to Run

The days of the week the Monitor should run. The default is Monday through Friday.

Stop checking if file(s) found

Enabling this option will suspend execution of the Monitor (for the rest of the day), after the file condition is met. This feature decreases the amount of system resources used by the Monitor when one set of file(s) are expected per day.

Project Tab

The Project tab contain the following settings:

Project

The name of the Project to execute when the Monitor conditions are satisfied. Browse for the Project by clicking the  button next to the field.

Login As

The User account that will be used to execute the project.

Password

The password to use for authenticating the specified user (Login as).

Run Priority

The run priority indicates how much attention (CPU) the job will receive from Managed File Transfer when it executes. The run priority can be a value from 1 to 10, in which jobs with a higher number will receive more attention than jobs with a lower number. For instance a job with a run priority of 6 will receive more attention (CPU) than a job with a run priority of 5.

Job Name

Specify a name which identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters. Spaces are allowed.

Variables

Use the Add Variable link to add any additional variables required by the project. In the Variable box, type a valid Variable name and value. The ${var} icon provides a drop-down list of pre-defined "Variables" on page 111. The ${monitor.fileList} variable contains a File List of one or more files found while monitoring. This variable can be passed into a Project allowing the files found by the Monitor to be processed.

File Availability Check

Two different methods are provided for determining if files are available for processing, which will help prevent a file from being considered if it's still being written to by another application:

- File Lock - Managed File Transfer will attempt to make an exclusive lock on the file to determine if it is available for processing. Please note that File Locks are not supported by FTP, FTPS and SFTP Monitors, as well as some file systems.
- Secondary Snapshot - Managed File Transfer will compare the size and last modified date of the file between the current snapshot and one taken after the specified snapshot delay. If the file has not been modified during that time, the file will be considered as available for processing. This approach is slower than a File Lock.

Secondary Snapshot Delay

Specify the duration of time between the current snapshot and the secondary snapshot, in seconds.

Advanced Tab

The Advanced tab allows you to specify how Managed File Transfer determines if a file is in use or available for processing. The Advanced tab contains the following settings:

File Availability Check

Two different methods are provided for determining if files are available for processing, which will help prevent a file from being considered if it's still being written to by another application:

- File Lock - Managed File Transfer will attempt to make an exclusive lock on the file to determine if it is available for processing. Please note that File Locks are not supported by FTP, FTPS and SFTP Monitors, as well as some file systems.
- Secondary Snapshot - Managed File Transfer will compare the size and last modified date of the file between the current snapshot and one taken after the specified snapshot delay. If the file has not been modified during that time, the file will be considered as available for processing. This approach is slower than a File Lock.

Secondary Snapshot Delay

Specify the duration of time between the current snapshot and the secondary snapshot, in seconds.

Email Notifications Tab

Email notifications can be sent to specified recipients when a Monitor fails to run, when a Project invoked by a Monitor completes successfully or fails, or a Monitor does not find any files. Project Success and Project Failure email notifications can also include the job log as an attachment. Separate multiple email addresses with commas.

Monitors use "Project Email Templates" on page 826 defined in XML files under the [installdirectory]/userdata/emailtemplates folder where [installdirectory] is the installation directory of the Managed File Transfer product. The templates can be modified to meet your specifications using an XML or a plain text editor.

Note: Emails are sent using the settings located on the SMTP tab in the Global Settings.

The Email Notifications tab contains the following settings:

On Error

An email notification will be sent to the recipient(s) email address when a monitor fails to run.

Project Success

An email notification will be sent to the recipient(s) email address when a Project invoked by a Monitor completes successfully. The job log can be attached to the Project Success email.

Project Failure

An email notification will be sent to the recipient(s) email address when a Project invoked by a Monitor fails. The job log can be attached to the Project Failure email.

No Files Found

An email notification will be sent the recipient(s) email address when no files are found for the scheduled day. View an "Monitor Example" on page 205 of how a Monitor can execute a Project when new files are found in a folder.

Promote Monitors

Authorized users can promote Monitors from one Managed File Transfer installation to another. This will copy the definition of the Monitor to the targeted installation. For example, after a Monitor is tested, the Monitor could be promoted from that test installation to a production installation of Managed File Transfer.

Promote Monitors by following the steps below:

1. Monitors can be promoted using the **Promote Monitors** page. Follow the steps below to access this page:
   a. Log in as an Admin User with the Job Manager role.
   b. From the main menu, select **Workflows** and then click the Monitors link.
   c. Click the checkboxes of the Monitors(s) to promote.
   d. Click the **Promote** button that appears in the page footer.
2. Enter values for the following fields:
   Target Server

   The host name (or IP address) of the Managed File Transfer installation on which to copy the Monitor(s). The value specified must be a URL of the form `http://[host]:[port]/informaticamft`, where [host] is the host name or IP address of the target Managed File Transfer installation, and [port] is the port number on which Managed File Transfer server is running, which by default is 8000. An example value would be http://10.1.4.1:8000/informaticamft

   User Name

   The user name to login to the target Managed File Transfer installation.

   Password

   The password for the user to login with. The password is case sensitive.

   Update Existing Monitors

   Indicate if the Monitor(s) should be replaced on the target Managed File Transfer installation if they already exist with the same name.
3. Click the **Promote** button to copy the Monitor(s) to the target installation.

Permissions Required

An Admin User must have the following permissions in order to promote a Monitor:

- Job Manager role on both the source and target Managed File Transfer installations.

Queued Monitors

The Queued Monitors page displays all monitors waiting to execute. Monitors will be queued when a Monitor is submitted and the maximum number of active Monitors has been reached. Once an active Monitor finishes, the next Monitor in the queue will be processed on a first in, first out basis. The maximum number of active Monitors is set using the Maximum Concurrent Monitors field on the Runtime tab in Global Settings.

Click the **Refresh** button to manually refresh the list or click the **Done** button to return to the "Work with Monitors" on page 198 page.

Available Options

System - Select a system from the drop-down list to only show the queued Monitors on that particular system. This option is only available when Managed File Transfer is running in a clustered environment.

Display Results - From the drop-down list, select the number of results to display on the page at one time.

Auto Refresh - Selecting the Auto Refresh box will refresh the page every five seconds.

Active Monitors

The Active Monitors page displays all actively running monitors. Monitors are considered active when they are scanning folders and comparing snapshots. If the Monitor has executed a Project, it will continue to display as active while the Project is running. If more Monitors are fired than is provided for in the Maximum Concurrent Monitors field on the Runtime tab in Global Settings, they will wait in a "Queued Monitors" on page 204 on a first in - first out basis.

Click the **Refresh** button to manually refresh the list or click the **Done** button to return to the "Work with Monitors" on page 198 page.

Available Options

System - Select a system to filter the results to only show the active Monitors running on that system. This option is only available when Managed File Transfer is running in a clustered environment.

Auto Refresh - Select the Auto Refresh box to refresh the page every five seconds.

Monitor Example

The following is an example of how to create a Project that sends new files (identified by a file Monitor) to an FTP server.

1. Define a new Project to process the files identified by the Monitor.
   a. From the main menu, select **Workflows** and then click the Projects link.
   b. In the Projects page, drill-down to the folder in which to create the new Project.
   c. Click the Create a Project link in the sub-menu.
   d. The Managed File Transfer Project Designer will open.
   e. Type the Project name and description, and then click **Save**.
   f. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
   On the Basic tab of the FTP Task, choose a FTP server resource.
   g. Click the **Add** button and select **Put Files**.
   h. On the Put Files Basic tab, specify the Source Files Variable and the Destination Directory. The ${files} variable will be defined in the Monitor. This variable will contain a list of files identified by the Monitor and will be used in this task after the Monitor runs.
   i. Click the **Save and Finish** button.
2. Create the Monitor that will identify the new files and execute the Project (created in the first step).
   a. From the menu bar, select **Workflows**, and then click **Monitors**.
   b. Click the Add Monitor link in the page toolbar.

c. On the Monitors General tab, specify values for the required fields such as the folder to scan for new files.

d. On the Monitors Schedule tab, specify how frequently the Monitor should run.

e. On the Monitors Project tab, specify the Project to execute (created in the first step) and define the variable that will contain the list of files identified by the Monitor. This is the variable used by the FTP task in step 1 - j above.

f. Click the **Save** button. The Monitor starts and will execute the Project each time it finds new files in the specified folder.

View Monitor

The View Monitor page displays the settings from each tab of the Monitor and the last time and date when the Monitor ran. When finished reviewing the information, click the **Done** button to return to the Monitors page.

Trigger Manager

Triggers can be defined to monitor the system for certain events. When those events occur (for example, file uploaded successfully), then Managed File Transfer looks at the list of triggers, checks their conditions, and if met will execute the appropriate action. This provides the opportunity to automate additional processes after an event. For instance, when a file is received from a trading partner, an email notification can be sent or a Project can be executed to further process that file.

Trigger Actions at a Glance

The following trigger actions are available:

Call Project

A local Managed File Transfer Project can be executed to further process the file.

Call Remote Project

A Project on a remote Managed File Transfer server can be executed to further process the file.

Execute Native Command

Runs batch, executable and shell scripts.

Delete File

Deletes a file.

Move File

Moves a file from one location to another.

Rename

Renames a file.

Send Email

An email is sent to one or more recipients. The email can be easily customized to include variables and other text.

If more than one Trigger exists for an event type, reorder a Trigger by grabbing the row and dragging it to a new position. Triggers are executed sequentially in the order they appear. Triggers that need to run before others should be placed earlier in the sequence.

To administrate Triggers, log in as an Admin User with the **Trigger Manager** role.

From the main menu bar, select **Workflows**, and then click the Triggers link.

Page Toolbar

The following actions are available from the page toolbar:

- "Add Trigger" on page 207 a Trigger by clicking the **Add Trigger** link in the toolbar
- "Import Trigger" on page 217 a Trigger by clicking the Import Trigger link in the toolbar
  - Disable all Triggers from running by clicking the Disable Triggers link in the toolbar. When the Disable Triggers link is clicked, all active Triggers will finish. Triggers that are scheduled to run will be suspended until the Enable Triggers link in the toolbar is clicked (even if Managed File Transfer is restarted).
  - Filter the Trigger list by selecting the Event Type from the drop-down list. Selecting an Event Type will only display those events on the page. Show all Events by selecting the blank line at the top of the Event Type drop-down list.

Trigger Actions

The following actions are available by selecting the Actions icon:

- "Trigger Details" on page 215 Trigger Details by clicking the icon
- "Edit Trigger" on page 213 a Trigger by clicking the icon
  - Delete a Trigger by clicking the icon
- "Copy Trigger" on page 214 a Trigger by clicking the icon
- "Trigger Execution History" on page 215 Trigger Execution History by clicking the icon
- "Promote Trigger" on page 216 the Trigger by clicking the icon
  - Export a Trigger by clicking the icon. The Trigger information is saved to an XML file and can be imported to another instance of Managed File Transfer.

Add Trigger

Add a Trigger using the Add Trigger page. Follow the instructions below to add a Trigger:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. In the "Trigger Manager" on page 206 page, click the Add Trigger link in the page toolbar.
4. The Select Event Window appears. Select an Event Type and then click the **Continue** button.
5. Type the Trigger information in the appropriate boxes.
6. Click the **Save** button to add the Trigger.

General

The General tab contains the following settings:

Name

The Trigger name identifies the Trigger on the Trigger Manager page.

Description

This is a description of what the Trigger does for reference purposes.

Event Type

A Trigger is started when a specific "Event Types" on page 799 occurs.

Status

This allows you to disable a Trigger.

Stop Processing More Triggers

After a particular event occurs, you may not want other Triggers with the same event type (For example, Download Successful) to run. Therefore, Triggers that must run before all Trigger processing would stop should be given higher priority. Triggers with this option selected are displayed on the "Trigger Manager" on page 206 page with a  icon.

Service

The service option allows you to specify which services the trigger will monitor.

Conditions

Conditions help narrow the scope of a Trigger (for example, a particular User or file name). Conditions automatically use lower case values when comparing parameters or searching for a value within a string. If grouping conditions, use the parenthesis to indicate the start and end of each comparison group.

You can perform the following actions:

- Delete a condition by clicking the  icon
- Move a condition statement up by clicking the  icon
- Move a condition statement down by clicking the  icon

Create a condition statement with the following steps:

1. If a new line is needed, click the Add Condition... link.
2. From the Attribute drop-down list, select a "Trigger Event Variables" on page 803.
3. From the Expression drop-down list, select an operator.
4. In the Comparison Value box, type the string or select the option that will form the condition.
5. Select an And/Or value if the condition must evaluate to true based on multiple conditions.
6. Repeat these steps to add any additional conditions.

Action

There are seven Action Types available:

Call Project

The Call Project action is used to invoke a Project. For example, the called project could extract specific values from a spreadsheet and insert them into a database.

The Action tab for the Call Project action has the following settings:

Project

Specify the Project to run. Click the  button to navigate to the Project.

User

The Admin User account that is used to execute the Project.

Password

The Admin User password. If encryption on the password is required, click the Encrypt... button.

Is Password Encrypted?

Indicates whether or not the password is encrypted. Select Yes if the Encrypt button was clicked above.

Run Mode

By default, an Managed File Transfer Project is run in batch mode, allowing the session to continue with other processes. When set to Interactive, the session will wait for a response from the Project before continuing. When set to Batch, the Job Queue can be specified.

Priority

The Project called by the Trigger can be assigned a priority within Managed File Transfer. The priority indicates which Projects receive a higher run priority (more CPU cycles) and queue priority in Managed File Transfer. The priority range is 1 (lowest) to 10 (highest). The default priority is 5.

Job Queue

When Batch is selected in the Run Mode field, you can specify the Job Queue the job will run in Managed File Transfer. If left blank, the job will run under the Default job queue.

Job Name

Specify a name which identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters.

Project

The Project refers to the folder and name of the Project to run in Managed File Transfer. The folder path and Project name are case sensitive. An example of a project is /Payroll/SendDirectDeposit, where SendDirectDeposit is the project name and Payroll is the folder. Click the  icon to browse for a project or specify a variable that refers to the project.

Variables

Use the Add Variable link to add any additional variables required by the Project. In the Name box, type a valid variable name expected by the Managed File Transfer Project. In the Value box, either specify a constant or an event variable. To delete a variable, click the  icon beside the entry.

Note: When available, the  icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Call Remote Project

The Call Remote Project action is used to invoke a Project on a different Managed File Transfer server.

The Action tab for the Call Remote Project action has the following settings:

Resource

The pre-configured Managed File Transfer"Informatica MFT Server Resource" on page 92 that is used to execute the Project.

Project

Specify the Project to run. Click the  button to navigate to the Project.

Override User

The Admin User account that is used to execute the Project on the remote Managed File Transfer server.

Override Password

The Admin User password. If encryption on the password is required, click the Encrypt... button.

Is Password Encrypted?

Indicates whether or not the password is encrypted. Select Yes if the Encrypt button was clicked above.

Run Mode

By default, an Managed File Transfer Project is run in batch mode, allowing the session to continue with other processes. When set to Interactive, the session will wait for a response from the Project before continuing. When set to Batch, the Job Queue can be specified.

Priority

The Project called by the Trigger can be assigned a priority within Managed File Transfer. The priority indicates which Projects receive a higher run priority (more CPU cycles) and queue priority in Managed File Transfer. The priority range is 1 (lowest) to 10 (highest). The default priority is 5.

Job Queue

When Batch is selected in the Run Mode field, you can specify the Job Queue the job will run in Managed File Transfer. If left blank, the job will run under the Default job queue.

Job Name

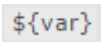
Specify a name which identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters.

Project

The Project refers to the folder and name of the Project to run in Managed File Transfer. The folder path and Project name are case sensitive. An example of a project is /Payroll/SendDirectDeposit, where SendDirectDeposit is the project name and Payroll is the folder. Click the  icon to browse for a project or specify a variable that refers to the project.

Variables

Use the Add Variable link to add any additional variables required by the Project. In the Name box, type a valid variable name expected by the Managed File Transfer Project. In the Value box, either specify a constant or an event variable. To delete a variable, click the  icon beside the entry.

Note: When available, the 

icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Delete File

The Delete File action deletes a file when the Trigger is executed. For instance, you might want to delete a file after a trading partner has downloaded it.

Define the **File** setting, the full path of the file that will be deleted. Click the  icon to browse for a file or specify the variable ${event.physicalPath} to refer to the file that is associated with the current event. Please note that if the file does not exist, the trigger will be marked as successful and a warning is written to the trigger log details.

Note: When available, the ${var} icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Execute Native Command

The Execute Native Command action can run a command, executable, or script on the host system when a Trigger with this action type is executed.

Define the following settings:

Executable

The file path and name of the executable command, program or script to execute. Specify the path and executable or click the  icon to browse for the executable.

Working Directory

The directory that the executable will use as the working directory. Type the path or click the  icon to select the path.

Wait For Process to End

Managed File Transfer can wait for the executable to end before continuing or it can continue processing while this trigger finishes.

Arguments

One or more arguments can be passed to the command as variables or constant values. To delete an Argument, click the  icon beside the entry.

Note: When available, the ${var} icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Move File

The Move File action moves a file to another folder. For example, after a report is uploaded it needs to be moved into a shared directory where others can view the report.

You can change the following settings:

Source File

The full path of a file that will be moved to a new location. Click the  icon to browse for a file or specify the event variable ${event.physicalPath} to refer to the file that is associated with the current event.

Destination Directory

This is the location of a directory to where the file will be moved. If the directory does not exist it will be created automatically. Click the  icon to browse for a folder.

When File Exists

This is the location of a directory to where the file will be moved. If the directory does not exist it will be created automatically. Click the  icon to browse for a folder.

Arguments

If a file with the same name already exists in the Destination Directory, the options are to Overwrite the existing file, Rename the file that is moving by appending a number to the end of the file name, Stop the file move action or produce an Error.

Note: When available, the ${var} icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Rename File

The Rename File action renames a file when the Trigger is executed.

You can change the following settings:

Source File

The full path and file name of the file that will be renamed. Click the  icon to browse for a file or specify a variable to refer to the file that is associated with the current even.

New Name

This is the name that the file will be renamed to.

When File Exists

This is the location of a directory to where the file will be moved. If the directory does not exist it will be created automatically. Click the  icon to browse for a folder.

Arguments

If a file with the same name already exists in the Destination Directory, the options are to Overwrite the existing file, Rename the file that is moving by appending a number to the end of the file name, Stop the file move action or produce an Error.

Note: When available, the ${var} icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Send Email

The Send Email action sends an email to one or more recipients when the Trigger is executed. For example, when a trading partner uploads a file, this Trigger alerts the specified recipients of the file upload.

You can change the following settings:

From Name

The From Name is the name that appears on the email as the sender.

From

The email address the email is sent from.

To

Email addresses for the recipients of this email. Separate multiple email addresses with a comma.

CC

Provide additional email addresses that should receive a Carbon Copy of this email. Separate multiple email addresses with a comma.

BCC

The Blind Carbon Copy option allows you to send the email to people without the knowledge of others. Separate multiple email addresses with a comma.

Reply To

If replies are expected from the recipients of the email, type the email address that will receive these replies.

Subject

The Subject will appear in the subject line of the recipient's email. You can insert more than one event variable along with text in this box.

Body

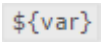
This box contains the body text that will be sent along in the email. You can insert more than one event variable along with text in this box.

Body Content Type

The default body content type for email is text/plain. Other body content types can be placed in this field if required (e.g. text/html, text/xml).

Attachment

If required, an attachment can be sent along with the email. Click the  icon to browse for a file.

Note: When available, the 

icon provides a drop-down list of pre-defined "Trigger Event Variables" on page 803.

Edit Trigger

Edit a Trigger using the Edit Trigger page. Follow the instructions below to edit a Trigger:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. In the "Trigger Manager" on page 206 page, click the  icon beside the Trigger you wish to edit.
4. When complete, click the **Save** button.

General

The General tab contains the following settings:

Name

The Trigger name identifies the Trigger on the Trigger Manager page.

Description

This is a description of what the Trigger does for reference purposes.

Event Type

A Trigger is started when a specific "Event Types" on page 799 occurs.

Status

This allows you to disable a Trigger.

Stop Processing More Triggers

After a particular event occurs, you may not want other Triggers with the same event type (For example, Download Successful) to run. Therefore, Triggers that must run before all Trigger processing would stop should be given higher priority. Triggers with this option selected are displayed on the "Trigger Manager" on page 206 page with a  icon..

Service

The service option allows you to specify which services the trigger will monitor.

Conditions

Conditions help narrow the scope of a Trigger (for example, a particular User or file name). Conditions automatically use lower case values when comparing parameters or searching for a value within a string. If grouping conditions, use the parenthesis to indicate the start and end of each comparison group.

You can perform the following actions:

- Delete a condition by clicking the  icon
- Move a condition statement up by clicking the  icon
- Move a condition statement down by clicking the  icon

Create a condition statement with the following steps:

1. If a new line is needed, click the Add Condition... link.
2. From the Attribute drop-down list, select a "Trigger Event Variables" on page 803.
3. From the Expression drop-down list, select an operator.
4. In the Comparison Value box, type the string or select the option that will form the condition.
5. Select an And/Or value if the condition must evaluate to true based on multiple conditions.
6. Repeat these steps to add any additional conditions.

Actions

The Actions tab will show the selected Trigger Action. Open the Action drop-down on the "Add Trigger" on page 207 page for more specific information for the available options.

Copy Trigger

The Copy Trigger function allows you to copy all the attributes of an existing Trigger into a new Trigger that you can edit. Follow the steps below to copy a Trigger:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.

3. In the "Trigger Manager" on page 206 page, click the  icon beside the Trigger you wish to copy and then click the  icon.
4. After clicking the  icon, the process and information for copying the Trigger is the same as the "Add Trigger" on page 207 process.
5. When complete, click the **Save** button.

Trigger Details

The Trigger Details page shows the properties for the Trigger, when it was created and when it was last modified. It also shows the Action assigned to the Trigger and on which Services it is active. Follow the steps below to view the Trigger Details:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. In the "Trigger Manager" on page 206 page, click the  icon beside the Trigger you wish to view. Then from the drop-down, click  **View**.

Trigger Execution History

Follow the instructions below to view Trigger Execution History:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. In the **Manage Triggers** page, from the  More Actions list, click the  icon.
4. In the Trigger Execution History page, view the details or change parameters and then click the **Search** button.
5. Click the  icon to view the "View Trigger Log Details" on page 689.

Search Options

The following settings are available:

Date Range

The Date Range allows you to specify the scope of your search based on date and time. Click the icon to select the date and time.

Trigger Name

This is the name of the trigger for which the execution history is displayed.

Status

The Status field reports if the Trigger was successful, failed or is still in progress.

Event ID

The Event ID can be specified to limit search results. Leave blank if unknown or to return more results.

Service

The Services are the transport services that were used for transmitting the files.

Event Type

The Trigger event type that launched the Trigger.

Results Per Page

The number of rows to display on the page at a time.

Actions

Click the  icon to view "View Trigger Log Details" on page 689.

Table Actions

- Click the  button to move back to the previous page of results.
- Click the button to move forward to the next page of results.
- Click the **Export Results** button to save the results from all pages to a .CSV file on your local computer.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Columns** buttons to select the columns that are displayed on the table.

  Note: If you use one of the Export options, only the visible columns are saved to the exported file. Click the Show/Hide Columns link to change the visible columns.

Promote Trigger

Triggers can be promoted from one Managed File Transfer instance to another using the promote trigger option (for example, promoting working triggers from a development server to a production server).

Follow the steps below to promote a Trigger:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. Click the  icon beside the Trigger that will be promoted and then click the  icon.
4. Complete the required fields for the target server and then click the **Promote** button.

Target Server

The IP or host name of the server to which the Trigger is being promoted. The Target Server format is [Protocol]://[IP or Hostname]:[Port Number]/informaticamft (for example, http://10.1.4.1:8000/informaticamft).

User Name

The user name of an Admin User on the target Managed File Transfer server that has the Trigger Manager role.

Password

The password for the Admin User on the target Managed File Transfer server.

Replace Target Trigger

If a Trigger already exists on the target server with the same name, selecting this option will overwrite the existing Trigger on the target server.

Import Trigger

The Import Trigger option allows the creation of a single Trigger from an XML file that was generated by the Trigger export process. Follow the steps below to import a Trigger:

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select Workflows, and then click the Triggers link.
3. In the "Trigger Manager" on page 206page, click the  Import Trigger link in the page toolbar.
4. On the Import Trigger page, specify the following:
   - Import From - The XML file can be imported from either a file on the end user's PC or a file on the Managed File Transfer server.
   - Input File - The path or location of the XML file containing the Trigger information.
   - Replace Target Trigger - When selected, an existing Trigger with the same name will be overwritten with the information from the import.
5. When complete, click the **Import** button. A message on the page displays the import results.

Job Queue Manager

Job queues are used for prioritizing and grouping batch jobs that are waiting to be executed by Managed File Transfer. By defining multiple Job Queues in the system, each queue can be used to execute Jobs that share common characteristics or service level agreements (SLAs). For example, you can create a Job Queue to run Jobs for a certain application or customer which may have a higher priority than other jobs. You could also create a single-threaded Job Queue for Jobs that need to run in sequential order. In a clustered environment, you can create a Job Queue to only execute Jobs on a specific Managed File Transfer system.

Projects can be submitted to a Job Queue through several methods. You can specify a Job Queue on the Project's "Project" on page 108, from the "Scheduling Projects" on page 187, "Call Remote Project Task" on page 437, or the RunProject command in Managed File Transfer Command. When no Job Queue is specified, the Project will be executed in the Default Job Queue.

Each Job Queue can have a Priority to indicate the order in which the queue will be considered for job execution. The Job Queue priority will be a value from 1 to 10, in which Job Queues in a higher queue priority will be executed before Job Queues with a lower queue priority. For instance, a Job Queue with a queue priority of 6 will execute jobs before a Job Queue with a queue priority of 5. Jobs within a Job Queue that have the same queue priority will be processed on a first in/first out basis.

You can specify the number of Jobs which can be executed at one time within each Job Queue. The Max Active Jobs setting is limited to the maximum concurrent batch jobs specified in the Global Settings of Managed File Transfer.

As a Product Administrator, you can use the Job Queues Manager page to create and work with Job Queues in Managed File Transfer.

To view the Job Queue Manager, log in as a user with the Job Manager or Product Administrator role.

From the menu bar select **Workflows**, and then click the Job Queue Manager link.

For each Job Queue, the page displays the status, the number of queued jobs, the number of active jobs, the maximum number of active jobs for the queue, the priority of the Job Queue, if the Job Queue is the default queue, and what Managed File Transfer System is running the Job Queue (when Managed File Transfer is running in a clustered environment).

Job Queues can be held within the Job Queues Manager page, which stops jobs from being released (for execution) from the Job Queue. Holding a Job Queue is especially important if problems need to be fixed before more jobs execute, or if you need to temporarily give other Job Queues the chance to run their jobs first.

Page Toolbar

The following actions are available from the page toolbar:

- Create a new Job Queue clicking the **Add Job Queue** button.
- Update the Job Queue list by clicking the **Refresh** button.

Job Queues Actions

The following actions are available by selecting the Actions icon:

- "Add/Edit Job Queue" on page 218 the selected Job Queue by clicking the Edit link.
  - View the "Job Queue Details" on page 220 page by clicking the View Properties link.
  - Delete a Job Queue by clicking the icon. The Job Queue must be held and cannot contain any active, queued, or scheduled jobs.
  - Hold all jobs in a Job Queue from processing by clicking the Hold Queue link.
  - Release held jobs in a Job Queue by clicking the Release Queue link. Managed File Transfer will begin processing jobs in the released Job Queue base on its assigned priority.
  - Remove any queued jobs from the Job Queue by clicking the Clear Queued Jobs link.
- "Work with Queued Jobs" on page 220 waiting to process in a Job Queue by clicking the View Queued Jobs link.
- "Active Jobs" on page 221 processing in a Job Queue by clicking the View Active Jobs link.

Add/Edit Job Queue

A Job Queue can be created or edited using the **Add Job Queue** page. To access this page, log in as an Admin User with the **Product Administrator** role. From the menu bar select **Workflows** and then click the Job

Queue Manager link. To create a new Job Queue, click the  Add Job Queue link in the page toolbar. To edit an existing Job Queue, click the  icon next to the Job Queue and then click the  icon.

Name

A user-defined name which identifies the Job Queue. This name should be descriptive enough so users can quickly identify this Job Queue from the list. The Name cannot exceed 20 characters. Spaces are allowed.

Default Queue

Indicates if this Job Queue is the system default. Batch jobs that are not assigned a specific queue will be placed in the default queue. This field is for display purposes only.

Description

A short paragraph that describes the Job Queue. The Description is optional and cannot exceed 512 characters.

Status

The status indicates if the Job Queue is active or inactive. An inactive Job Queue will not be processed.

Priority

The priority indicates the order in which the Job Queue will process its jobs in relation to other Job Queues. The queue priority can be a value from 1 to 10, in which jobs in a higher queue priority will be executed before jobs in a lower queue priority. For instance jobs in a Job Queue priority of 6 will be executed before jobs in a Job Queue priority of 5.

Limit Active Jobs

When enabled, a limit can be specified to restrict the number of active jobs that can be executed concurrently from this queue.

Max Active Jobs

The maximum number of jobs that can be executed concurrently from this Job Queue. When running Managed File Transfer in a clustered environment, this maximum represents the total number of active jobs across all systems. To run Jobs in sequential order in the Job Queue, specify 1 for this field.

Limit System Execution

In a clustered environment, by default, Managed File Transfer will execute Jobs in a Job Queue on the first available system. This option allows you to specify the system that will process Jobs from this Job Queue. This field is only available when Managed File Transfer is running in a clustered environment.

Execute On System

Select the System that will execute this Job Queue. This field is only available when Managed File Transfer is running in a clustered environment.

Job Queue Details

The Job Queue Details page shows details about the Job Queue. Follow the instructions below to view the details for a Job Queue:

1. Log in as a user with the Job Manager or Product Administrator role.
2. From the menu bar, select **Workflows**, and then click the Job Queue Manager link.
3. A list of Job Queues will be displayed on the page.
4. Click the  icon next to the Job Queue you want to view.
5. Click the  View Properties link to view the Job Queue Details page.
6. The Job Queue Details page appears.
7. Click the **Done** button when finished viewing the Job Queue Details.

Work with Queued Jobs

The Queued Jobs page shows any batch jobs that are waiting to execute in Managed File Transfer. For each job displayed on the Queued Jobs page, the page shows the assigned job number, the Job Queue, the name of the Project, the user who submitted the job, when the job was submitted, the queue priority and the run priority.

To view Queued Jobs, log in as a user with the Job Manager Role.

From the menu bar, select **Workflows**, and then click the Queued Jobs link.

Display Results

The number of Jobs to display in the queue. By default, the Queued Job page displays the first 20 jobs in the queue.

Job Queue

The Queued Jobs page can be filtered to display jobs processing in a specific Job Queue. The default is All.

Queue Priority

The Queue Priority (shown for each job on the page) indicates the order in which the job will leave the queue and execute. The queue priority will be a value from 1 to 10, in which jobs with a higher queue priority will be executed before jobs with a lower queue priority. For instance a job with a queue priority of 6 will be executed before a job with a queue priority of 5. Jobs with the same queue priority will be processed on a first in/first out basis.

Run Priority

The Run Priority indicates how much attention (CPU) the job will receive from Managed File Transfer when it executes. The run priority is a value from 1 to 10, in which jobs with a higher run priority will receive more attention than jobs with a lower run priority. For instance a job with a run priority of 6 will receive more attention than a job with a run priority of 5.

Functions Available

The Completed Jobs page includes functions to create, edit and view the details and logs for all completed jobs.

- Remove a job from the Queued Jobs list by clicking the icon. You can optionally delete multiple jobs by selecting the corresponding checkboxes and clicking the **Delete** button.
- View more Queued Job Actions by clicking the icon.
  More Actions
- Remove a job from the Queued Jobs list by clicking the icon.
- Edit the selected Project by clicking the Edit Project link.
- View the folder where the Project is located by clicking the View Project Folder link.

  Note: The Global Setting of "Maximum Concurrent Batch Jobs" dictates the number of batch jobs which can be executing at one time. Once the Maximum Concurrent Batch Jobs size is reached, any new batch jobs are placed in the job queue until additional slots (threads) become available.

Active Jobs

For each active Job, the Active Jobs page shows the assigned Job number, which system is executing the Job (if Managed File Transfer is running in a clustered environment), the name of the Project, the user that submitted the Job, when the Job was submitted, when the Job started executing, the Job Queue, and the priority.

The **Priority** indicates how much attention (CPU) the Job will receive from Managed File Transfer as it executes. The priority is a value from 1 to 10, in which Jobs with a higher priority will receive more attention than Jobs with a lower priority. For instance, a Job with a priority of 6 will receive more attention (CPU) than a Job with a priority of 5.

The Active Jobs page provides functions to hold active Jobs, cancel Jobs, view Job logs and view stack traces. When Managed File Transfer is running in a clustered environment, you can filter the list by selecting the system from the drop-down list.

To view the Jobs that are being executed in Managed File Transfer, log in as an Admin User with the **Job Manager** or Project Executor role.

From the menu bar, select **Workflows**, and then click the Active Jobs link.

Note:
By default, the Active Jobs page will automatically refresh every 5 seconds.

Page Toolbar

The following actions are available from the page toolbar:

- Refresh the page.

Job Queue

The Active Jobs page can be filtered to display jobs processing in a specific Job Queue. The default is All.

Active Jobs Quick Actions

- Cancel a Job by clicking the  icon.
- Hold or Pause a Job by clicking the  icon. Release the Job by clicking the  icon next to the Job.
- View more Active Job Actions by clicking the  icon.

Active Jobs Actions

The following actions are available by selecting the  Actions icon:

- Cancel a Job clicking the  icon.
- Hold or Pause a Job by clicking the  icon. Release the Job by clicking the  icon next to the Job.
- "Job Log and Details" on page 186 the current Job Log by clicking the  icon.
  - View the Job Stack Trace by clicking the  icon. This information is only needed when requested by Informatica technical support to help solve a problem.
  - Edit the selected Project by clicking the  Edit Project link.
  - View the folder where the Project is located by clicking the  View Project Folder link.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Cancel one or more selected Jobs.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Completed Jobs

This page allows you to search for jobs using a variety of criteria such as date/time range, user submitted by, status and Project name. When Managed File Transfer is running in a clustered environment, you can also filter by the system that executed the job. After typing the criteria, click the **Search** button to perform the search. If you know the job number, click the **Search by Job Number** tab, to search by job number.

To view the completed jobs in Managed File Transfer, you can log in as an Admin User with the Job Manager, Auditor or Project Executor role.

From the menu bar, select **Workflows**, and then click the Completed Jobs link.

You can also access the Completed Jobs from the Audit Logs. From the main menu bar, point to Logs and then click **Audit Logs**. Select **Completed Jobs** from the Job Logs section from the left pane. The Completed Jobs Log will appear in the right pane.

Note: A user with a Project Executor role can only work with the jobs they submitted, whereas a user with a Job Manager or Auditor role can work with all job logs.

Completed Jobs Search Tools

Search for Completed Jobs using the following search tools:

Basic Search

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The user account that was used to submit the job.

Project

The name of the Project as listed on the "Project Explorer" on page 164 page.

Folder

The location of the Project in the "Project Folders" on page 168 list on the Projects page.

Status

The outcome of the job (Successful, Failed or Canceled).

Resolution

Indicates if a failed Job was marked resolved by an Admin User.

Advanced Search

The Advanced Search provides additional search options including the Basic Search options for Completed Jobs.

User

A drop-down list provides conditions (Equals, Begins With, Ends With, or Contains) that can be used to search for a known portion of the user account name that was used to submit the job.

Project

A drop-down list provides conditions (Equals, Begins With, Ends With, or Contains) that can be used to search for a known portion of the Project name.

Folder

A drop-down list provides conditions (Equals, Begins With, Ends With, or Contains) that can be used to search for a known portion of the location of the Project in the "Project Folders" on page 168 list on the Projects page.

Job Name

A drop-down list provides conditions (Equals, Begins With, Ends With, or Contains) that can be used to search for a known portion of the name that identifies the Job.

Submitted By

A drop-down list provides conditions (Equals, Begins With, Ends With, or Contains) that can be used to search for a known portion of the user or feature that invoked the Job.

DX Endpoint Name

A drop-down list provides conditions (Equals, Begins With, Ends With, or Contains) that can be used to search for a known portion of the name that identifies the endpoint that triggered a job.

The DX endpoint name appears blank in the grid if Data Exchange does not trigger the job.

Submitted From

A drop down list of Workflow features that can invoke a Job (Administrator UI, Scheduler, Trigger, Monitor, API-INFAMFTCMD, API-RunProject).

Search by Job Number

Job Number

A unique job number given to each Project at runtime.

Completed Jobs Actions

The following actions are available by selecting the Actions icon:

- "Job Log and Details" on page 186 the Job Details by clicking the icon.
- "Job Log and Details" on page 186 the Job Log by clicking the icon.
  - Edit the selected Project by clicking the Edit Project icon.
  - View the folder where the Project is located by clicking the View Project Folder icon.
  - Resolve a failed Job by clicking the Resolve icon.
  - View or Add Job Notes by clicking the Notes icon.
- "File Audit Log" on page 690 the File Audit Log by clicking the View File Activity icon.
  - View the Submitted By detailed information by clicking the View Submitted By icon.

Table Navigation Tools

The following table navigation tools are available:

- "Job Log and Details" on page 186 the Job Log by clicking the Job Number link.
  - View the Project by clicking the Project Name link.
  - View the Project Folder by clicking the In Folder link.
  - View detailed information on the source of the submitted job by clicking the Submitted By link.
  - Click the **Previous** button to move back to the previous page of results.
  - Click the **Next** button to move forward to the next page of results.
  - Select the number of Rows to display on each page.
  - Click the **Export Results** button to save the results from all pages to a .CSV file on your local computer.
  - Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.

    Note: The default saved Job Log file name is "JobLogsYYYYMMDD.csv" (where YYYYMMDD is the current year, month, and day).
  - Click the **Columns** button to select which Completed Jobs properties are displayed in the table. The following properties are available:
  - Job Number - A unique job number given to each Project at runtime.
  - System - The system that executed the job.
  - Project Name - The name of the Project as listed on the "Project Explorer" on page 164 page.
  - In Folder - The location of the Project in the "Project Folders" on page 168 list on the Projects page.
  - Status - The outcome of the job (= Successful, = Failed or = Canceled).
  - Run User - The user account that was used to submit the job.
  - Start Time - The date and timestamp of when the job started executing.
  - End Time - The date and timestamp of when the job completed.
  - Time - The amount of time the job took to complete (in seconds).

- Submitted By - Displays the details of the user or feature that invoked the Job.
- DX Endpoint Name - Displays the name of the DX endpoint that triggered the Job.
- Submitted From - The origin of the processed Job.
- Remarks - The system messages that were generated during the execution of the Job.
- Job Name - The name that identifies the Job.
- Job Queue - The name of Job Queue where the Job was executed.
- Submit Time - The time the Job was submitted.
- Mode - The Job run mode.
- Queue Priority - The order in which the Job Queue was processed in relation to other Job Queues.
- Run Priority - The order in which the Job was processed in relation to other Jobs.
- Resolved - Indicates if a failed Job was marked resolved by an Admin User.
- Resolved On - The date the failed Job was marked resolved.
- Resolved By - The Admin User who marked the failed Job as resolved.
- Job Notes - The notes added by an Admin User.

CHAPTER 5

Task Reference

Listed below is a summary of the tasks that are available for building Projects in Managed File Transfer. These tasks are grouped by category. Click any task for more details.

Application Tasks

"Open MQ Session Task" on page 236	Opens a Message Queue Session with the MQ Server.
"MQ Retrieve Message Task" on page 238	Retrieves messages from the MQ Server.
"MQ Send Message Task" on page 240	Sends messages to the MQ Server.
"MQ Commit/Rollback Task" on page 243	Commits messages before the MQ Session is closed.
"Close MQ Session Task" on page 245	Closes the Message Queue Session with the MQ Server.
"Execute Native Command Task" on page 246	Executes a command (for example, executable, script, etc.) that is locally accessible by Managed File Transfer.
"Execute SSH Command Task" on page 249	Connects to a remote server using SSH.

Custom Tasks

Tasks listed in the Custom Tasks section are managed on the "Custom Tasks" on page 775 page.

File Compression Tasks

"Compress and Send a File with SSH Authentication" on page 254	Compresses one or more files together using the ZIP standard.
"Decompress the File with SSH Authentication" on page 256	Decompresses a ZIP file.
"Tar Task" on page 259	Packages several files together using the TAR standard (can optionally compress the files with GZIP).
"Untar Task" on page 261	Unpackages a TAR file.
"GZip Task" on page 263	Compresses a single file using the GZIP standard.
"GUnzip Task" on page 265	Decompresses a GZIP file.

Database Task

"SQL Task" on page 267	Runs SQL statements against a database server, which is useful for retrieving rows (records) from tables (physical files) or performing updates, inserts, etc.

Data Translation Task

"Read CSV Task" on page 272	Reads and parses the contents of delimited text (CSV) files.
"Write CSV Task" on page 278	Writes data into a delimited text (CSV) formatted file.
"Read Excel Task" on page 282	Reads and parses the contents of Excel documents.
"Write Excel Task" on page 287	Writes data into an Excel document.
"Password Protect Excel" on page 298	Password protects an Excel document.
"Read Fixed-width Task" on page 301	Reads and parses the contents of Fixed-width text files.
"Write Fixed-width Task" on page 306	Writes data into a Fixed-width text formatted file.
"Read Flat File Task" on page 311	Reads and parses the contents of flat files.
"Read XML Task" on page 313	Reads and parses the contents of XML documents.

"Write XML Task" on page 318	Writes data into an XML document.
"Modify RowSet" on page 329	Modifies the contents of a RowSet.

Email Task

"Retrieve Email Task" on page 346	Retrieves email (based on filter criteria) and processes any file attachments.
"Send Email Task" on page 340	Sends email to one or more recipients (with optional file attachments).

File Encryption Tasks

"PGP Decrypt Task" on page 351	Decrypts OpenPGP files.
"PGP Encrypt Task" on page 354	Encrypts files using *OpenPGP* encryption.
"PGP Sign Task" on page 358	Embeds a *Digital Signature* into a file.
"PGP Verify Task" on page 362	Verifies a Digital Signature that is embedded in a file.

File System Tasks

"Copy Task" on page 364	Copies one or more files either into the same directory (with different names) OR into another directory.
"Move Task" on page 367	Moves one or more files from one directory to another directory.
"Delete Task" on page 369	Deletes one or more files from a directory.
"Rename Task" on page 370	Renames one or more files in a directory.
"Make Directory Task" on page 372	Creates a new directory (folder).
"Search and Replace Task" on page 373	Searches for a string in a file and replaces it with a new value.

"Merge Files Task" on page 377	Merges the content of two or more files into a single file.
"Create File List Task" on page 380	Builds a list of files based on filter criteria (for example, wildcards, size, date). This "file list" can then be used in other tasks.

File Transfer Protocol Task

"FTP Task" on page 381	Connects to a FTP server for sending/retrieving files.
"FTPS Task" on page 397	Connects to a FTPS (FTP over SSL) server for sending/retrieving files.
"SFTP Task" on page 413	Connects to a SFTP (SSH File Transfer Protocol) server for sending/retrieving files.
"SCP Task" on page 427	Connects to a SCP (FTP over SFTP) server for sending/retrieving files.
"Close Session Task" on page 432	Closes an open SFTP, SCP, or SSH session.

Job Control Task

"Call Module Task" on page 433	Calls a second *Module* within a Project.
"Call Project Task" on page 434	Calls another Project located in the same installation of Managed File Transfer.
"Call Remote Project Task" on page 437	Calls another Project located on a different (remote) installation of Managed File Transfer.
"Exit Module Task" on page 439	Exits a module at the specified location if a condition evaluates to true. If the module is a secondary module, the project returns to where the module was called.
"Exit Project Task" on page 440	Exits a Project at the specified location if a condition evaluates to true.

Miscellaneous Task

"Close RowSet Task" on page 442	Manually closes a RowSet to release database locks.
"Workspaces" on page 160	Creates a directory (unique to a job) for temporarily storing files. Read more details in the "Workspaces" on page 160 section.

"Workspaces" on page 160	Deletes the Workspace directory for the job.
"Deny Trigger Event Task" on page 445	Can be used to prevent a MDN Receipt from being sent from the AS2 service, to stop a Secure Mail from being sent, or to reject a new file from being uploaded into Shared Drive.
"Print Task" on page 452	Writes user-specified text into the job log.
"Raise Error Task" on page 456	Generates an error in the Project, which can be used to abort the job or route control to another module.
"Set Variable Task" on page 457	Assigns a new value to a Variable. Read more details in the "Variables" on page 111 section.
"Dates, Times and Timestamps" on page 144	Initializes system variables or user-defined variables to the current date, time or timestamp. Read more details in the "Dates, Times and Timestamps" on page 144 section.
"Notify Consumer Task" on page 452	Sends a custom notification to consumer.

MLLP Tasks

"MLLP Task" on page 232	Send the selected acknowledgement type for an MLLP message sent by the MLLP resource.
"MLLP Ack Task" on page 235	Send the selected acknowledgement type for an MLLP message received by the MLLP service.

Report Tasks

"Reports" on page 462	Produces a variety of reports including audit log activity, analytics and management information in PDF format.

Web Task

"AS2 Servers Resource" on page 72	Sends messages to an AS2 server. AS2 messages are MIME formatted, but sent via HTTP(S)
"Informatica HTTPS Server Resource" on page 96	Posts and Gets data from the secure HTTPS server in the Managed File Transfer module.
"HTTP Servers Resource" on page 81	Posts and Gets data from a HTTP server (for example, web site).
"HTTPS Servers Resource" on page 83	Posts and Gets data from a secure HTTPS server (for example, web site) using *SSL*.
"ICAP Resource" on page 87	Sends files to an ICAP server to be scanned for data loss prevention or viruses.

Application

Application tasks allow you to connect to other systems to execute Massage Queue transfers, IBM i commands, or native system commands.

MLLP Task

Define the following properties for the MLLP Task:

Basic Tab

Label

Provide a name for this task.

MLLP Server

Select a pre-configured MLLP server from the list.

Source File

Specify the file name and path for the file to be sent. A file name is required.

Source File Variable

Specify the name of a variable of type File List that contains the files to send to the MLLP server, for example $(variableName).

Advanced Tab

Input Connection ID

Specify the name of the variable used in a MLLP task. The connection is re-used and no new connection is created.

Output Connection ID

Specify the name of the variable obtained by the first MLLP task. The variable stores the MLLP connection information.

Note: For persistent connections, add the output connection ID of the initial task as the input connection ID for the consecutive tasks.

Response Tab

Destination

The queue on the MLLP server that will hold the information. The following options are available:

- Joblog: The synchronous response will be saved to the job log.
- File: The synchronous response will be saved to the file specified in the Response File attribute.
- Discard: The response will be discarded.

File

Specify the name of the file to which the response, if any, should be saved. This is required if the Destination attribute is set to File.

When File Exists

Select the action to take when the specified file already exists.

Default Value: rename

Fail Job if Not AA/CA

Specify if to fail the job if the acknowledgement type received for a message to the MLLP server is not Application Accept (AA) or Commit Accept (CA).

Default: Yes

Retry if AR/CR

Specify if to retry the job if the acknowledgement type received is Application Reject (AR) or Commit Reject (CR).

Default: No

Message Retry Attempts

Specify the number of message retry attempts where the response cannot be Application Accept (AA) or Application Error (AE) on the first attempt.

Default: 0

Message Retry Interval

Specify the length of time in seconds between message retry attempts.

Default: 0

Output Variable Tab

Output Variable

Specify the name of the variable that will contain an MLLP server response for the variable.

MLLP Server Tab

Basic Section Properties

Use these options to configure the connection properties to an MLLP Server. If using an MLLP Server resource, these attributes can be used to override properties defined in the resource.

Host

Specify the host name or IP address of the MLLP Server. This is needed if an MLLP resource was not specified or to override the host name specified for the MLLP resource.

Port

Specify the port number to connect to.

Default: 2575

Connection Section Properties

Response Timeout

Specify the maximum amount of time to wait in seconds from the moment the response from the MLLP server is received after sending the message. A timeout value of zero is interpreted as an infinite timeout.

Default: 30

Connection Timeout

Specify the maximum amount of time to wait in seconds to establish a connection to the MLLP server. A timeout value of zero is interpreted as an infinite timeout.

Default: 30

Connection Retry Attempts

Specify the number of times to retry the connection if not established on the first try.

Default: 0

Connection Retry Interval

Specify the number of seconds to wait between each retry attempt.

Default: 0

Proxy Section Properties

Specify the following options if MLLP connections from this server require the use of a proxy server. If there is direct access to the MLLP Server, leave these options blank.

Proxy Type

Select the type of proxy server you would like to use to connect to the target server. If left blank and a proxy host is specified, this value will default to a proxy type of HTTP.

Default: http

Host

Specify the host name or IP address of the proxy server. This is required if your system uses a proxy server to make HTTP/HTTPS connections.

Alternate Host

Specify an alternate host name or IP address of the proxy server.

Port

Specify the port number on which the proxy server is listening.

Default: 80

User

Specify the user name or login name if the proxy server requires authentication.

Password

Specify the password for the proxy server.

Is Password Encrypted?

Specify if the proxy server password is in encrypted form.

Control Tab

Log Level

Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug.

Default Value: Inherited from parent Module.

Execute Only If

Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.

Disabled

Whether or not this task is disabled.

Default Value: false

On Error Tab

On Error

Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true).

Default Value: Inherited from parent Module

MLLP Ack Task

Define the following properties for the MLLP Ack Task:

Basic Tab

Label

Provide a name for this task.

Ack Type

Select the MLLP acknowledgement type for received MLLP messages.

Error Message

Define an optional error message to be sent if the acknowledgement type is Commit Error (CE) or Commit Reject (CR).

Control Tab

Log Level

Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug.

Default Value: Inherited from parent Module.

Execute Only If

Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.

Disabled

Whether or not this task is disabled.

Default Value: false

On Error Tab

On Error

Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true).

Default Value: Inherited from parent Module

MQ Tasks

Message Queue tasks allow Managed File Transfer to integrate with messaging servers to send and retrieve messages from queues and topics. Messages received by Managed File Transfer can be used by subsequent tasks to provide information or set variable values that can initiate additional processes. Messages sent by Managed File Transfer can facilitate information or processes in other applications.

Open MQ Session Task

The Open MQ Session task creates a connection to a Message Queue (MQ) server and stores a reference to this connection using the Session ID output variable. This variable can then be used in subsequent MQ related tasks for sending and retrieving messages. It is recommended to place a Close MQ Session Task in the Project when a connection is no longer needed.

By default, transactional processing of messages is not enabled. This means that the MQ server will commit the changes as soon as a message is sent or retrieved. If sending or receiving more than one message on a given session, the Session Type can be set to transacted. In transacted mode, the MQ server will only commit the changes if the Commit attribute is set to true on the Close Session or Commit/Rollback Session tasks. For example, if the MQ Send Message Task was in a loop and an error occurred trying to send the second message, the first message would be ignored by the MQ server.

Example 1: Open MQ Session

Follow the steps below to add an Open MQ Session Task to a Project for establishing a connection with an MQ server:

1. From within the Project Designer page, navigate to the **Application** > **MQ** folder in the Component Library, and then drag the Open MQ Session task to the Project Outline.
2. On the Basic tab of the Open MQ Session task, specify values for the following attributes:

MQ Server

Select an MQ server resource from the drop-down list or click the **Create** button to create an MQ server resource.

Session ID

This is the variable used by other MQ related tasks to refer to the open MQ session.

3. Click the **Save** button when finished.

Open MQ Session Task

The Open MQ Session task creates a connection to a Message Queue Server.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
MQ Server	Select a pre-configured MQ server from the drop down list.
Session ID	Specify an ID for this MQ Session. A variable with the specified session ID will be created. The session ID can be referenced in the subsequent MQ related tasks such as MQ Send Message or MQ Close Session.
Session Type	Specify the type of session to create. Default Value: normal
MQ Server Tab	
Refer to the "MQ Servers Resource" on page 89 page for the FTP Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

MQ Retrieve Message Task

The MQ Retrieve Message task retrieves all available messages from a queue or topic. Messages are retrieved through an existing MQ connection, which was created by the "Open MQ Session Task" on page 236.

The MQ Retrieve Message task can be placed in a "Loops" on page 148 to re-check for new messages over the same open session. If you only want to retrieve messages meeting specific criteria based on their headers and property settings, use the "MQ Message Filters" on page 836 field on the Advanced tab.

The number of messages to retrieve can be limited by specifying a Retrieve Limit value on the Advanced tab.

The details (for example, the message properties, ID, priority, etc.) for each retrieved message can be stored in the Processed Messages output variable, on the Output Variables tab. This variable also stores the "File Paths" on page 161 locations of where the message bodies were saved. The Processed Messages variable can then be used in a "For-Each Loop" on page 152 loop to process each message individually. Refer to the "MQ Message List" on page 124 for more information.

The Output Files variable, on the Output Variables tab, relates to the message body content. Use the Output Files variable to pass the file path locations of where the message bodies were saved to a task that will transfer them to a different location. (for example, a Copy, Move or FTP Put Task).

Example 1: MQ Retrieve Message

Follow the steps below to retrieve messages on the MQ server and save them locally:

1. From within the Project Designer page, navigate to the **Application** > **MQ** folder in the Component Library, and then drag the MQ Receive Message task to the Project Outline.
2. On the Basic tab of the MQ Receive Message task, specify values for the following attributes:

   Session ID

   The Session ID variable created in the Open MQ Session Task containing the MQ session connection information.

   Source Name

   The queue or topic name on the MQ server from which the messages will be retrieved.

   Source Type

   In this example the message is being retrieved from a queue on the MQ server.

   Output Directory

   The "File Paths" on page 161 where the messages will be saved. Type the file path or click the  icon to browse for a file path location.

   Output File Name

   It is recommended to use the Current Message Variable's ID in the file name (for example, ${MQMessage:id}.dat) to ensure that all retrieved messages are stored with unique file names.
3. Click the **Save** button when finished.

MQ Retrieve Message Task

The MQ Retrieve Message task retrieves all available messages from a queue or topic.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Session	Specify the reference to a valid MQ Session that was created using the Open MQ Session task (e.g. ${MQSession}).
Source Name	Specify the name of queue or topic from which message(s) should be retrieved.
Source Type	Select the type of source. Default Value: queue
Topic Subscription	Specify the subscription ID for the topic. This is typically provided by your MQ server administrator. This is required if the specified Source Type is topic.
Current Message Variable	Specify the name of a variable to which the current message should be assigned. This can be used for example, to save the payload to a file using the message ID as the file name.
Output Directory	Specify the directory to which the retrieved messages, if any, should be saved.
Output Files Name	Specify the name of the file to which the retrieved messages, if any, should be saved. You can use the Current Message Variable to name the file using one or more attributes of the retrieved message.
When File Exists	Select the action to take when the specified output file already exists. Default Value: rename
Advanced Tab	
Message Filter	Specify the filter criteria to use when retrieving messages. If a filter is specified, only messages that match the filter criteria are retrieved. Refer to the Help for more information on how to specify the filter criteria.
Timeout (Seconds)	Specify the number of seconds to wait for the availability of the message. Default Value: -1 (no wait time)
Retrieve Limit	Specify the maximum number of messages to be retrieved. A value of zero indicates that all available messages will be retrieved. Default Value: 0
Output File Encoding	Specify the encoding or character set to use when saving the message to the output file. This option is used if and only if the type of message is determined to be text. Default Value: The platform's default file encoding.
Output Variables Tab	
Output Files Variable	If desired, specify the name of a variable which will contain the file(s) that were saved to the output directory. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Processed Messages Variable	Specify the name of a variable to which all the retrieved messages should be assigned.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

MQ Send Message Task

The Message Queue (MQ) Send Message task sends a message to a queue or topic. Messages are sent over an existing connection, which was created by the "Open MQ Session Task" on page 236. Additional properties can be added to the message by adding one or more Property Elements to the task.

This task can be called repeatedly within a Project to send multiple messages over the same session.

Example 1: MQ Send Message

Follow the steps below to send a message to a queue on the MQ server and add a Property to aid in sorting the queue list:

1. From within the Project Designer page, navigate to the **Application** > **MQ** folder in the Component Library, and then drag the MQ Send Message task to the Project Outline.
2. On the Basic tab of the MQ Send Message task, specify values for the following attributes:

   Session ID

   The Session ID variable created in the Open MQ Session Task containing the MQ session connection information.

   Destination Name

   The queue or topic name on the MQ server that will hold the message.

   Destination Type

   In this example, the message is being sent to a queue on the MQ server.

Message Text

The content of the message sent to the recipient. Variables can be used to place values in the message text.

3. Click the **Add** button in the sub-menu and select the Add Property menu item.
4. On the Basic tab of the Message Properties element, specify values for the following attributes:

   Name

   The name of the Message Property.

   Value

   The distinct characteristic that will help group and sort the message.

5. Click the **Save** button when finished.

MQ Send Message

The Message Queue (MQ) Send Message task sends a message to a queue or topic.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Session ID	Specify the reference to a valid MQ Session that was created using the Open MQ Session task (e.g. ${MQSession}).
Destination Name	Specify the name of queue or topic to which the message should be sent.
Destination Type	Select the type of destination. Default Value: queue
Message File	Specify the file whose contents should be sent as the message's payload. It is not allowed to specify both Message File and Message Text.
Message Type	Select the type of message. If the file is a text file, choose text, otherwise, choose bytes. Default Value: bytes
Message File Encoding	Specify the encoding or character set of the message file. This option is used only if the message type is set to text. Default Value: The platform's default file encoding.
Message Text	Specify the text to be sent as the message's payload. It is not allowed to specify both Message File and Message Text. Furthermore, when Message Text is specified, the message type is always assumed to be text.
Advanced Tab	
Delivery Mode	Select the mode in which the message should be delivered. Default Value: persistent

Priority	Specify the priority for the message. Valid values are 0 through 9, with 0 being the lowest priority, and 9 being the highest. Default Value: 4
TTL (Time to Live)	Specify how long the message should be kept at the destination before it is marked as expired. A value of zero means that the message lives forever (or until the message is consumed by a consumer). Default Value: 0
TTL Unit	Select the time unit for the TTL. Default Value: days
Correlation ID	Specify the ID of the message to which the message being sent is related, if any.
Reply To	Specify the name of the queue or topic to be set in the Reply-To header field. If sending a message to a queue, the value specified here is also assumed to be a queue. If sending the message to a topic, the value specified here is also assumed to be a topic.
Output Variables Tab	
Sent Message Variable	If desired, specify the name of a variable which will contain an MQMessage variable. It will be created if it does not exist, or overwritten otherwise.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Property

The Property Element of the MQ Send Message task provides additional header information, like a tag, that can be used by the Message Queue (MQ) server or the recipient to sort messages as they arrive. The Property

Element can contain user supplied text or use variables to provide the information required for the message header.

Add a Property Element to an MQ Send Message Task by clicking the **Add** button in the sub-menu and selecting the **Add Property** option.

<table>
<tr><th>Field</th><th>Definition</th></tr>
<tr><td>Basic Tab</td><td></td></tr>
<tr><td>Name</td><td>Specify or select the name of the property. The name of the property to specify need not exist in the dropdown.</td></tr>
<tr><td>Type</td><td>The data type indicates the type of data specified in the Value field. The default value is string.
Valid data Types:
<table><tr><td>int</td><td>A numerical value in the range of -2,147,483,648 to 2,147,483,647</td></tr><tr><td>long</td><td>A numerical value in the range of -9,223,372,036,854,775,808 to 9,223,372,036,854,775,807</td></tr><tr><td>boolean</td><td>A value of true or false</td></tr><tr><td>string</td><td>A value or variable containing characters and integers</td></tr><tr><td>short</td><td>A numerical value in the range of -32,768 to 32,767</td></tr><tr><td>byte</td><td>A small numerical value in the range of -128 to 127</td></tr><tr><td>float</td><td>A floating point number</td></tr><tr><td>double</td><td>A double precision floating point number</td></tr></table></td></tr>
<tr><td>Value</td><td>Specify the value for the property.</td></tr>
</table>

MQ Commit/Rollback Task

If the Session Type in the "Open MQ Session Task" on page 236 task is set to Transacted when a session is opened, none of the messages in the queue are transacted until the session is closed. The MQ Commit/Rollback task provides the ability to commit a message or roll it back, in the case of an error, before the session is closed.

The MQ Commit/Rollback task is useful if processing messages in a Loop. It can manually process messages at a set point in the Loop or if in the event of an error, it can rollback all messages received since the last successful commit.

Note: Using the MQ Commit/Rollback task will produce an error if the Session Type in the "Open MQ Session Task" on page 236 task is set to Normal. The normal session type auto-commits each message as it is processed.

Example 1: MQ Commit/Rollback

Follow the steps below to add a MQ Commit/Rollback task to a Project for manually committing messages:

1. From within the Project Designer page, navigate to the **Application** > **MQ** folder in the Component Library, and then drag the MQ Commit/Rollback task to the Project Outline.
2. On the Basic tab of the Commit/Rollback MQ task, specify values for the following attributes:

   Session ID

   The variable used by other MQ related tasks to refer to the open MQ session.

   Commit Session

   Indicates whether sent or received messages are committed on the MQ Server.
3. Click the **Save** button when finished.

MQ Commit/Rollback Task

The MQ Commit/Rollback Session task provides the ability to commit a message or roll it back, in the case of an error, before the session is closed.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Session ID	Specify the reference to a valid MQ Session that was created using the Open MQ Session task (e.g. ${MQSession}).
Commit Session	Specify whether or not to commit the changes that were made in this session. A value of true will commit the changes. A value of false will rollback the changes. Attempting to use this task in a normal session (non-transacted session) will result in an error. Default Value: true
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Close MQ Session Task

The Close MQ Session task closes an MQ session that was opened using the Open MQ Session task.

Example 1: Close MQ Session

Follow the steps below to close an MQ Session:

1. From within the Project Designer page, navigate to the **Application** > **MQ** folder in the Component Library, and then drag the Close MQ Session task to the Project Outline.
2. On the Basic tab of the Close MQ Session task, specify the Session ID value:

   Session ID

   The open Session ID that will be closed.
3. Click the **Save** button when finished.

Close MQ Session Task

The Close MQ Session task closes an MQ session that was opened using the Open MQ Session task.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Session ID	Specify the reference to a valid MQ Session that was created using the Open MQ Session task (e.g. ${MQSession}).
Commit Session	Specify whether or not to commit the changes that were made in this session. A value of true will commit the changes. A value of false will rollback the changes. This option is ignored if the session is a normal (non-transacted) session. Default Value: true
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.

Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Native Call Tasks

Native call tasks can call commands or execute programs on the system where Managed File Transfer is installed.

Execute Native Command Task

Native commands can be executed on the system on which Managed File Transfer is running. For instance, on Windows platforms, this task could run batch (.bat) and executable files. On Linux and Unix platforms, this task could run shell scripts.

One or more arguments can be passed to the command as Variables or constant values.

By default, this task will wait for the command to return control back to Managed File Transfer before proceeding with the next task. If you want the *Project* to continue processing without waiting for the command to finish, then the **Spawn** attribute should be set to true.

Example 1: Execute Native Command

Follow the steps below to run a batch file on a Windows machine:

1. From within the Project Designer page, navigate to the **Application** > **Native Calls** folder in the Component Library, and then drag the Execute Native Command task to the Project Outline.
2. On the Basic tab of the Execute Native Command task, specify the Executable value:

   Executable

   The "File Paths" on page 161 and name of the executable command, program, or script to execute.
3. Click the **Save** button when finished.

Example 2: Execute Native Command with an Argument

Follow the steps below to pass an Argument to a batch file on a Windows machine:

1. From within the Project Designer page, navigate to the **Application** > **Native Calls** folder in the Component Library, and then drag the Execute Native Command task to the Project Outline.
2. On the Basic tab of the Execute Native Command task, specify the Executable value:

   Executable

   The "File Paths" on page 161 and name of the executable command, program, or script to execute.
3. Click the **Add** button and select the Add Argument menu item.

4. On the Basic tab of the Add Arguments element, specify a value for the argument. The value can be string text or an "Expressions" on page 125.
5. Click the **Save** button when finished. When the batch file is executed, the value of the argument will be supplied to the batch script.

Example 3: Execute Native Command using Variables and Arguments on Unix

In this example, a variable will be used to store a directory location. When the Unix 'ls' command is executed, Arguments will pass in a command parameter as well as the directory location variable to the command.

1. From within the Project Designer page, right click on the Project module and select **Add a Variable**.
2. On the Basic tab of the variable element, specify the following fields:

   Variable Name

   Specify a name for this variable. The name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores(_) and periods(.).

   Value

   Specify the initial value for this variable.
3. From within the Project Designer page, navigate to the **Application** > **Native Calls** folder in the Component Library, and then drag the Execute Native Command task to the Project Outline.
4. On the Basic tab of the Execute Native Command Task, specify the Executable value:

   Executable

   Specify the command to execute.
5. Click the **Add** button and select the Add Argument menu item.
6. On the Basic tab of the Add Arguments element, specify a value for the argument. The value can be string text or an "Expressions" on page 125.
7. Click the **Add** button and select the Add Same menu item to add another Argument.
8. On the Basic tab of the Add Arguments element, specify the variable created in Step 2 above.
9. Click the **Save** button when finished. When the Project is executed, Managed File Transfer will execute the
   "ls -l /home/linoma" command on the Unix operating system where it is installed.

Execute Native Command Task

The Execute Native Command task allows you to execute a command, program, or script on the system Managed File Transfer is running.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Executable	Specify the directory location and name of the executable command, program, or script to execute.

Working Directory	Specify the directory that the executable will use as the working directory.
Advanced Tab	
Spawn	Specify whether or not to spawn a separate process to run the executable and finish normally. Default Value: false
Timeout	Specify the duration (in seconds) to allow the executable to run. Specify only when the executable is not spawned and needs a time limit. If the timeout duration is reached, the executable process will be destroyed and an error will be thrown. A value of 0 (zero) indicates an infinite timeout. Default Value: 0
Input File	Specify the path and name of the input file that will be fed to the executable as standard input.
Redirect Output To	Specify where the standard output from the executable, if any, will be directed. Default Value: joblog
Output File	Specify the path and name of the file that the standard output will be written to if the redirectOutputTo attribute is set to 'file'.
When Output File Exists	Specify the action to take when an output file already exists. The default value is 'rename' which changes the output file to a new name so the existing file remains untouched. Default Value: rename
Clear Environment	Specify whether or not to clear all currently set environment variables before running the executable. Default Value: false
Error if Executable Fails	Specify whether or not to throw an error when a non-zero return code is received from the completed executable. Default Value: true
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the output file created by this executable. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Return Code Variable	If desired, specify the name of a variable which will contain the return code of the completed executable. The variable may be used in subsequent tasks.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Argument

The Argument element allows you to specify a parameter used by programs called from the Execute Native Commands task.

Field	Definition
Basic Tab	
Value	Specify an argument or parameter to be used by the executable.

Environment Variable

The Environment Variable element allows you to set the value of existing environment variables on the system running Managed File Transfer.

Field	Definition
Basic Tab	
Name	Specify a value for this environment variable.
Value	Specify a name for this environment variable.

Execute SSH Command Task

SSH commands can be executed from Managed File Transfer on a remote server.

Session Persistence

By default, when the Execute SSH Command task is finished, the connection with the server (session) will be disconnected and closed. When using an Execute SSH Command task in a Loop or as part of a multi-step workflow, the SSH session can be kept open and reused rather than closing and reopening the session for each Execute SSH Command task to the same server. To keep a session open or to hand off the open session to the next Execute SSH Command task in a Project, use the Input Session ID and Output Session ID variables on the Advanced tab of the Execute SSH Command task. If this is the first SSH session in the Project and other tasks will use this connection, only specify the Output Session ID (for example, SSHSession). The next task that uses the session would specify ${SSHSession} in the Input Session ID field. When no additional tasks in the Project need the open session, it should be closed using the "Close Session Task" on page 432 (using the Session ID value of ${SSHSession}).

SOCKS, HTTP, and Informatica Managed File Transfer Proxy

Managed File Transfer connects to a proxy server as a client and the proxy server redirects the traffic to the target SSH server. Proxy settings for SSH connections are defined at the "SFTP Servers Resource" on page 66 level or per Execute SSH Command task. The Execute SSH Command task can use SOCKS, HTTP, or Managed File Transfer Gateway proxy protocols when making a connection to a proxy server. The SOCKS connection in Managed File Transfer supports both version 4 and 5. The HTTP proxy, otherwise known as an HTTP tunneling proxy, provides an HTTP tunnel through which a transport can be established. When using a proxy server, obtain the correct proxy type and connection credentials from the proxy server administrator.

Host Key Fingerprints

For added authentication, Host Key Fingerprints can be used by the client (Managed File Transfer), to verify the authenticity of the host SSH server. If, when connecting to the SSH server, the host key fingerprint entered into Managed File Transfer DOES NOT match the fingerprint on the server's private key, Managed File Transfer will error out saying it does not trust the target server. This is to prevent connecting to the wrong server in a case where someone is trying to spoof the IP of the SSH server in question resulting in the data going to a wrong and most likely malicious destination. Follow the steps below to add Host Key Fingerprint verification to a SSH Task:

1. Contact the administrator of the host server to which the Managed File Transfer Execute SSH Command task is connecting.
2. Ask them for the Fingerprint of the Private Key used in the SSH session.
3. On the Execute SSH Command page, click the **SSH Server** tab, open the SSH Keys fold and then type the fingerprint in the Host Key field.

SSH Algorithms

The options on the Algorithms fold allow customization of the supported algorithms for each SSH connection. The entries in the left column are the available algorithms and the entries in the right column are the selected algorithms. By selecting one or more algorithms, only those will be used during the SSH communication. If no algorithms are selected for a section, the defaults will be used. The Default Algorithms are listed on the Algorithms tab on the "SFTP Servers Resource" on page 66.

During the handshake process, the selected options are negotiated with the server, starting with the entry at the top of the list. The first cipher and mac and compression algorithms to match an algorithm supported by the server will be used for the connection. If your company prefers certain algorithms over others, use the arrow buttons to move that cipher to the Selected column and to set the order with the most preferred algorithm at the top. Press the CTRL key while clicking to select multiple entries.

Example 1: Execute SSH Command

Follow the steps below to execute an SSH command that returns the file name and sizes for all files in a home directory and saves the output to a file:

1. From within the Project Designer page, navigate to the **Application** > **Native Calls** folder in the Component Library, and then drag the Execute SSH Command task to the Project Outline.
2. On the Basic tab of the Execute SSH Command task, specify the SSH Server and Command:

   SSH Server

   Select a pre-configured SSH server from the drop-down list.

Command

Specify the command to execute on the remote system.

3. On the Advanced tab, specify where the output of the command will be redirected to:

Redirect Output To

Specify where the standard output from the command, if any, will be directed. By default, the output will be written to the job log.

Output File

Specify the output file path and name of where you want the output written to. This is required when redirecting output to a file.

4. Click the **Save** button when finished.

Example 2: Execute SSH Command Using Environment Variables

The Execute SSH Command can pass values to Environment Variables for use in commands and scripts on the SSH server. When the task executes, the value of the environment variables will be passed to the SSH server before the SSH command is executed. The task supports the use of multiple environment variables.

Note: Environment Variable Names must be defined within the AcceptEnv keyword section of the SSHD_CONFIG file on the SSH Server. When the SSH session is opened, the SSH server passes the accepted environment variable names to Managed File Transfer. Managed File Transfer then uses the Environment Variables element to assign a value to the variable.

The following example uses the LC_NAME environment variable to pass in the value of the search attribute in the grep command. When the task executes, the SSH server will search for files that contain the name "kharris" in the /root/Public directory and then write the results to a file.

1. From within the Project Designer page, navigate to the **Application** > **Native Calls** folder in the Component Library, and then drag the Execute SSH Command task to the Project Outline.
2. On the Basic tab of the Execute SSH Command task, specify the SSH Server and Command:

SSH Server

Select a pre-configured SSH server from the drop-down list.

Command

Specify the command to execute on the remote system. Note: The "$LC_NAME" environment variable is used in the command. A value for the LC_NAME variable will be created in step 6 below.

3. On the Advanced tab, specify where the output of the command will be redirected to:

Redirect Output To

Specify where the standard output from the command, if any, will be directed. By default, the output will be written to the job log.

Output File

Specify the output file path and name of where you want the output written to. This is required when redirecting output to a file.

4. Click the **Add** button and select the Environment Variable menu item.
5. On the Basic tab of the Environment Variables element, specify values for the following attributes:

Name

A name for the environment variable.

Value

The value of the environment variable.

6. Click the **Save** button when finished.

Execute SSH Command Task

The Execute SSH Command task sends a command to an SSH server.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
SSH Server	Select a pre-configured SSH server from the drop-down list.
Command	Specify the command to execute on the remote system.
Advanced Tab	
Input Session ID	Specify the reference to a valid SSH Session that was created using the output session id of an ExecSSH task (e.g. ${SSHSession}).
Output Session ID	Specify an ID for this SSH Session. A variable with the specified Session ID will be created. The Session ID can be referenced in the subsequent ExecSSH tasks.
Redirect Output To	Specify where the standard output from the command, if any, will be directed Default Value: joblog
Output File	Specify the output file path and name of where you want the output written to. Required if Redirect Output To is file.
When Output File Exists	Specify what will happen when the output file already exists. Default Value: rename
Command Timeout	Specify the duration (in seconds) to wait for the command to execute. If the timeout duration is reached, the project will abandon the command on the server and an error will be thrown. A value of 0 (zero) indicates an infinite timeout. Default Value: 120
Error if Command Fails	Specify whether or not to error the task if the command fails. Default Value: true
Output Variables Tab	
Return Code Variable	Specify the name of a variable that will contain the return code that is returned from the command.
Output File Variable	Specify the name of a variable which will contain the output file created by this command. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.

SSH Server Tab	
Refer to the "SFTP Servers Resource" on page 66 page for the SSH Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Environment Variable

The Environment Variable element passes a value to an environment variable on an SSH server.

Field	Definition
Basic Tab	
Name	Specify a name for this environment variable.
Value	Specify a value for this environment variable.

Compression Tasks

Compression tasks are very useful when working with large amounts of data. Large files can be compressed considerably (depending on their data contents), which will save disk space and decrease transmission times.

Note: Compression tasks cannot compress or decompress files or folders located from SMB Network Shares or Encrypted Folders. Alternatively, files or folders from these resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to a SMB Network Share or Encrypted folder.

Compress and Send a File with SSH Authentication

A .ZIP file can be created to package, compress, and encrypt one or more files. .ZIP files are very useful for reducing disk space, minimizing transmission times, and for keeping related files organized together.

Note: The ZIP and UNZIP processes in Informatica Managed File Transfer have been tested for compatibility with other vendors, including PKZIP® and WinZip®. When creating a .ZIP file, a password can additionally be specified to secure the data using either standard protection or AES (Advanced Encryption Standard). This is a symmetric form of encryption, in which the same password will be used to both encrypt and decrypt the file.

Typical data can often be reduced to 1/10th of its original size. Informatica Managed File Transfer supports the zipping and unzipping of large files that can be multi-gigabytes in size.

After zipping the files with Informatica Managed File Transfer, the resulting .ZIP file can then be placed on the Local File System, distributed to a FTP server, or sent to one or more email recipients.

Compression tasks cannot compress or decompress files or folders located from SMB network shares or encrypted folders. Alternatively, files or folders from these resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to an SMB network share or an encrypted folder.

Zipping a File Using a Zip Task

Perform the following steps to add a Zip task to a Project for compressing files:

1. From within the Project Designer page, expand the Compression folder in the Component Library, and then drag the Zip task to the Project Outline.
2. On the Basic tab of the Zip task, specify values for the following attributes:

   Input File

   If you want to zip a single file, specify the file path to this file. Do not specify the file path when you use an **Input Files Variable** or a File Set.

   Input Files Variable

   If you want to zip all of the files that are contained in a File List Variable, specify the name of that variable. Do not specify the name of the variable when you use an **Input File** or a File Set.

   Output File

   The name of the zip file to create.

   When File Exists

   The action to take if a file with the same name exists in the location.
3. Specify additional attributes for the Zip task in the other tabs, for example, password, encryption method.
4. Click the **Save** button.

ZIP Task Fields

The ZIP Task compresses a file or set of files into a .ZIP file.

The following table describes the fields in the **Basic Tab** of a Zip Task:

Field	Description
Label	Specify a label for the task.
Input File	Specify the path and name of a single file to zip.
Input Files Variable	Specify a variable that contains files to be compressed. The type of the variable must be File List. For example, ${variableName}.
Output File	Specify the name and location of the output ZIP file.
When File Exists	Specify the action to take when the zipped file already exists. Default is rename. The default value changes the destination file name to a new name. Therefore, the existing file does not change.

The following table describes the fields in the **Advanced Tab** of a PGP Verify Task:

Field	Description
Password	Specify the password to use to encrypt the zip file. If you specify a password, the contents of the zipped file are encrypted and are only accessible using this password.
Is Password Encrypted?	Specify whether the above password is in encrypted form. Default is false.
Encryption Method	Specify the encryption method to use to encrypt the ZIP file. Specify the encryption method only if a password is specified. Default is standard.
Compression Level	Specify the level of compression to use. Default is medium.
Save Full Path Into	Specify whether to save the full path information in the output ZIP file. Default is false.

The following table describes the fields in the **Output Variables Tab** of a Zip Task:

Field	Description
Output File Variable	You can specify the name of a variable that contains the verified files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Processed Input Files Variable	You can specify the name of a variable that contains the signed input files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Number of Files Archived Variable	You can specify the name of a variable that contains the number of files that have been successfully archived. The variable is created if it does not exist.

The following table describes the fields in the **Control Tab** of a Zip Task:

Field	Description
Version	The version of the task.
Log Level	Specify the level of logging to use while executing this task. You can select **silent**, **normal**, **verbose**, or **debug**. The default value is inherited from the parent module.
Execute Only If	Specify the secret key ring that contains the sender's public keys. Specify the secret key ring only if no PGP key ring resource was specified or if you need to override the secret key ring specified in the PGP key ring resource.
Disabled	Whether this task is disabled. Default is false.

The following table describes the fields in the **On ErrorTab** of a Zip Task:

Field	Description
On Error	Specify the action to take when the task errors out. You can select **abort**, **continue**, **call:[module]**, or **setVariable:[name]=[value]**. When you select **call:[module]**, replace `[module]` with the name of the module in the project, for example, `call:ErrorModule`. When you select **setVariable:[name]=[value]**, replace `[name]` with a variable name and `[value]` with the variable value, for example, `setVariable:error=true`. The default value is inherited from the parent module.

Decompress the File with SSH Authentication

The Unzip task will decompress and optionally decrypt a .ZIP file. If the .ZIP file is password protected, that password should be specified in the Password attribute on the **Advanced Tab** in the Unzip Task.

Note: The ZIP and UNZIP processes in Managed File Transfer have been tested for compatibility with other vendors, including PKZIP® and WinZip®. Compression tasks cannot compress or decompress files or folders located from SMB network shares or encrypted folders. Alternatively, files or folders from the resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to an SMB network share or encrypted folder.

Unzipping a File Using Unzip Task

Perform the following steps to unzip a single file that is not password protected:

1. From within the Project Designer page, expand the Compression folder in the Component Library, and then drag the Unzip task to the Project Outline.
2. On the Basic tab of the Unzip task, specify values for the following attributes:

   Input File

   The file path and name of the file to unzip.

   Output Directory

   The file path where the contents of the ZIP file should be extracted.
3. Click the **Save** button when finished.

   Note: The Unzip Task allows for File Sets to be specified in order to process multiple .ZIP files at once. If multiple .ZIP files are specified and they are password protected then the **Password** attribute value must apply to all .ZIP files or the task will fail.

Unzip Task

The following table describes the fields in the **Basic Tab** of an Unzip Task:

Field	Description
Label	Specify a label for the task.
Input File	Specify the path and name of a single file to unzip.
Input Files Variable	Specify a variable that contains files to uncompressed. The type of the variable must be File List. For example, ${variableName}.
Output Directory	Specify the directory path to which the contents of the input ZIP files should be extracted.
When File Exists	Specify the action to take when a file being extracted already exists. The default value is rename. The default value changes the destination file name to a new name so that the existing file does not change.

The following table describes the fields in the **Advanced Tab** of an Unzip Task:

Field	Description
Password	Specify the password to use to decrypt the zip files. Specify only if the input zip files are encrypted. **Note:** When you unzip multiple encrypted ZIP files, they must have the same password. Otherwise, the task will fail.
Is Password Encrypted?	Specify whether the password is in the encrypted form. Default is false.

Field	Description
Ignore Path Information	Specify whether to ignore the path information contained in the input zip files when you extract a file. If set to true, all entries in the zip files are be extracted to the specified output directory. No sub-directories will be created even if the entries in the zip file have directory information associated with them. If set to false, all entries in the zip files will be extracted to the specified output directory. The directory information in the zip files is preserved. Default is false.
Make Base Directories	Specify whether or not a separate base directory should be created for storing the contents of each input zip file. When set to true, in the specified output directory, a sub-directory will be created for each input zip file. The directory name will be derived from the input zip file name. Default is false.
When Base Directory Exists	Specify the action to take when the base directory exists. This is applicable only when the 'Make Base Directories' option is set to true. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default is rename.
Preserve Dates	Specify whether or not the dates on the extracted files should be preserved. If set to 'true', the dates will be taken from the input zip files. If set to 'false', the dates on the extracted files will be overridden to the date and time when they are extracted. Default is true.

The following table describes the fields in the **Output Variables Tab** of an Unzip Task:

Field	Description
Output Files Variable	Specify the name of a variable that contains all the extracted files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Processed Input Files Variable	Specify the name of a variable that contains the processed input zip files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Number of Files Archived Variable	Specify the name of a variable that contains the number of files that have been successfully extracted. The variable is created if it does not exist.

The following table describes the fields in the **Control Tab** of an Unzip Task:

Field	Description
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. You can select **silent**, **normal**, **verbose**, or **debug**. The default value is inherited from the parent module.

Field	Description
Execute Only If	Specify the secret key ring that contains the sender's public keys. This is required only if no PGP key ring resource was specified or if you need to override the secret key ring specified in the PGP key ring resource.
Disabled	Whether this task is disabled. Default is false.

The following table describes the fields in the **On Error Tab** of an Unzip Task:

Field	Description
On Error	Specify the action to take when the task errors out. You can select **abort**, **continue**, **call:[module]**, or **setVariable:[name]=[value]**. When you select **call:[module]**, replace `[module]` with the name of the module in the project, for example, `call:ErrorModule`. When you select **setVariable:[name]=[value]**, replace `[name]` with a variable name and `[value]` with the variable value, for example, `setVariable:error=true`. The default value is inherited from the parent module.

Tar Task

A tar file combines one or more files into one larger file for distribution or archiving purposes.

Typically the Tar task will be used by adding a "File Lists and File Sets" on page 116 through the **Add** button. Doing so will place all files found into the **Output File** specified. When creating a tar file it is common practice to name the file with a .tar extension.

The Tar Task can also compress the output file with GZip compression. It is recommended to name a compressed tar file with a .tar.gz extension.

Note: Compression tasks cannot compress or decompress files or folders located from SMB Network Shares or Encrypted Folders. Alternatively, files or folders from these resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to a SMB Network Share or Encrypted folder.

Example 1: Tar a File

Follow the steps below to Tar and compress a list of files through the use of a File Set:

1. From within the Project Designer page, expand the Compression folder in the Component Library, and then drag the Tar task to the Project Outline.
2. On the Basic tab of the Tar task, specify the Output File value:

   Output File

   The name and "File Paths" on page 161 of the output Tar file.
3. On the Advanced tab of the Tar task, specify the Compress value:

   Compress

   Whether or not to use GZip compression when creating the Tar file.
4. Click the **Add** button in the sub-menu and select the **Add a File Set** menu item.

5. On the Basic tab of the File Set element, specify a value for the following attribute:

   Base Directory

   The starting directory for this File Set. If no filters are defined, all files in this directory will be included.

6. Click the **Save** button when finished.

   The following image illustrates the Project Outline for the Tar task:

Tar Task

The Tar task compresses a file or set of files into a .tar file.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and name of a single file to tar.
Input Files Variable	Specify a variable that contains file(s) to be compressed. The type of this variable must be File List. For example, ${variableName}.
Output Directory	Specify the name and location of the output TAR file.
When File Exists	Specify the action to take when the tarred file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Save Full Path Info	Specify whether or not to save the full path information in the output TAR file. Default Value: false
Compress	Specify whether or not to use GZip compression when creating the TAR file. Default Value: false
Output Variables Tab	
Output Files Variable	If desired, specify the name of a variable which will contain the tarred file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Archived Variable	If desired, specify the name of a variable which will contain the number of files that have been successfully archived. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Untar Task

The Untar task will extract all files in a tar file and place them into a directory. If the tar file is compressed with GZip then the **Is Tar File Compressed** attribute on the Advanced tab should be set to true.

Note: Compression tasks cannot compress or decompress files or folders located from SMB Network Shares or Encrypted Folders. Alternatively, files or folders from these resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to a SMB Network Share or Encrypted folder.

Example 1: Untar a File

Follow the steps below to extract and decompress a tar file:

1. From within the Project Designer page, expand the Compression folder in the Component Library, and then drag the Untar task to the Project Outline.
2. On the Basic tab of the Untar task, specify values for the following attributes:

   Input File

   The "File Paths" on page 161 and name of a single file to untar.

   Output Directory

   The directory path to which the contents of the input TAR files should be extracted to.
3. On the Advanced tab of the Untar task, specify the Is Tar File Compressed? value:

   Is Tar File Compressed?

   Whether or not the tar file should be decompressed using GUnzip.

4. Click the **Save** button when finished.

   Note: If you want to extract multiple files, then leave the **Input File** blank, click the  **Action** link in the sub-menu and select the **Add a File Set** menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Untar Task

The Untar task will extract files from a .tar file.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and name of a single file to tar.
Input Files Variable	Specify a variable that contains file(s) to uncompressed. The type of this variable must be File List. For example, ${variableName}.
Output Directory	Specify the directory path to which the contents of the input TAR files should be extracted.
When File Exists	Specify the action to take when a file being extracted already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Is Tar File Compressed?	Specify whether or not the tar file being untarred is compressed using GZip Default Value: false
Ignore Path Information	Specify whether or not to ignore the path information contained in the input tar file(s) while extracting. If set to true, all entries in the tar file(s) will be extracted to the specified output directory. No sub-directories will be created even if the entries in the tar file have directory information associated with them. If set to false, all entries in the tar file(s) will be extracted to the specified output directory. The directory information in the tar file(s) is preserved. Default: false
Make Base Directories	Specify whether or not a separate base directory should be created for storing the contents of each input tar file. When set to true, in the specified output directory, a sub-directory will be created for each input tar file. The directory name will be derived from the input tar file name. Default Value: false
When Base Directory Exists	Specify the action to take when the base directory exists. This is applicable only when the 'Make Base Directories' option is set to true. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Preserve Dates	Specify whether or not the dates on the extracted files should be preserved. If set to 'true', the dates will be taken from the input tar files. If set to 'false', the dates on the extracted files will be overridden to the date and time when they are extracted. Default Value: true

Output Variables Tab	
Output Files Variable	If desired, specify the name of a variable which will contain all extracted files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input tar file(s). The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Archived Variable	If desired, specify the name of a variable which will contain the number of files that have been successfully extracted. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

GZip Task

The GZip task can compress one or more files on the local file system using the GZip standard.

"File Lists and File Sets" on page 116 can be added to the GZip Task to compress multiple files, in which case it will create a compressed file for each file in the File Set, appending a .gz to each of the resulting file names.

Note: Compression tasks cannot compress or decompress files or folders located from SMB Network Shares or Encrypted Folders. Alternatively, files or folders from these resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to a SMB Network Share or Encrypted folder.

Example 1: GZip a File

Follow the steps below to GZip a single file:

1. From within the Project Designer page, expand the Compression folder in the Component Library, and then drag the GZip task to the Project Outline.
2. On the Basic tab of the GZip task, specify values for the following attributes:

   Input File

   The "File Paths" on page 161 and file name of a single file to GZip.

   Output File

   The file path and file name where the GZipped file should be saved.
3. Click the **Save** button when finished.

Note: If multiple files need to be compressed, you may consider using the "Tar Task" on page 259 to package/compress those files together into a single file.

GZip Task

The GZip task can compress one or more files on the local file system using the GZip standard.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single file to GZip.
Input Files Variable	Specify the name of a variable of type File List which contains files to GZip. For example, ${variableName}
Output File	Specify the path and file name where the GZipped file should be saved. This is not allowed when GZipping multiple files using inputFilesVariable attribute or a nested File Set element.
Output Directory	Specify the directory where the output files should be saved.
When File Exists	Specify the action to take when the GZipped file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Compression Level	Specify the compression level to use. Valid values range between 'very low' and 'maximum'. A higher compression level will cause the file(s) to be more compressed, however compression will take longer. A lower compression level will cause the file(s) to compress faster. Default Value: medium
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the GZipped files. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Processed Input Files Variable	If desired, specify the name of a variable which will contain the input files that were successfully Gzipped. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Archived Variable	If desired, specify the name of a variable which will contain the number of files compressed. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

GUnzip Task

The GUnzip task will decompress one or more files that are compressed with the GZip standard.

Either a single file can be decompressed or "File Lists and File Sets" on page 116 can be added to the GUnzip Task to decompress multiple files. If a File Set is used, a decompressed file will be created for each file in the File Set.

Note: Compression tasks cannot compress or decompress files or folders located from SMB Network Shares or Encrypted Folders. Alternatively, files or folders from these resources can be copied into a Project Workspace to be compressed or decompressed, and then moved to a SMB Network Share or Encrypted folder.

Example 1: GUnzip a File

Follow the steps below to GUnzip a single file:

1. From within the Project Designer page, expand the Compression folder in the Component Library, and then drag the GUnzip task to the Project Outline.
2. On the Basic tab of the GUnzip task, specify values for the following attributes:

Input File

The "File Paths" on page 161 and file name of a single GZipped file to decompress.

Output File

The file to which the input file should be extracted, when uncompressing a single GZip file.

3. Click the **Save** button when finished.

Note: If you want to GUnzip multiple files, then leave the **Input File** blank and click the  **Action** link in the sub-menu and select the **Add a File Set** menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

GUnzip Task

The GUnzip task will decompress one or more files that are compressed with the GZip standard.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single GZipped file to uncompress.
Input Files Variable	Specify the name of a variable of type File List which contains a list or a collection of lists of files to uncompress.
Output File	Specify the file to which the input file should be extracted, when uncompressing a single GZip file. By default, the file name will be retrieved from the headers of the compressed file.
Output Directory	Specify the directory to which the input files should be extracted. By default files will be extracted to the same directory where the input file is in.
When File Exists	Specify the action to take when a file being extracted already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Output Variables Tab	
Output Files Variable	If desired, specify the name of a variable which will contain a list of the files that were extracted. This variable will be of type File List. It will be created if it does not exist, and overwritten otherwise. Specify the variable name if the extracted files will be used in a subsequent task (For example, FTP the extracted files).
Processed Input Files Variable	If desired, specify the name of a variable which will contain a list of input GZipped files that were processed by this task. It will be created if it does not exist, and overwritten otherwise. Specify the variable name if the zip file(s) will be used in a subsequent task (For example, Delete the zip file).
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Database Tasks

Database tasks can connect to a wide variety of database servers including DB2, Oracle, SQL Server, PostgreSQL, Informix, Sybase and MySQL. Any SQL statement supported by the database server can be issued by Managed File Transfer Projects including SELECT, UPDATE, INSERT, DELETE, CALL and CREATE statements.

SQL Task

The SQL task can connect to a database server for running SQL statements, which is useful for retrieving rows (records) from tables (physical files) or performing updates, inserts, etc. The database server connections can be pre-defined as reusable Resources, which can be selected from a drop-down menu in the SQL Task.

Example 1: SQL SELECT

Follow the steps below to perform a SQL SELECT statement within a Project.

1. From within the Project Designer page, expand the Database folder in the Component Library, and then drag the SQL task to the Project Outline.
2. On the Basic tab of the SQL task, select the database server resource from the drop-down list. If not already defined, click the **Create** button to define a new database server resource.
3. Click the **Add** button to Add a Query to the SQL task.
4. Type in your SQL Select Statement on the page. Alternatively, you can use the "SQL Wizard" on page 788 for quickly building the Select statement. With the SQL wizard, you can choose schemas (libraries), tables (physical files), columns (fields), column headings, "where" criteria and "order by" criteria. To

access the SQL Wizard for building a SELECT statement, click the  icon on the right side of the SQL Statement field.

5. Specify the Output Variable name, which will contain the data as type "RowSet" on page 121 from the Select Statement's results. Click the **Next** button to add any additional tasks to work with the data in the Output Variable. For instance, you may want to use the Output Variable as the input into other tasks such as the "Write CSV Task" on page 278, "Write Excel Task" on page 287, "Write Fixed-width Task" on page 306 or "Write XML Task" on page 318 tasks.

   Note: You must have Use permission to the Database Resource in order to execute the Project.

Example 2: SQL INSERT

A 'myData' RowSet variable contains the following data that will be inserted into a SQL database:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
Employee ID	First Name	Last Name	Hire Date	Dept. Code	Salary
34594	Heather	Banks	1998-01-19	BB001	72000
34593	Tina	Young	2010-04-01	BB001	65000
34590	Kathy	Harris	2007-09-30	KH001	105000
34592	Mark	Walker	2012-11-15	KH001	87500
34591	John	Davis	2001-06-15	KH001	85000

Follow the steps below to perform an SQL INSERT statement using data from a RowSet:

1. From within the Project Designer page, expand the Database folder in the Component Library, and then drag the SQL task to the Project Outline. .
2. On the Basic tab of the SQL task, select the database server resource from the drop-down list. If not already defined, click the **Create** button to define a new database server resource.
3. Click the **Add** button to Add a Query to the SQL task.
4. Type in your SQL Insert Statement on the page. In this example, a '?' is used as a place holder for each Index in the 'myData' RowSet. The 'myData' RowSet contains six columns, therefore six '?' placeholders will be used in the query.
5. Specify the RowSet variable name '${myData}' into the Input RowSet Variable field. The specified SQL Statement will be executed once per each row in this RowSet.
6. Click the **Save** button when complete. When the Project is executed, data from the 'myData' RowSet variable will be inserted into the database.

Example 3: SQL INSERT Using Query Parameters

In the previous example, the entire 'myData' RowSet variable was inserted into a SQL database. On some occasions, you may only want to add selected columns from the RowSet variable into the database. To add specific columns, you must use a Parameter element for each column you wish to insert.

Follow the steps below to insert columns one and six from the 'myData' RowSet variable into the database.

1. From within the Project Designer page, expand the Database folder in the Component Library, and then drag the SQL task to the Project Outline.
2. On the Basic tab of the SQL task, select the database server resource from the drop-down list. If not already defined, click the **Create** button to define a new database server resource.
3. Click the **Add** button to Add a Query to the SQL task.
4. Type in your SQL Insert Statement on the page. In this example, only two placeholder '?' are used for the Indexes referenced in the 'myData' RowSet.
5. Specify the RowSet variable name '${myData}' into the Input RowSet Variable field. The specified SQL Statement will be executed once per each row in this RowSet.
6. Click the **Add** button to Add a Parameter to the SQL query.
7. Enter '1' in the Parameter Index field. The '1' represents the first '?' placeholder position in the SQL Statement.
8. Enter '1' in the Map From field. This inserts data from column 1 of the 'myData' RowSet variable into the first column of the database.
9. Click the **Add** button and choose Add Same to add another Parameter to the SQL query.
10. Enter '2' in the Parameter Index field. The '2' represents the second '?' placeholder in the SQL Statement.
11. Enter '6' in the Map From field. This inserts data from column 6 of the 'myData' RowSet variable into the database.
12. Click the **Save** button when complete. When the Project is executed, data from columns 1 and 6 from the 'myData' RowSet variable are inserted into the SQL Database.

    The following image illustrates the Project Outline for the SQL Query INSERT task which uses two Query Parameter elements:

SQL Task

The SQL task allows you to specify the SQL server that will be used for your SQL query.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Database Server	Select a pre-configured database server from the drop down list.

Auto-Commit	Specify whether or not to commit the changes automatically. A value of 'true' means that the changes will be committed automatically after executing each query. A value of 'false' means that an explicit commit will be issued after successfully executing all queries. If any of the query fails for any reason, a rollback is issued. Default Value: true
Database Server Tab	
JDBC Driver	Specify the JDBC driver to use to connect to the target database. The driver need not exist in the dropdown menu, but must be installed in Managed File Transfer before it can be used. Specifying this value is only necessary if a Database Server resource was not selected or if it is desired to override the JDBC Driver specified in the Database Server resource.
JDBC URL	Specify the connection information for the specified database server. The syntax for specifying the connection information is driver dependent. A JDBC URL Wizard has been provided to assist with generating JDBC URLs. Click the '..' button to launch the JDBC URL Builder. Specifying this value is only necessary if a Database Server resource was not selected or if it is desired to override the JDBC URL specified in the Database Server resource.
User	Specify a user name for logging in to the specified Database Server. This is only necessary if a Database Server resource was not selected or if it is desired to override the user name specified in the Database Server resource.
Password	Specify a password for logging into the specified database. This is only necessary if a Database Server resource was not selected or if it is desired to override the password specified in the Database Server resource.
Is Password Encrypted?	Specify whether or not the password is encrypted. Default Value: false
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Query Element

The Query element allows you to specify a SQL statement that will execute on your SQL server.

Field	Definition
Basic Tab	
Label	Specify a label for this query.
SQL Statement	Specify the SQL statement to be executed. Any valid SQL statement that is supported by the target database server is allowed. Some example statement types include - SELECT, INSERT, UPDATE, DELETE, CALL, CREATE etc. An easy to use graphical tool is provided to build SELECT statements. Click on the '..' button to launch the SQL Wizard.
Input RowSet Variable	Specify a variable of type RowSet which should be fed as input to the SQL Statement being executed. For example, ${variableName}. The specified SQL Statement will be executed once per each row in this RowSet. This is specifically used to insert or update multiple records which are read from a different data source such as a flat file or another database.
Complete Output Variable	If desired, specify the name of a variable which contains the result of the statement execution. The type of this variable is list of objects. The type of object depends on the SQL statement. For SELECT statements, the type of the object is RowSet, and for all other statements, the type of the object is a number which contains the number of records affected, if any.
RowSet Output Variable	If desired, specify the name of a variable which contains the result of the selected statement execution. The type of this variable depends on the SQL statement. The RowSet Output Variable contains the result of a statement execution. The type of this variable is RowSet. It contains the first RowSet corresponding to a selected or a stored procedure.
Advanced Tab	
Null Substitute	Specify the value that should be used as a replacement for null values that are in the Input RowSet. This value is ignored if the specified SQL statement is a SELECT statement. This value can also be overridden on an individual parameter.
Create Scrollable RowSet?	Specify whether or not to create a scrollable RowSet. This attribute is only applicable for queries that return a result set. A scrollable RowSet can be traversed in both forward and reverse directions, thus allowing it to be re-used several times across multiple tasks. A non-scrollable RowSet can only be used once. By default, a scrollable RowSet will be created and should be adequate for most scenarios. Only configure this option if you are sure a non-scrollable RowSet is required. Default Value: true
Batch Size	Specify the batch size to use. If left blank, batching insert/update processing is not used (default). This attribute is only applicable when inserting or updating records and may greatly increase the speed of large insert/update operations at the cost of a larger memory footprint.
When No Data Found	Specify the action to take when the query produces an empty RowSet. By default, the project will continue with executing the next task. Please note that this attribute does not have any effect for SQL statements that DO NOT produce a RowSet such as insert or update statements. Default Value: continue

Parameter Element

The Parameter element allows you to specify the data mapped to placeholders ('?') in your query.

Field	Definition
Basic Tab	
Parameter Index	The index number of this parameter. Counting begins with 1.
Data Type	The data type of this parameter. By default, the data type CHAR is used unless this parameter is mapped to a column in the Input RowSet, in which case, the data type will be determined from the Input. Default Value: CHAR
Value	Specify a value for this parameter. You can leave this blank if the Map From attribute was specified.
Map From	Specify the index or name of the column in the Input RowSet (if one was defined in the Query) that should be mapped to this parameter. Mapping means that the value from the specified column be taken as the value of this input parameter when executing the SQL Statement.
Null Substitute	Specify the value that should be used as a replacement for null values that are in the Input RowSet. This value is ignored if the specified SQL statement is a SELECT statement.

Data Translation Tasks

Data translation tasks can read and write data using several popular formats including CSV, Excel, Fixed-width, Flat file and XML.

Read CSV Task

The Read CSV task can read data from delimited text files and load that data into a "RowSet" on page 121. That variable can then be used to import the data into a database or translate it into another file type like Excel, fixed-width, or *XML*.

If the input data does not have any special formatting requirements, then you can generally just specify the Input File and Output RowSet Variable attributes in the Read CSV task. However, if some of the fields have special formatting (for example, dates, trailing spaces, etc.), then you will want to Specify Data Options that can be added from the **Add** button on the page toolbar.

Formatting Options

Data Options specified will apply to every column in the file. For example, if you want to remove the leading and trailing white spaces on every field you can set that by using the Trim attribute. If you have a lot of columns in your file and you want all of the data trimmed except for a couple of columns then you can override the data options for a specific column by adding a Column element from the **Add** button on the page toolbar.

Column elements allow you to specify specific options for each column in your delimited file. You can add a name to the column, indicate the data type, change the formatting and more. The Pattern attribute of the

Column element allows you to specify the date or "Number Patterns" on page 797 format of the input. For example, if your input contains a numeric value like $4,500.99 then you can specify a pattern of $###,###.00. After the data is read in it will be converted to 4500.99, which is a format that is accepted by databases. If the input doesn't match that pattern then the *Project* will fail preventing garbage data from being processed.

Example 1: Read CSV File

Follow the steps below to read a CSV file that trims the leading and trailing spaces and also takes a containing dollar figures and converts them to a standard number without formatting. The following image represents the input CSV file:

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read CSV task to the Project Outline.
2. On the Basic tab of the Read CSV task, specify values for the Read CSV Task attributes:

   Input File

   The "File Paths" on page 161 and file name of a single file from which to read the data.

   Output Row

   Set VariableThe name of a variable which will contain the data read from the specified input file.

3. Click the **Add** button, and then click **Specify Data Options**.
4. On the Data Options tab, specify the trim option, which is how the leading and trailing spaces will be trimmed.
5. Click the **Add** button, and then click **Add Column** to add an element to the Read CSV task.
6. On the Basic tab of the Column element, specify the Index value of the column (to perform type conversion for).
7. On the Type Conversion tab of the Column element , specify the following attributes:

   TypeThe data type of this column. Use the value NUMERIC to convert the currency amounts into a standard number as per the example parameter above.

   Pattern

   The pattern to use to format "Number Patterns" on page 797 fields.
8. Click the **Save** button when complete. When the project executes, a RowSet variable named myData will contain the following data. Note, the data format of ${myData[6]} has been updated to remove the currency format:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
34594	Heather	Banks	1998-01-19	BB001	72000.00
34593	Tina	Young	2010-04-01	BB001	65000.00
34590	Kathy	Harris	2007-09-30	KH001	105000.00

34592	Mark	Walker	2012-11-15	KH001	87500.00
34591	John	Davis	2001-06-15	KH001	85000.00

Example 2: Read CSV Using a File Set

The Read CSV task can use the File Set element to read a collection of CSV files from a directory and then store the data into a single RowSet variable. The CSV files must be uniform in data structure, and each CSV file must contain the same number of columns and the columns must be of the same data type (such as VARCHAR or INT). When the Read CSV task has been processed, the output RowSet variable can be used as the input RowSet variable for a write task, such as "Write Excel Task" on page 287, or "Database Tasks" on page 267.

Follow the steps below to read a set of CSV files:

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read CSV task to the Project Outline.
2. On the Basic tab of the Read CSV task, specify the value for Output RowSet Variable. The output RowSet variable will contain the combined data read from each file in the File Set.
3. Click the **Add** button, and then Add a File Set.
4. On the Basic tab, specify a Base Directory that contains CSV files.
5. Click the **Add** button, and then Add a Wildcard Filter element to the Read CSV task.
6. Wildcard Filter elements do not contain any attributes to change. Click Next to add an Include Files element.
7. Enter a wildcard Pattern on the **Basic** tab. In this example, "*.csv" is used to only read files that end with the CSV file extension.
8. Click Save. When the Read CSV task is processed, the data from each CSV file in the File Set is stored into a single RowSet variable.

Read CSV Task

The Read CSV task allows you to specify file and variable parameters for translating a CSV file into a RowSet variable.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single file to read the data from.
Input Files Variable	Specify the name of a variable of type File List which contains the files to read the data from. For example, ${variableName}.

Output RowSet Variable	Specify the name of a variable which will contain the data read from the specified input file(s). The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable. The variable will be created if it does not exist.
Field Delimiter	Specify the character used in the input file(s) to separate data in each field. Default Value: comma
Advanced Tab	
Skip Invalid Records	Specify whether or not to ignore invalid records and continue on. The default is false, which will signal a error when invalid data is encountered. Default Value: false
Skip First Row	Specify whether or not to skip the first row of the csv file(s). If the csv file(s) contain header information in the first row, set this value to 'true'. Default Value: false
Record Delimiter	Specify the character or sequence of characters that are used to separate each record in the input file(s). The default record delimiter is CRLF (carriage return immediately followed by line feed). Default Value: CRLF
Text Qualifier	Specify the character used to enclose data in each field. Default Value: none
Encoding	Specify the character encoding of the input file(s). The default value is same as the platform's default file encoding. Default Value: The platform's default file encoding.
Output Variables Tab	
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Data Options

The Data Options element allows you to specify data format options for the fields in a CSV file.

Field	Definition
Data Options Tab	
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. By default no data is trimmed, i.e., all leading and trailing white spaces are preserved. This setting may also be overridden by the individual column settings. Default Value: none
Null Indicator	Specify the value that should be interpreted as null when reading the data from the input files. If the data in any column in any row matches the value specified here, it will be interpreted as a null. This value can be overridden by the individual columns.
Data Format Tab	
Whole Number Format	Specify the pattern used by the whole number fields (tinyint, smallint, int, bigint) in the input files. For example, ###,### (2,345). Please note that this setting will only be used if and only if there is at least one whole number (tinyint, smallint, int, bigint) type column defined under this data element. This value can be overridden by the individual columns.
Decimal Number Format	Specify the pattern used by the decimal number fields (real, float, double, decimal and numeric) in the input files. For example, $###,###.00 ($2,345.46). Please note that this setting will only be used if there is at least one decimal number (real, float, double, decimal, numeric) type column defined under this data element. This value can be overridden by the individual columns.
Date Format	Specify the pattern used by the date fields in the input file(s). For e.g. MM/dd/yyyy (08/02/2007). Please note that this setting will only be used if and only if there is at least one date type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd
Time Format	Specify the pattern used by the time fields in the input files. For e.g. hh:mm:ss a (08:12:56 PM). Please note that this setting will only be used if and only if there is at least one time type column defined under this data element. This value can be overridden by the individual columns. Default Value: HH:mm:ss

Timestamp Format	Specify the pattern used by the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). Please note that this setting will only be used if and only if there is at least one timestamp type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric, date/time data is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual column(s). Please note that this setting will only be used if and only if there is at least one numeric or date/time type column defined under this data element. Default Value: en_US

Column

The Column Field Element allows you to specify the data parameters for columns in a CSV file.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of this column.
Size	Specify the size (maximum numer of characters) of the column. This setting may not be used by this task but could be used by subsequent tasks that use the RowSet generated by this task.
Type Conversion Tab	
Type	Specify the data type of this column. For e.g. integer, date or decimal. Default Value: VARCHAR
Pattern	Specify the pattern that was used to format numeric or date/time fields. This will be used if and only if this column is defined as a numeric, date, time or timestamp type column. Default Value: Inherited from parent Data element.
Locale	Specify the locale to which the data in this column is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). Please note that this setting will only be used if and only if this column is defined as a numeric or date/time type column. Default Value: Inherited from parent Data element.
Data Options Tab	

Trim	Specify how the leading and trailing white spaces in this column should be trimmed. Default Value: Inherited from parent Data element.
Null Indicator	Specify the value that should be interpreted as null when reading the data from this column. If the data in this column in any row matches the value specified here, it will be interpreted as a null value. Default Value: Inherited from parent Data element.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Write CSV Task

The Write CSV task will write a delimited text file based on the contents of a "RowSet" on page 121. That variable can contain data from a database or from another file type such as Excel, fixed-width, or *XML*.

Writing a CSV file can be as easy as specifying the Input RowSet Variable and Output File attributes. By default, the file will be comma delimited and the contents will be identical to the data found in the RowSet variable.

Formatting Options

If the output data needs special formatting, you can Specify Data Options by selecting it though the **Add** button in the sub-menu.

Note: If you are appending to an existing file, no header information is sent to the file even if the Task is configured to write header info.

Example 1: Write CSV File

Follow the steps below to write a CSV file. This example also shows how to format a column from a standard number into its dollar representation (see Step 7). The input RowSet data being used is based on the example in the "RowSet" on page 121.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Write CSV task to the Project Outline.
2. On the Basic tab of the Write CSV task, specify values for the following attributes:

   Input RowSet Variable

   The name of a variable of type RowSet which contains data to write to a file.

   Output File

   The "File Paths" on page 161 and file name of a single file to write.
3. Click the **Add** button in the sub-menu and select the Specify Data Options menu item.
4. Click the **Add** button in the sub-menu and select the Add Column menu item.
5. On the Basic tab of the Write CSV Column element, specify the Index value:

   Index

   The index of the column in the input RowSet.

6. On the Type Conversion tab of the Write CSV Column element, specify values for the following attributes:

   Data Type

   The data type of this column. The output data type does not need to match in input type. The example in the Read CSV Task converted the Currency Data Type to a Number. This allows you to convert the number back to a Currency Data Type.

   Pattern

   The pattern to use to format "Number Patterns" on page 797 or date/time fields.

7. Click the **Save** button when finished.

Write CSV Task

The Write CSV task allows you to specify file and data parameters for translating a RowSet variable into a CSV file.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input RowSet Variable	Specify the name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}
Output File	Specify the path and file name of a single file to write.
When Output File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the file name to a new name so the existing file remains untouched. Default Value: rename
Field Delimiter	Specify the character to use for separating each field in the generated CSV file. Default Value: comma
Advanced Tab	
Maximum Rows	Specify the maximum number of rows to be written to the output file. When this limit is reached, the remaining rows in the input RowSet will be silently skipped.
Encoding	Specify the character encoding of the output file. Default Value: The platform's default file encoding.
Include Column Headings	Specify whether or not to include column headings in the generated CSV file. Default Value: false
Record Delimiter	Specify the character(s) to use for separating each record (or row) in the generated CSV file. Default Value: CRLF
Text Qualifier	Specify the character used to enclose data in each field. Default Value: none

Apply Text Qualifier To	Specify whether the text qualifier (if specified) should be applied to all columns or only to non-numeric columns. By default, the column types are determined from the metadata of the Input RowSet. The column types can also be overridden by defining the nested column elements. Please note that in some cases the text qualifier may be applied to numeric fields if the numeric value is formatted to contain special characters (e.g. comma). Text qualifier is always applied to all column headings (irrespective of the column type) if the column headings are included. Default Value: none
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Data Options

The Data Options element allows you to specify data format options for the data written to the CSV file.

Field	Definition
Basic Tab	
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. By default no data is trimmed, i.e., all leading and trailing white spaces are preserved. This setting may also be overridden by the individual column settings.
Null Indicator	Specify the value that should be interpreted as null when reading the data from the input files. If the data in any column in any row matches the value specified here, it will be interpreted as a null. This value can be overridden by the individual columns.
Data Format Tab	

Whole Number Format	Specify the pattern used by the whole number fields (tinyint, smallint, int, bigint) in the input files. For example, ###,### (2,345). Please note that this setting will only be used if and only if there is at least one whole number (tinyint, smallint, int, bigint) type column defined under this data element. This value can be overridden by the individual columns.
Decimal Number Format	Specify the pattern used by the decimal number fields (real, float, double, decimal and numeric) in the input files. For example, $###,###.00 ($2,345.46). Please note that this setting will only be used if there is at least one decimal number (real, float, double, decimal, numeric) type column defined under this data element. This value can be overridden by the individual columns.
Date Format	Specify the pattern used by the date fields in the input file(s). For e.g. MM/dd/yyyy (08/02/2007). Please note that this setting will only be used if and only if there is at least one date type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd
Time Format	Specify the pattern used by the time fields in the input files. For e.g. hh:mm:ss a (08:12:56 PM). Please note that this setting will only be used if and only if there is at least one time type column defined under this data element. This value can be overridden by the individual columns. Default Value: HH:mm:ss
Timestamp Format	Specify the pattern used by the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). Please note that this setting will only be used if and only if there is at least one timestamp type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric, date/time data is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual column(s). Please note that this setting will only be used if and only if there is at least one numeric or date/time type column defined under this data element. Default Value: en_US

Column

The Column Field Element allows you to specify the data parameters written to columns in a CSV file.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of this column.
Type Conversion Tab	
Data Type	Specify the data type of this column. For e.g. integer, date or decimal. The data type specified here can be different than the actual data type in the input RowSet. If the data type is overridden, the task performs appropriate data type conversions when reading the data from the input RowSet. Default Value: Same as input data.

Pattern	Specify the pattern to use for formatting the data in this column. This will have effect if and only if the data type of this column is numeric, date, time or timestamp. The default pattern is taken from the parent Data element based on the type of this column. Default Value: Inherited from parent Data element.
Locale	Specify the locale to which the data in this column is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). The default locale is taken from the parent Data element. Please note that this setting will only be used if and only if this column is defined as a numeric or date/time type column. Default Value: Inherited from parent Data element.
Data Options Tab	
Trim	Specify how the leading and trailing white spaces in this column should be trimmed. The default is inherited from the parent Data element. Default Value: Inherited from parent Data element.
Null Indicator	Specify the value that should be written to the output file when this column of the input RowSet has a null value. The default is inherited from the parent Data element. Default Value: Inherited from parent Data element.

Read Excel Task

The Read Excel task can read data from Microsoft Excel 2003 and 2007 documents and load this data into "RowSet" on page 121. Those RowSet variables can then be used in other tasks for importing the Excel data into databases or for translating this data into other file types such as *CSV*, fixed-width, or *XML*.

Complex Excel documents can be read by Managed File Transfer, including documents with formatted data, formulas and multiple sheets.

Column elements can be placed under the Read Excel Task to specify options for each column in the Excel document. For instance, you can specify a name for a column, its data type and formatting (using the pattern attribute).

Columns containing date or time values will be formatted based on ISO standards. For instance, when a cell contains a date and time formatted as '12/25/2005 11:58 PM', the Read Excel Task will parse it into a ISO formatted date and time string as '2005-12-25 11:58:00.000'.

By default, all sheets in the Excel document will be read unless you specify a sheet name in the Sheet Name(s) attribute. If multiple sheets are being read, then the data on all sheets must start on the same row number and each sheet must contain the same number of columns or the *Project* will fail.

Example 1: Read Excel Task

Follow the steps below to read an Excel document and format a date column.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read Excel task to the Project Outline.
2. On the Basic tab of the Read Excel task, specify values for the following attributes:

Input File

The "File Paths" on page 161 and file name of an Excel document from which to read data.

Output RowSet Variable

The name of a variable to contain the data read from the Excel document.

3. On the Advanced tab of the Read Excel task, specify values for the following attributes:

Data Start Row Number

The row number where the data starts in the document. In the example above, the Data starts on row four (4).

Headings Row Number

The row number where the column headings are found in the document.

4. Click the **Add** button and click the **Specify Data Options** option.
5. Click the **Add** button and click the **Add Column** option.
6. On the Basic tab of the Column element, specify the Index value:

Index

The index of the column in the document.

7. On the Type Conversion tab of the Column element, specify values for the following attributes:

Type

The data type of this column. In the example above the data type is DATE.

Pattern

The pattern to use to format "Number Patterns" on page 797 or date/time fields. The pattern is automatically determined based on ISO formatting. Only specify the pattern if ISO date format is not desired.

8. Click the **Save** button when finished.

When the project executes, a RowSet variable named myData will contain the following data:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
ID	First Name	Last Name	Hire Date	Dept Code	Wages
34594	Heather	Banks	1998-01-19	BB001	72000
34593	Tina	Young	2010-04-01	BB001	65000
34590	Kathy	Harris	2007-09-30	KH001	105000
34592	Mark	Walker	2012-11-15	KH001	87500
34591	John	Davis	2001-06-15	KH001	85000

Note: The Read Excel Task will ignore any formatting such as alignment options, size, and font family. Also, formulas are processed before they are read, so if a cell contains the formula of =SUM(A1:A10), then the value will be read as the sum of the cells A1 through A10.

Read Excel Task

The Read Excel task allows you to specify file and variable parameters for translating an Excel file into a RowSet variable.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single file to read the data from.
Input Files Variable	Specify the name of a variable of type File List which contains the files to read the data from. For example, ${variableName}.
Output RowSet Variable	Specify the name of a variable which will contain the data read from the specified input file(s). The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable. The variable will be created if it does not exist.
Advanced Tab	
Skip Invalid Records	Specify whether or not to ignore invalid records and continue on. The default is false, which will signal a error when invalid data is encountered. Default Value: false
Skip Empty Rows	Specify whether or not to skip empty rows. If this value is set to true and a row is encountered that contains no data, that row will be silently skipped.
Data Start Row Number	Specify the row number where the data starts in the input file(s). Default Value: 1
Headings Row Number	Specify the row number where the column headings are in the input file(s). This is needed only if column headings are present in the input file(s). The first row is 1, not 0.
Sheet Name(s)	Specify the names of the sheets to read from the specified input files. The sheet names must be separated by commas. If no sheet names are specified, the default action is to read all sheets from the input files.
Number of Columns to Read	Specify the number of columns to read from the excel spreadsheet. By default, the number of columns will be auto determined from the number of columns containing data in the data start row. This setting is helpful if the data start row has a different number of columns than needs to be read from the spreadsheet.
Output Variables Tab	
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Data Options

The Data Options element allows you to specify data format options for the fields in an Excel file.

Field	Definition
Basic Tab	
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. By default no data is trimmed, i.e., all leading and trailing white spaces are preserved. This setting may also be overridden by the individual column settings.
Null Indicator	Specify the value that should be interpreted as null when reading the data from the input files. If the data in any column in any row matches the value specified here, it will be interpreted as a null. This value can be overridden by the individual columns.
Data Format Tab	
Whole Number Format	Specify the pattern used by the whole number fields (tinyint, smallint, int, bigint) in the input files. For example, ###,### (2,345). Please note that this setting will only be used if and only if there is at least one whole number (tinyint, smallint, int, bigint) type column defined under this data element. This value can be overridden by the individual columns.
Decimal Number Format	Specify the pattern used by the decimal number fields (real, float, double, decimal and numeric) in the input files. For example, $###,###.00 ($2,345.46). Please note that this setting will only be used if there is at least one decimal number (real, float, double, decimal, numeric) type column defined under this data element. This value can be overridden by the individual columns.
Date Format	Specify the pattern used by the date fields in the input file(s). For e.g. MM/dd/yyyy (08/02/2007). Please note that this setting will only be used if and only if there is at least one date type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd

Time Format	Specify the pattern used by the time fields in the input files. For e.g. hh:mm:ss a (08:12:56 PM). Please note that this setting will only be used if and only if there is at least one time type column defined under this data element. This value can be overridden by the individual columns. Default Value: HH:mm:ss
Timestamp Format	Specify the pattern used by the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). Please note that this setting will only be used if and only if there is at least one timestamp type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric, date/time data is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual column(s). Please note that this setting will only be used if and only if there is at least one numeric or date/time type column defined under this data element. Default Value: en_US

Column

The Column Field Element allows you to specify the data parameters for columns in a Excel file.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of this column.
Size	Specify the size (maximum numer of characters) of the column. This setting may not be used by this task but could be used by subsequent tasks that use the RowSet generated by this task.
Type Conversion Tab	
Type	Specify the data type of this column. For e.g. integer, date or decimal. Default Value: VARCHAR
Pattern	Specify the pattern that was used to format numeric or date/time fields. This will be used if and only if this column is defined as a numeric, date, time or timestamp type column. Default Value: Inherited from parent Data element.
Locale	Specify the locale to which the data in this column is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). Please note that this setting will only be used if and only if this column is defined as a numeric or date/time type column. Default Value: Inherited from parent Data element.
Data Options Tab	

Trim	Specify how the leading and trailing white spaces in this column should be trimmed. Default Value: Inherited from parent Data element.
Null Indicator	Specify the value that should be interpreted as null when reading the data from this column. If the data in this column in any row matches the value specified here, it will be interpreted as a null value. Default Value: Inherited from parent Data element.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Write Excel Task

The Write Excel task will write data to a Microsoft Excel 2007 document (.xlsx) or previous Excel versions (.xls) from the contents of a "RowSet" on page 121 variable. That variable can contain data from a database or from another file type such as *CSV*, fixed-width, or *XML*.

Writing an Excel document can be as simple as specifying the Input RowSet Variable and Output File attributes. By default, this will create an Excel document with raw unformatted data. However the Write Excel Task can also create elaborate spreadsheets with page headers, footers, titles, column headings, text formatting, and more. Almost every formatting option found in Excel is available through the options in the Write Excel Task's sub-elements.

A Template File can be specified which may contain your corporate logo and special formatting options (such as color and font themes) for creating professional spreadsheets. Formats can be overridden for individual columns and rows, which will supersede any settings you may have created in the template file.

Example 1: Write Excel File

Follow the steps below to create an Excel 2007 document with a page header, a title, and column headings. The input RowSet data being used is based on the example illustrated in the "RowSet" on page 121.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Write Excel task to the Project Outline.
2. On the Basic tab of the Write Excel task, specify values for the following attributes:

   Input RowSet Variable

   The name of a variable of type RowSet which contains the source data.

   Output File

   The "File Paths" on page 161 and file name of the Excel document to write to.

   Excel Format

   The Excel document format, either Excel 2007 or Excel 2003.
3. On the Advanced tab of the Write Excel task, specify the Include Column Headings value:

   Include Column Headings

   Whether or not to include column headings in the generated Excel document.
4. Click the **Add** button in the sub-menu and select the Specify Page Header menu item.
5. On the Basic tab of the Page Header element, specify values for the following:

Left Section

The text that should be displayed in the left section. You can insert page number, number of pages, date, time etc. by using the appropriate variable names listed in the options drop-down.

Right Section

The text that should be displayed in the right section.

6. Right-click the Write Excel Task in the Project Outline on the left side of the page and select the Specify Title menu item.
7. On the Basic tab of the Title element, specify the Title Text value:

   Title Text

   The title text.
8. On the Cell Format tab of the Title element, specify the values for the following attributes:

   Background Color

   The background color for the title cell.

   Underline

   Option to underline the title text.
9. Right-click the Write Excel task in the Project Outline on the left side of the page and select the Specify Column Headings menu item.
10. On the Basic tab for the Column Headings element, specify the Row Number value:

    Row Number

    The row number where the column headings should appear.
11. On the Format tab of the Column Headings element, specify the Bold value:

    Bold

    The font weight of the Column Headings.
12. Right-click the Write Excel task in the Project Outline on the left side of the page and select the Specify Data Options menu item.
13. Click the **Add** button, and then click **Add Column** to add an element to the Write Excel Task.
14. On the Basic tab of the Column element, specify the Index value of the column (to perform a type conversion):
15. On the Type Conversion tab of the Column element , specify the following attributes:

    Type

    The data type of this column. Use the value NUMERIC to convert the currency amounts into a standard number as per the example parameter above.

    Pattern

    The pattern to use to format "Number Patterns" on page 797 fields.
16. Click the **Save** button when finished.

Note: Refer to the "Excel Pattern Syntax" on page 296 for more formatting options.

Write Excel Task

The Write Excel task allows you to specify file and data parameters for translating a RowSet variable into an Excel file

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input RowSet Variable	Specify the name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}
Output File	Specify the path and file name of a single file to write.
When Output File Exists	Specify the action to take when the output file already exists. The default value is 'rename file' which changes the file name to a new name so the existing file remains untouched. Default Value: rename file
Excel Format	Specify which Excel format to use. If left blank, the document will be written in Excel 2003 (XLS) format. Default Value: excel2003
Template File	Specify the path and file name of the template to use. The template file must be an Excel file. The new sheet will be created based of the first sheet from the template file.
Advanced Tab	
Maximum Rows	Specify the maximum number of rows to be written to the output file. When this limit is reached, the remaining rows in the input RowSet will be silently skipped.
Sheet Name	Specify the name of the sheet to which the data should be written. If the specified sheet name does not exist, it will be created. Default Value: Sheet 1
When Sheet Is Full	Specify the action to take when the spreadsheet becomes full. Default Value: error
Include Column Headings	Specify whether or not to include column headings in the generated Excel file. Default Value: false
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module

Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Data Options

The Data Options element allows you to specify data format options for the data written to the Excel file.

Field	Definition
Basic Tab	
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. By default no data is trimmed, leaving all leading and trailing white spaces. This setting may also be overridden by the individual column settings. Default Value: none
Null Substitute	Specify the value that should be written to the output file when any field in any row of the input RowSet has a null value. This value can be overridden by the individual columns.
Start Row Number	Specify the row number (1 based) where the data should start. The default row number is after the title row or the headings row if they are present. When there is no title and no column headings, this defaults to 1 (the first row).
Data Format Tab	
Whole Number Format	Specify the pattern to use for formatting the whole number fields (tinyint, smallint, int, bigint) in the output file. For e.g. ###,### (2,345). Please note that this setting will only be used if and only if there is at least one whole number (tinyint, smallint, int, bigint) type column defined under this data element. This value can be overridden by the individual columns.
Decimal Number Format	Specify the pattern to use for formatting the decimal number fields (real, float, double, decimal and numeric) in the output file. For e.g. $###,###.00 ($2,345.46). Please note that this setting will only be used if there is at least one decimal number (real, float, double, decimal, numeric) type column defined under this data element. This value can be overridden by the individual columns.
Date Format	Specify the pattern for formatting the date fields in the output file. For e.g. MM/dd/yyyy (08/02/2007). Please note that this setting will only be used if and only if there is at least one date type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd

Time Format	Specify the pattern to use for formatting the time fields in the input files. For e.g. hh:mm:ss AM/PM (08:12:56 PM). Please note that this setting will only be used if and only if there is at least one time type column defined under this data element. This value can be overridden by the individual columns. Default Value: hh:mm:ss
Timestamp Format	Specify the pattern to use for formatting the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss AM/PM (Aug 02, 2007 08:12:56 PM). Please note that this setting will only be used if and only if there is at least one timestamp type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd hh:mm:ss.000
Cell Format Tab	
Horizontal Alignment	Specify how the contents of the data cells should be aligned horizontally. This can be overridden on a specific column, if needed. Default Value: general
Vertical Alignment	Specify how the contents of the data cells should be aligned vertically. This can be overridden on a specific column, if needed. Default Value: bottom
Background Color	Specify the background color to use for all the data cells. Leaving this value blank indicates that no background color will be used. This can be overridden on a specific column, if needed.
Font	Specify the font to use for the data. This can be overridden on a specific column, if needed. Default Value: Arial
Font Size	Specify the size of the font to use for the data. This can be overridden on a specific column, if needed. Default Value: 10
Font Color	Specify the color of the data font. This can be overridden on a specific column, if needed. Default Value: Automatic
Bold	Specify whether or not to apply bold style for the data. This can be overridden on a specific column, if needed. Default Value: false
Italic	Specify whether or not to apply italic style for the data. This can be overridden on a specific column, if needed. Default Value: false
Strikethrough	Specify whether or not the strikethrough effect should be applied to the data. This can be overridden on a specific column, if needed. Default Value: false
Underline	Specify how the data cells should be underlined. This can be overridden on a specific column, if needed. Default Value: none

Wrap	Specify whether or not the contents of the data cells should be wrapped. This can be overridden on a specific column, if needed. Default Value: false
Orientation	Specify the orientation of the data cells. This can be overridden on a specific column, if needed.

Column

The Column Field Element allows you to specify the data parameters written to columns in an Excel file.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input RowSet. The first column starts with index 1. Either index or name must be specified to customize the output data. If both index and name are specified, the index value will be used.
Name	Specify the name of the column in the input RowSet. The column names are case insensitive. Either index or name must be specified to customize the output data. If both index and name are specified, the index value will be used. The name specified here overrides the input RowSet column name.
Type Conversion Tab	
Data Type	Specify the data type of this column. For e.g. integer, date or decimal. The data type specified here can be different than the actual data type in the input RowSet. If the data type is overridden, the task performs appropriate data type conversions when reading the data from the input RowSet. Default Value: Same as input data.
Pattern	Specify the pattern to use for formatting the data in this column. This will have effect if and only if the data type of this column is numeric, date, time or timestamp. The default pattern is taken from the parent Data element based on the type of this column. Default Value: Inherited from parent Data element.
Data Options Tab	
Trim	Specify how the leading and trailing white spaces in this column should be trimmed. The default is inherited from the parent Data element. Default Value: Inherited from parent Data element.
Null Substitute	Specify the value that should be written to the output file when this column of the input RowSet has a null value. The default is inherited from the parent Data element. Default Value: Inherited from parent Data element.
Cell Format Tab	
Horizontal Alignment	Specify how the contents of this column should be aligned horizontally. Default Value: general
Vertical Alignment	Specify how the contents of this column should be aligned vertically.

Background Color	Specify the background color to use for column.
Font	Specify the font to use for the data in this column.
Font Size	Specify the size of the font to use for the data in this column.
Font Color	Specify the color of the data font in this column. Default Value: Automatic
Bold	Specify whether or not to apply bold style for the data in this column. Default Value: false
Italic	Specify whether or not to apply italic style for the data in this column. Default Value: false
Strikethrough	Specify whether or not the strikethrough effect should be applied to the data in this column. Default Value: false
Underline	Specify how the data cells in this column should be underlined. Default Value: none
Wrap	Specify whether or not the contents of the data cells in this column should be wrapped. Default Value: false
Orientation	Specify the orientation of the data cells in this column.
Width	Specify how wide (number of characters) this column should be. Default Value: -1 (Auto sizes the column)

Header

The Header element allows you to add text, page numbers, number of pages, or data and time to the header of the printed Excel file.

Field	Definition
Basic Tab	
Left Section	Specify the text that should be displayed in the left section. You can insert page number, number of pages, date, time etc. using the appropriate variable names listed in the options drop-down.
Center Section	Specify the text that should be displayed in the center section. You can insert page number, number of pages, date, time etc. using the appropriate variable names listed in the options drop-down.
Right Section	Specify the text that should be displayed in the right section. You can insert page number, number of pages, date, time etc. using the appropriate variable names listed in the options drop-down.

Footer

The Footer element allows you to add text, page numbers, number of pages, or data and time to the footer of the printed Excel file.

Field	Definition
Basic Tab	
Left Section	Specify the text that should be displayed in the left section. You can insert page number, number of pages, date, time etc. using the appropriate variable names listed in the options drop-down.
Center Section	Specify the text that should be displayed in the center section. You can insert page number, number of pages, date, time etc. using the appropriate variable names listed in the options drop-down.
Right Section	Specify the text that should be displayed in the right section. You can insert page number, number of pages, date, time etc. using the appropriate variable names listed in the options drop-down.

Title

The Title element allows you specify formatting options to the title row in an Excel spreadsheet.

Field	Definition
Basic Tab	
Title Text	Specify the title text.
Row Number	Specify the row number (1 based) where the title should appear. The first row starts at 1. Default Value: 1
Column Span	Specify the number of columns the title should span across. The specified number of cells on the title row will be merged. By default, the title row will span to the number of columns in the input RowSet.
Cell Format Tab	
Horizontal Alignment	Specify how the contents of the title cell should be aligned horizontally. Default Value: center
Vertical Alignment	Specify how the contents of the title cell should be aligned vertically. Default Value: bottom
Background Color	Specify the background color for the title cell. Leaving this value blank indicates that no background color will be used.
Font	Specify the font to use for this title. Default Value: Arial
Font Size	Specify the size of the font to use for this title. Default Value: 16
Font Color	Specify the color of the title font. Default Value: Automatic

Bold	Specify whether or not to apply bold style for the title. Default Value: true
Italic	Specify whether or not to apply italic style for the title. Default Value: false
Strikethrough	Specify whether or not the strikethrough effect should be applied to the title. Default Value: false
Underline	Specify how the titled should be underlined. Default Value: none
Wrap	Specify whether or not the contents of the title cell should be wrapped. Default Value: false
Orientation	Specify the orientation of the title cell.

Column Headings

The Column Headings element allows you specify formatting options to the column headers in an Excel spreadsheet.

Field	Definition
Basic Tab	
Row Number	Specify the row number where the column headings should appear. If a title is present, the default is the row after the title. Otherwise, defaults to row 1.
Cell Format Tab	
Horizontal Alignment	Specify how the contents of the heading cells should be aligned horizontally. Default Value: left
Vertical Alignment	Specify how the contents of the heading cells should be aligned vertically. Default Value: bottom
Background Color	Specify the background color for the heading cells. Leaving this value blank indicates that no background color will be used.
Font	Specify the font to use for the column headings. Default Value: Arial
Font Size	Specify the size of the font to use for the column headings. Default Value: 10
Font Color	Specify the color of the column headings. Default Value: Automatic
Bold	Specify whether or not to apply bold style for the column headings. Default Value: true

Italic	Specify whether or not to apply italic style for the column headings. Default Value: false
Strikethrough	Specify whether or not the strikethrough effect should be applied to the column headings. Default Value: false
Underline	Specify how the column headings should be underlined. Default Value: none
Wrap	Specify whether or not the contents of the column heading cells should be wrapped. Default Value: false
Orientation	Specify the orientation of the column headings.

Excel Pattern Syntax

The Write Excel Task requires that patterns adhere to the Excel Pattern Syntax. This syntax differs from the Date/Time patterns used elsewhere in Managed File Transfer and are specific to the "Write Excel Task" on page 287.

Patterns

Patterns are applied only to columns that are either NUMBER (integer or decimal), DATE, TIME or TIMESTAMP data types. Currently, patterns are not applied to character fields (VARCHAR, CHAR, etc.).

The pattern symbols in the table below are categorized by their applicable data types.

Number Formats

Symbol	Description
0	Digit placeholder. For example, if you type 8.9 and you want it to display as 8.90, then use the format #.00
#	Digit placeholder. Follows the same rules as the 0 symbol except Excel does not display extra zeros when the number you type has fewer digits on either side of the decimal than there are # symbols in the format. For example, if the custom format is #.## and you type 8.9 in the cell, the number 8.9 is displayed.
?	Digit placeholder. Follows the same rules as the 0 symbol except Excel places a space for insignificant zeros on either side of the decimal point so that decimal points are aligned in the column. For example, the custom format 0.0? aligns the decimal points for the numbers 8.9 and 88.99 in a column.
. (period)	Decimal point.
%	Percentage. If you enter a number between 0 and 1, and you use the custom format 0%, Excel multiplies the number by 100 and adds the % symbol in the cell.

Symbol	Description
, (comma)	Thousands separator. Excel separates thousands by commas if the format contains a comma surrounded by '#'s or '0's. A comma following a placeholder scales the number by a thousand. For example, if the format is #.0,, and you type 12,200,000 in the cell, the number 12.2 is displayed.
E- E+ e- e+	Scientific format. Excel displays a number to the right of the "E" symbol that corresponds to the number of places the decimal point was moved. For example, if the format is 0.00E+00 and you type 12,200,000 in the cell, the number 1.22E+07 is displayed. If you change the number format to #0.0E+0 the number 12.2E+6 is displayed.
$-+/():space	Displays the symbol. If you want to display a character that is different than one of these symbols, precede the character with a backslash (\) or enclose the character in quotation marks (" ").
\	Display the next character in the format. Excel does not display the backslash. For example, if the number format is 0\! and you type 3 in the cell, the value 3! is displayed.
*	Repeat the next character in the format enough times to fill the column to its current width. You cannot have more than one asterisk in one section of the format. For example, if the number format is 0*x and you type 3 in the cell, the value 3xxxxxx is displayed. Note, the number of "x" characters displayed in the cell vary based on the width of the column.
_ (underline)	Skip the width of the next character. This is useful for lining up negative and positive values in different cells of the same column. For example, the number format _(0.0_);(0.0) align the numbers 2.3 and -4.5 in the column even though the negative number has parentheses around it.
"text"	Display whatever text is inside the quotation marks. For example, the format 0.00 "dollars" displays "1.23 dollars" (without quotation marks) when you type 1.23 into the cell.

Date Formats

Symbol	Description
m	Display the month as a number without a leading zero.
mm	Display the month as a number with a leading zero when appropriate.
mmm	Display the month as an abbreviation (Jan-Dec).
mmmm	Display the month as a full name (January-December).
d	Display the day as a number without a leading zero.
dd	Display the day as a number with a leading zero when appropriate.
ddd	Display the day as an abbreviation (Sun-Sat).
dddd	Display the day as a full name (Sunday-Saturday).
yy	Display the year as a two-digit number.
yyyy	Display the year as a four-digit number.

Time Formats

Symbol	Description
h	Display the hour as a number without a leading zero.
[h]	Elapsed time, in hours. If you are working with a formula that returns a time where the number of hours exceeds 24, use a number format similar to [h]:mm:ss.
hh	Display the hour as a number with a leading zero when appropriate. If the format contains AM or PM, then the hour is based on the 12-hour clock. Otherwise, the hour is based on the 24-hour clock.
m	Display the minute as a number without a leading zero.
[m]	Elapsed time, in minutes. If you are working with a formula that returns a time where the number of minutes exceeds 60, use a number format similar to [mm]:ss.
mm	Display the minute as a number with a leading zero when appropriate. The m or mm must appear immediately after the h or hh symbol, or Excel displays the month rather than the minute.
s	Display the second as a number without a leading zero.
[s]	Elapsed time, in seconds. If you are working with a formula that returns a time where the number of seconds exceeds 60, use a number format similar to [ss].
ss	Display the second as a number with a leading zero when appropriate. **Note:** If you want to display fractions of a second, use a number format similar to h:mm:ss.00.
AM/PM am/pm A/P a/p	Display the hour using a 12-hour clock. Excel displays AM, am, A, or a for times from midnight until noon, and PM, pm, P, or p for times from noon until midnight.

Password Protect Excel

The Password Protect Excel task encrypts Microsoft Excel .xlsx documents, which then requires a password to be opened.

Example 1: Password Protect a Single Excel Document

Follow the steps below to password protect an Excel document.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Password Protect Excel task to the Project Outline.
2. On the Basic tab of the Password Protect Excel task, specify values for the following attributes:

   Source File

   Specify the path and file name of a single file to be password protected.

   Destination File

   Specify the path and file name where the file will be created with password protection.

Password

Specify the password to protect the Excel file.

3. When the user attempts to open the Excel file, a Password prompt appears. Enter the password from step 3 above and click OK.

Example 2: Password Protect a Set of Excel Files

Follow the steps below to password protect a set of Excel files.

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
2. On the Basic tab of the Create File List task, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created. If this variable exists it will be overwritten, otherwise it will be created.

3. Click the **Add** button. This displays a sub-menu of "Action" items that can be performed.
4. Choose the **Add a File Set** option from the sub-menu.
5. On the Basic tab of the File Set option, specify values for the following attributes:

   Base Directory - The starting directory for this File Set. If no filters are defined, all files in this directory will be included.

6. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Password Protect Excel task to the Project Outline.
7. On the Basic tab of the Password Protect Excel task, specify values for the following attributes:

   Source Files Variable

   Specify the name of a variable of type File List which contains the files to password protect. For example, ${fileList}.

   Destination Directory

   Specify the directory to which the specified source files should be placed after they are password protected. You must specify this attribute if you are password protecting multiple files using one or more File Set elements, or a Source Files Variable.

   Password

   Specify the password to protect the Excel files.

Password Protect Excel Task

The Password Protect Excel task encrypts Microsoft Excel .xlsx documents.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Source File	Specify the path and file name of a single file to be password protected.

Source Files Variable	Specify the name of a variable of type File List which contains the files to password protect. For example, ${variableName}.
Destination File	Specify the path and file name where the file will be created with password protection.
Destination Directory	Specify the directory to which the specified source files should be placed after they are password protected. You must specify this attribute if you are password protecting multiple files using one or more File Set elements, or a Source Files Variable.
Password	Specify the password to protect the Excel file.
Is Password Encrypted?	Specify whether or not the password is in encrypted form. Default Value: false
When File Exists	Specify the action to take when the destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Encryption Algorithm	Specify the encryption algorithm. Default Value: AES128
Hash Algorithm	Specify the hash algorithm to use. Default Value: SHA1
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the file(s) in the destination location. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Read Fixed-width Task

The Read Fixed-width task can read data from text files and load that data into a "RowSet" on page 121. The variable's contents can then be imported into a database or translated into another file type like Excel, *CSV*, or *XML*.

Fixed-width files contain one or more columns using a predetermined length for each column. The size of each column must be specified by adding Column elements through the **Add** button in the sub-menu. Columns are added from left to right, always beginning on the first column position of the fixed-width file. The last column specified must end on a record delimiter (such as CRLF) or end on the last column in the record length.

Example 1: Read Fixed-width File

In the data example below, each column in the fixed-width file is separated by a space. The data in the first column represents a 5-digit employee ID followed by 1 space for a total column length of 6. The data in the next column represents an 11 character first name followed by a space, for a total column length of 12. Each record ends with a hidden CRLF delimiter. When adding these columns to the RowSet variable 'myData,' the data will be trimmed of any trailing spaces.

Follow the steps below to read the first two columns from a fixed-width file.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read Fixed-width task to the Project Outline.
2. On the Basic tab of the Read Fixed-width task, specify values for the following attributes:

   Input File

   The "File Paths" on page 161 and file name of a single file from which to read data.

   Output RowSet Variable

   The name of a variable which will contain the data read from the specified input file.
3. On the Advanced tab of the Read Fixed-width task, specify the Skip First Row value:

   Skip First Row

   Whether or not to skip the first row of the input file. If the input file contains header information in the first row, set this value to 'true'. In the example above, there is no header information, so the setting would be set to false.
4. Click the **Add** button to Specify Data Option for the Read Fixed-width task.
5. In the Data window, click the **Add** button and select the **Add Column** option.
6. On the Basic tab of the Column element, specify values for the following attributes:

   Index

   The index of the column in the input file. In the example above, the column used for the first Index is the Employee ID column, which is Index 1.

   Name

   Specify the name of the column.

   Size

   The size of the column. In the example above, the size is 6.
7. On the Type Conversion tab of the Column element, specify values for the following attributes:

Type

The default type is Variable Character (VARCHAR). Specify a different type if needed.

Pattern

The pattern to use to format "Number Patterns" on page 797 or date/time fields.

8. On the Data Options of the Column element, specify a value for the trim attribute:
9. Click the **Add** button and choose Add Same to add another column.
10. On the Basic tab of the Column element, specify values for the following attributes:

Index

The index of the column in the input file. In the example above, the column used for the second Index is the First Name column, which is Index two (2).

Name

Specify the name of the column.

Size

The size of the column. In the example above, the size is twelve (12).

11. On the Type Conversion tab of the Column element, specify values for the following attributes:

Type

The default type is Variable Character (VARCHAR). Specify a different type if needed.

Pattern

The pattern to use to format "Number Patterns" on page 797 or date/time fields.

12. On the Data Options of the Column element, specify a value for the trim attribute:
13. Repeat steps 10-13 for each column in the file. You can also specify a column name for each field, which can be referred to in later tasks by utilizing the Name attribute.
14. Click the **Save** button when finished.

Read Fixed-width Task

The Read Fixed-width task allows you to specify file and variable parameters for translating a fixed-width file into a RowSet variable.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single file to read the data from.
Input Files Variable	Specify the name of a variable of type File List which contains the files to read the data from. For example, ${variableName}.
Output RowSet Variable	Specify the name of a variable which will contain the data read from the specified input file(s). The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable. The variable will be created if it does not exist.

Advanced Tab	
Skip Invalid Records	Specify whether or not to ignore invalid records and continue on. The default is false, which will signal a error when invalid data is encountered. Default Value: false
Skip First Row	Specify whether or not to skip the first row of the input file(s). If the input file(s) contain header information in the first row, set this value to 'true'. Default Value: true
Record Delimiter	Specify the character or sequence of characters that are used to separate each record in the input file(s). The default record delimiter is CRLF (carriage return immediately followed by line feed). Default Value: CRLF
Encoding	Specify the character encoding of the input file(s). The default value is same as the platform's default file encoding. Default Value: The platform's default file encoding.
Output Variables Tab	
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Data Options

The Data Options element allows you to specify data format options for the fields in a fixed-width file.

Field	Definition
Basic Tab	

Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. By default no data is trimmed, i.e., all leading and trailing white spaces are preserved. This setting may also be overridden by the individual column settings.
Null Indicator	Specify the value that should be interpreted as null when reading the data from the input files. If the data in any column in any row matches the value specified here, it will be interpreted as a null. This value can be overridden by the individual columns.
Data Format Tab	
Whole Number Format	Specify the pattern used by the whole number fields (tinyint, smallint, int, bigint) in the input files. For example, ###,### (2,345). Please note that this setting will only be used if and only if there is at least one whole number (tinyint, smallint, int, bigint) type column defined under this data element. This value can be overridden by the individual columns.
Decimal Number Format	Specify the pattern used by the decimal number fields (real, float, double, decimal and numeric) in the input files. For example, $###,###.00 ($2,345.46). Please note that this setting will only be used if there is at least one decimal number (real, float, double, decimal, numeric) type column defined under this data element. This value can be overridden by the individual columns.
Date Format	Specify the pattern used by the date fields in the input file(s). For e.g. MM/dd/yyyy (08/02/2007). Please note that this setting will only be used if and only if there is at least one date type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd
Time Format	Specify the pattern used by the time fields in the input files. For e.g. hh:mm:ss a (08:12:56 PM). Please note that this setting will only be used if and only if there is at least one time type column defined under this data element. This value can be overridden by the individual columns. Default Value: HH:mm:ss
Timestamp Format	Specify the pattern used by the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). Please note that this setting will only be used if and only if there is at least one timestamp type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric, date/time data is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual column(s). Please note that this setting will only be used if and only if there is at least one numeric or date/time type column defined under this data element. Default Value: en_US
Alignment	Specify how the data in various columns was aligned in the input files. This value can be overridden on an individual column. Default Value: left
Padding Character	Specify the character that was used to pad the data in various columns. This value can be overridden on an individual column. Default Value: white space character

Column

The Column Field Element allows you to specify the data parameters for columns in a fixed-width file.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of this column.
Size	Specify the size (maximum numer of characters) of the column. This setting may not be used by this task but could be used by subsequent tasks that use the RowSet generated by this task.
Type Conversion Tab	
Type	Specify the data type of this column. For e.g. integer, date or decimal. Default Value: VARCHAR
Pattern	Specify the pattern that was used to format numeric or date/time fields. This will be used if and only if this column is defined as a numeric, date, time or timestamp type column. Default Value: Inherited from parent Data element.
Locale	Specify the locale to which the data in this column is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). Please note that this setting will only be used if and only if this column is defined as a numeric or date/time type column. Default Value: Inherited from parent Data element.
Data Options Tab	
Trim	Specify how the leading and trailing white spaces in this column should be trimmed. Default Value: Inherited from parent Data element.
Null Indicator	Specify the value that should be interpreted as null when reading the data from this column. If the data in this column in any row matches the value specified here, it will be interpreted as a null value. Default Value: Inherited from parent Data element.
Data Format Tab	
Alignment	Specify how the data is aligned in this column. Default Value: Inherited from parent Data element.
Padding Character	Specify the character that was used to pad the data in this column. Default Value: Inherited from parent Data element.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Write Fixed-width Task

The Write Fixed-width task will write a text file based on the contents of a "RowSet" on page 121. That variable can contain data from a database or from another file type like *CSV*, fixed-width, or *XML*.

If you only specify the Input RowSet Variable and Output File attributes, each column's length will be based on the metadata associated to the RowSet. If the RowSet contains numeric data or dates, you may want to

Specify Data Options through the **Add** button in the sub-menu to change the format or alignment of the columns. Column elements can be added to specify options for each column written.

Example 1: Write Fixed-width File

Follow the steps below to write a Fixed-width file. The input RowSet data being used in this example is based on the example data table in the "RowSet" on page 121.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Write Fixed-width task to the Project Outline.
2. On the Basic tab of the Write Fixed-width task, specify values for the following attributes:

   Input RowSet Variable

   The name of a variable of type RowSet which contains data to write to a file.

   Output File

   The "File Paths" on page 161 and file name of a single file to write.
3. On the Advanced tab of the Write Fixed-width task, specify the Include Column Headings value:

   Include Column Headings

   Whether or not to include column headings in the first row of the fixed-width file.
4. Click the **Add** button in the sub-menu and select the Specify Data Options menu item.
5. Click the **Add** button in the sub-menu and select the Add Column menu item.
6. On the Basic tab of the Write Fixed-width Column element, specify the Index value:

   Index

   The index of the column in the input RowSet.

   Size

   Specify the size of this column. The default size is determined by the largest column in the first 50 columns in the RowSet. In this example, the largest column from the input RowSet is six characters. Therefore, the default column size for each column is six. A setting of 10 will be used to add empty spaces between the columns to make the output more easily readable.
7. Repeat steps 5-6 to set the column size for each column in the RowSet.
8. Click the **Save** button when finished.

Write Fixed-width Task

The Write Fixed-width task allows you to specify file and data parameters for translating a RowSet variable into a fixed-width file

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input RowSet Variable	Specify the name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}
Output File	Specify the path and file name of a single file to write.
When Output File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Maximum Rows	Specify the maximum number of rows to be written to the output file. When this limit is reached, the remaining rows in the input RowSet will be silently skipped.
Encoding	Specify the character encoding of the output file. Default Value: The platform's default file encoding.
Include Column Headings	Specify whether or not to include column headings in fixed-width file. Default Value: true
Record Delimiter	Specify the character(s) to use for separating each record (or row) in the generated fixed-width file. Default Value: CRLF
User Friendly Output	Specify whether or not the generated output should be user-friendly. When this is set to true, the generated file will contain a separator line between each column. Default Value: false
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.

Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Data Options

The Data Options element allows you to specify data format options for the data written to the fixed-width file.

Field	Definition
Basic Tab	
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. By default no data is trimmed, leaving all leading and trailing white spaces. This setting may also be overridden by the individual column settings. Default Value: none
Null Substitute	Specify the value that should be written to the output file when any field in any row of the input RowSet has a null value. This value can be overridden by the individual columns.
Data Format Tab	
Whole Number Format	Specify the pattern to use for formatting the whole number fields (tinyint, smallint, int, bigint) in the output file. For e.g. ###,### (2,345). Please note that this setting will only be used if and only if there is at least one whole number (tinyint, smallint, int, bigint) type column defined under this data element. This value can be overridden by the individual columns.
Decimal Number Format	Specify the pattern to use for formatting the decimal number fields (real, float, double, decimal and numeric) in the output file. For e.g. $###,###.00 ($2,345.46). Please note that this setting will only be used if there is at least one decimal number (real, float, double, decimal, numeric) type column defined under this data element. This value can be overridden by the individual columns.
Date Format	Specify the pattern for formatting the date fields in the output file. For e.g. MM/dd/yyyy (08/02/2007). Please note that this setting will only be used if and only if there is at least one date type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd
Time Format	Specify the pattern to use for formatting the time fields in the input files. For e.g. hh:mm:ss a (08:12:56 PM). Please note that this setting will only be used if and only if there is at least one time type column defined under this data element. This value can be overridden by the individual columns. Default Value: HH:mm:ss

Timestamp Format	Specify the pattern to use for formatting the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). Please note that this setting will only be used if and only if there is at least one timestamp type column defined under this data element. This value can be overridden by the individual columns. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric and date/time data should be formatted. The locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual column(s). Please note that this setting will only be used if and only if there is at least one numeric or date/time type column defined under this data element. Default Value: en_US
Alignment	Specify how the data should be aligned in the columns. This value can be overridden based on the data type or at the individual column level. Default Value: left
Whole Number Alignment	Specify how whole numbers (INTEGER, BIGINT, SMALLINT and TINYINT) should be aligned. Default Value: Value specified in the Alignment field
Decimal Number Alignment	Specify how decimal numbers (DECIMAL, NUMERIC, FLOAT and REAL, DOUBLE) should be aligned. Default Value: Value specified in the Alignment field
Date Alignment	Specify how dates should be aligned. Default Value: Value specified in the Alignment field
Time Alignment	Specify how times should be aligned. Default Value: Value specified in the Alignment field
Timestamp Alignment	Specify how timestamps should be aligned. Default Value: Value specified in the Alignment field
Padding Character	Specify the character to use to pad the data in various columns. Data will be padded with this character when the actual size of the data is less than the size defined on the column, or the size obtained from the input RowSet's metadata. Please note that the left aligned columns will be padded on the right side, columns that are aligned right will be padded on the left, and columns with center alignment will be padded on both sides. Default Value: white space character
Decimal Field Width Formula	Specify the formula to use for determining the default size a decimal/numeric field occupies. This setting works only when the input RowSet metadata contains the decimal field's precision and scale information. Otherwise, the results will be unknown. Default Value: sign always/decimal always

Column

The Column Field Element allows you to specify the data parameters written to columns in a fixed-width file.

Field	Definition
Basic Tab	

Index	Specify the index of the column in the input RowSet. The first column starts with index 1. Either index or name must be specified to customize the output data. If both index and name are specified, the index value will be used.
Name	Specify the name of the column in the input RowSet. The column names are case insensitive. Either index or name must be specified to customize the output data. If both index and name are specified, the index value will be used. The name specified here overrides the input RowSet column name..
Size	Specify the size of this column. The default value is obtained from the input RowSet's metadata.
Type Conversion Tab	
Data Type	Specify the data type of this column. For e.g. integer, date or decimal. The data type specified here can be different than the actual data type in the input RowSet. If the data type is overridden, the task performs appropriate data type conversions when reading the data from the input RowSet. Default Value: Same as input data.
Pattern	Specify the pattern to use for formatting the data in this column. This will have effect if and only if the data type of this column is numeric, date, time or timestamp. The default pattern is taken from the parent Data element based on the type of this column. Default Value: Inherited from parent Data element.
Locale	Specify the locale to which the data in this column is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). The default locale is taken from the parent Data element. Please note that this setting will only be used if and only if this column is defined as a numeric or date/time type column. Default Value: Inherited from parent Data element.
Data Options Tab	
Trim	Specify how the leading and trailing white spaces in this column should be trimmed. The default is inherited from the parent Data element. Default Value: Inherited from parent Data element.
Null Substitute	Specify the value that should be written to the output file when this column of the input RowSet has a null value. The default is inherited from the parent Data element. Default Value: Inherited from parent Data element.
Data Format Tab	
Alignment	Specify how the data should be aligned in this column. Default Value: Inherited from parent Data element.
Padding Character	Specify the character that is used to pad the data in this column. Data is padded with this character when the actual size of the data is less than the size defined on the column, or the size obtained from the input RowSet's metadata. Please note that the left aligned columns will be padded on the right side, columns that are aligned right will be padded on the left, and columns with center alignment will be padded on both sides. Default Value: Inherited from parent Data element.

Read Flat File Task

The Read Flat File task reads records from a file that are delimited by a standard end of line character. The output from this task is a "RowSet" on page 121 variable, where each line will be a single column in the resulting RowSet. The RowSet can be used by an SQL task or be written to a different file format using one of Managed File Transfer's Write File tasks.

Example 1: Read Flat File

Follow the steps below to read the flat file data and load the data into a RowSet.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read Flat File task to the Project Outline.
2. On the Basic tab of the Read Flat File task, specify values for the following attributes:

   Input File

   The "File Paths" on page 161 and file name of a single file from which to read the data.

   Output RowSet Variable

   The name of a variable which will contain the data read from the specified input file(s).
3. On the Advanced tab of the Read Flat File task, specify the Record Delimiter type:

   Start Row

   Specify the row to start reading data from the file(s).

   Skip Empty Rows

   Specify whether or not to skip empty rows.

   Record Delimiter

   The character or sequence of characters that separate each record.
4. When complete, click the **Save** button.

Read Flat File Task

The Read Flat File task allows you to specify file and variable parameters for translating a flat file file into a RowSet variable.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single file to read the data from.
Input Files Variable	Specify the name of a variable of type File List which contains the files to read the data from. For example, ${variableName}.
Output RowSet Variable	Specify the name of a variable which will contain the data read from the specified input file(s). The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable. The variable will be created if it does not exist.
Advanced Tab	

Start Row	Specify the row to start reading data from the file(s). This setting allows any header rows to be skipped. The first row starts at 1.
Skip Empty Rows	Specify whether or not to skip empty rows. Rows with only spaces will also be skipped. Default Value: false
Record Delimiter	Specify the character or sequence of characters that are used to separate each record in the input file(s). The default record delimiter is CRLF (carriage return immediately followed by line feed). Default Value: CRLF
Encoding	Specify the file encoding. This is required if the files are using a different encoding than the platform's default. Default Value: The platform's default file encoding.
Data Format Tab	
Trim	Specify how the leading and trailing white spaces in the rows should be trimmed. By default no data is trimmed, i.e., all leading and trailing white spaces are preserved. Default Value: none
Null Indicator	Specify the value that should be interpreted as null when reading the data from the input files. If the data in any row matches the value specified here, it will be interpreted as a null.
Output Variables Tab	
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Read XML Task

The Read XML task can read data from *XML* files and load that data into a "RowSet" on page 121. That variable can then be used to import the data into a database or translated to another file type such as Excel, fixed-width, or *CSV*.

XML files by nature can contain multiple levels of elements and various data throughout them. Therefore you can add multiple RowSet elements to the Read XML Task by adding them through the **Add** button in the sub-menu. For example, you could have an XML file that contains customer information along with a list of the products they ordered. The customer information can be parsed into one RowSet and the list of products into another RowSet. Those variables can then be used to load two separate database tables.

Note: The path to an XML element or attribute is case sensitive. If the path is not typed correctly or if the case is wrong, an error will not be generated. If validating an XML file using an external Schema, type the path to the Schema file in the Schema URL box on the Advanced tab of the Read XML Task page. The URL syntax is: file://path/file.xsd

Example 1: Read XML File

Follow the steps below to read a XML file and load the data into a RowSet. The following page shot represents the input file:

```
<?xml version="1.0" encoding="UTF-8"?>
- <EmployeeData>
  - <employee id="34594">
      <firstName>Heather</firstName>
      <lastName>Banks</lastName>
      <hireDate>1/19/1998</hireDate>
      <deptCode>BB001</deptCode>
      <salary>72000</salary>
    </employee>
  - <employee id="34593">
      <firstName>Tina</firstName>
      <lastName>Young</lastName>
      <hireDate>4/1/2010</hireDate>
      <deptCode>BB001</deptCode>
      <salary>65000</salary>
    </employee>
</EmployeeData>
```

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read XML task to the Project Outline.
2. On the Basic tab of the Read XML task, specify values for the File attribute:

   File

   The "File Paths" on page 161 and file name of the XML file to read.
3. When complete, click the **Add** button and select **RowSet**.

4. On the Basic tab of the RowSet element, specify a value for the Variable Name attribute:

   Variable Name

   The name of a variable which will contain the parsed data. The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable.

5. When complete, click the **Add** button and select to add a Column.
6. On the Basic tab of the Column element, specify values for the following attributes:

   Index

   The index of the column in the input file(s). The first column starts with index 1.

   Value

   The path to the element or attribute from which this column should draw data. To retrieve data from an element, the element path should be defined like "/Element1/Element2/Element3". To retrieve data from an attribute, the attribute should be defined like "Element1/Element2/@Attribute".

7. When complete, click the **Add** button and select to add another Column
8. On the Basic tab of the Column element, specify values for the following attributes:

   Index

   The index of the column in the input file(s). The next column is index 2.

   Value

   The path to the element or attribute from which this column should draw data. To retrieve data from an element, the element path should be defined like "/Element1/Element2/Element3". To retrieve data from an attribute, the attribute should be defined like "Element1/Element2/@Attribute".

9. Click the **Add** button in the sub-menu and select the Add Same. Repeat steps 6-9 for each attribute or element you wish to retrieve.
10. Click the **Save** button when finished.

The following image illustrates the Project Outline for the Read XML task, and contains columns for each element and attribute read from the XML file:

The following table illustrates the data contained in the RowSet variable created from the XML Read task:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
34594	Heather	Banks	1998-01-19	BB001	72000
34593	Tina	Young	2010-04-01	BB001	65000

Example 2: Using Nested Shared Values to Correct XML Parsing

Informatica Managed File Transfer is designed to read very large XML documents in the fastest and most efficient way possible. For complex XML files, nested attribute values can cause a Project to create unexpected results in your output.

For example, the following Department XML elements contain two attributes; name and code.

```
<EmployeeData>
<Department name=”Infosec” code=”BB001”>
<Department name=”HR” code=”F02A1”>
```

```
<Department name=”Drafting” code=”BC940”>
</EmployeeData>
```

When you create the ReadXML task, you wish for the Department code values to appear before the Department name values. Your two column elements are defined as:

```
Index 1 - /EmployeeData/Department/@code
Index 2 - /EmployeeData/Department/@name
```

When you execute the Project, you expect your output to appear like this:

```
BB001 | Infosec
F02A1 | HR
BC940 | Drafting
```

Instead, the actual output is pairing the department names to the wrong department codes:

```
BB001|InfoSec
F02A1|InfoSec
F02A1|HR
BC940|HR
BC940|Drafting
```

Nested Shared Values

When Nested Shared Values is set to true, Managed File Transfer will correctly parse attributes and elements in the order in which they appear in the XML file.

Note: Nested Shared Values requires additional scanning of the XML file to produce an accurate output result set, and may increase the processing time for large XML files.Use the following instructions to enable Nested Shared Values:

1. In your Project Outline, select on the RowSet element on the Read XML Task.
2. Click the **Advanced** tab.
3. Set Nested Shared Values to true.
4. Click Save.

Read XML Task

The Read XML task allows you to specify file and variable parameters for translating an XML file into a RowSet variable.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of the XML file to read.
Input Files Variable	Specify the name of a variable of type File List which contains XML files to read. For example, ${variableName}
Advanced Tab	
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. This setting may also be overridden by the individual columns. Default Value: both

Null Indicator	Specify the value that should be interpreted as null when reading the data from the input files. If the data in any column in any row matches the value specified here, it will be interpreted as a null. This value can be overridden by the individual columns.
Skip Invalid Records	Specify whether or not to skip records that contain unparseable data. The default is 'false' which will throw an error and stop the task. Default Value: false
Data Format Tab	
Number Format	Specify the format of the number fields (tinyint, smallint, int, bigint, real, float, double, decimal and numeric) in the XML file being read. For e.g. ###,### (2,345) or $###,###.00 ($2,345.46). This value can be overridden by the individual columns.
Date Format	Specify the format of the date fields in the XML file being read. For e.g. MM/dd/yyyy (08/02/2007). This value can be overridden by the individual columns. Default Value: yyyy-MM-dd
Time Format	Specify the format of the time fields in the XML file being read. For e.g. hh:mm:ss a (08:12:56 PM). This value can be overridden by the individual columns. Default Value: HH:mm:ss
Timestamp Format	Specify the format of the timestamp fields in the XML file being read. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). This value can be overridden by the individual columns. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric and date/time data is formatted. The locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual columns. Default Value: en_US
XML Validation Tab	
Validation	Specify the type of validation to be performed. By default, validation is 'none' which means no validation is performed. Valid options are - none, schema, dtd Default Value: none
Schema URL	Specify the URL path to the schema source. Use this attribute only if the schema source to validate against is not already defined in the XML document, or to override the schema. Leaving this value blank will validate the document against the schema defined in the XML document. This attribute is ignored if validation is not set to schema.
When Validation Fails	Specify the action to take when a validation error occurs. By default, all validation errors will be logged to the job log and the project will continue. Note that any fatal errors encountered by the parser means that the XML document is unreliable and the project will fail regardless of this setting. Valid options are - ignore, log, error Default Value: error
Output Variables Tab	
Processed Input Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Add a RowSet Field Definitions

The Add a RowSet Element allows you to use XML Elements and Attributes to define the Column Elements that are stored in the RowSet variable that is created when the task executes.

Field	Definition
Basic Tab	
Variable Name	Specify the name of a variable which will contain the parsed data. The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable. The variable will be created if it does not exist.
Advanced Tab	
Nested Shared Values	Specify whether or not to allow nested, shared values to be read accurately. This will only work if the columns appear exactly according to the index order of the column sub elements. Default Value: false

Column

The Column Element allows you to specify the data parameters for columns in an XML file.

Field	Definition
Basic Tab	

Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of this column.
Size	Specify the size (maximum numer of characters) of the column. This setting may not be used by this task but could be used by subsequent tasks that use the RowSet generated by this task.
Type Conversion Tab	
Type	Specify the data type of this column. For e.g. integer, date or decimal. Default Value: VARCHAR
Pattern	Specify the pattern that was used to format numeric or date/time fields. This will be used if and only if this column is defined as a numeric, date, time or timestamp type column. Default Value: Inherited from parent Data element.
Locale	Specify the locale to which the data in this column is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). Please note that this setting will only be used if and only if this column is defined as a numeric or date/time type column. Default Value: Inherited from parent Data element.
Data Options Tab	
Foreign Key	Specify whether or not this column references a foreign key value. By declaring a column a foreign key, a record will be skipped even if a foreign key column contains data, so long as the rest of the non-foreign key columns are null (empty). Default Value: false
Trim	Specify how the leading and trailing white spaces in this column should be trimmed. Default Value: Inherited from parent Data element.
Null Indicator	Specify the value that should be interpreted as null when reading the data from this column. If the data in this column in any row matches the value specified here, it will be interpreted as a null value. Default Value: Inherited from parent Data element.

Write XML Task

The Write XML task will write an XML file based on the contents of one or more "RowSet" on page 121. Those variables can contain data from a database or from another file type like *CSV*, fixed-width, or Excel.

XML files consist of elements and attributes. Elements allow you to organize your data into a tree structure that is easy to traverse. Attributes can be added to specify options for those elements.

Example 1: Write XML File

The input RowSet data used in this example is based on the example data as it appears in the "RowSet" on page 121. Follow the steps below to write the XML file.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Write XML task to the Project Outline.
2. On the Basic tab of the Write XML task, specify the Output File value:

   Output File

   The "File Paths" on page 161 and file name of the XML file to write.
3. In the Write XML task window, from the **Add** button in the sub-menu, click **Element**. The first Element in the Project Outline will become the root node in the XML document.
4. On the Basic tab of the Element, specify a value for the following attributes:

   Name

   The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

   Enclose in CDATA

   Whether or not the text in the Value attribute should be wrapped in CDATA tags.
5. In the Element window, from the **Add** button in the sub-menu, click **For-Each**. The XML Write task's For-Each element iterates through each row in a RowSet variable.
6. On the Basic tab of the For-Each element, specify the Input RowSet Variable value:

   Input RowSet Variable

   The name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}.
7. In the For-Each window, from the Add link in the sub-menu, click **Element**.
8. On the Basic tab for the Element, specify the Name value:

   Name

   The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.
9. In the Element window, from the **Add** button in the sub-menu, click **Attribute**.
10. On the Basic tab of the Attribute element, specify values for the following attributes:

    Name

    The attribute name as it will appear in the output XML file. For example, <element attributeName="attributeValue" />.

    Value

    The value of this attribute. This may be expressed by a combination of constant values and RowSet column references. For example ${RowSetVariable[2]}, where RowSetVariable is the name of the variable of type RowSet and 2 is the column index of that RowSet. Please note that only RowSets which are in use by a parent For-Each element may be used.
11. From the Project Outline, select the element above the attribute, and from the Add link in the sub-menu, click **Element**.
12. On the Basic tab of the Element, specify a value for the following attributes:

Name

The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

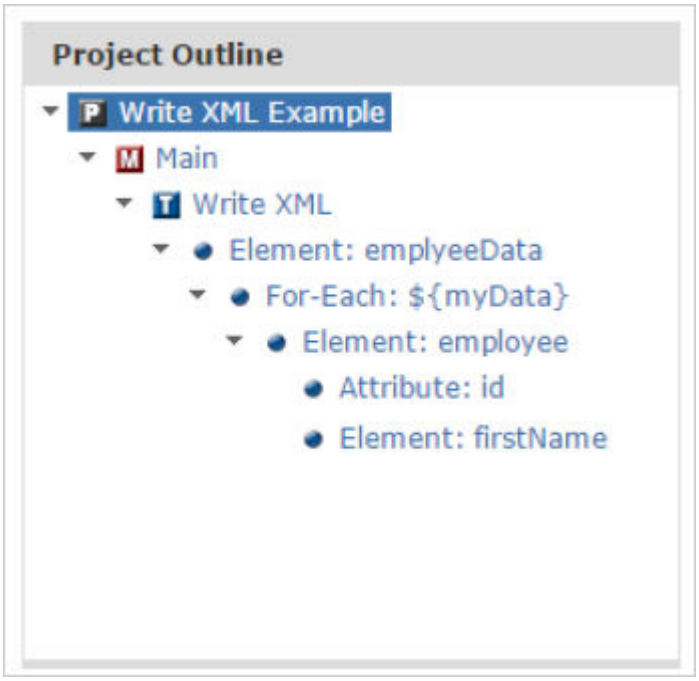
Enclose in CDATA

Whether or not the text in the Value attribute should be wrapped in CDATA tags.

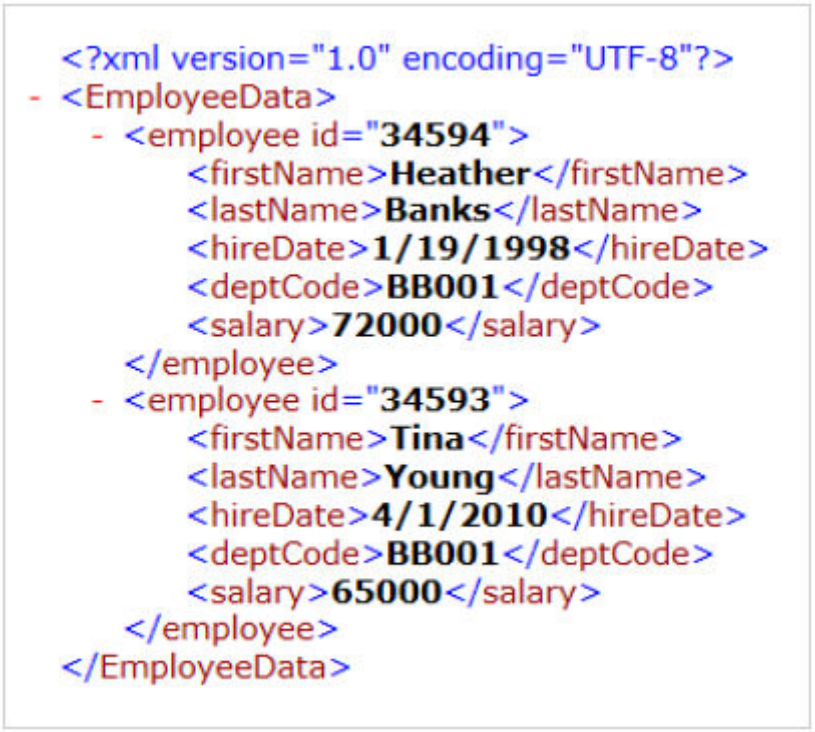
13. If needed, add additional Attributes, from the Add link in the sub-menu by selecting the **Add Same** option. Repeat step 11 for each attribute.

14. Click the **Save** button when finished.

The following image illustrates the Project Outline for the Write XML task:



The following image illustrates the XML file created from the Write XML task:



Example 2: Write XML Task Using IF Element

The XML IF element is used to write XML elements based on Primary Key/Foreign Key or Header/Detail relationships. The test condition only compares the value from one RowSet variable to the value from another RowSet variable. The two valid comparison operators are 'eq' (equals) and 'ne' (not equals).

Example Test Condition: ${orderHeader[OrderNum]} eq ${orderDetails[OrderNum]}

In the following example, RowSet data from two "Database Tasks" on page 267 tasks will be written to a single XML file. The 'orderHeader' RowSet data will be merged with the 'orderDetails' RowSet data using the 'OrderNum' column as the primary key. This task will be accomplished using two nested loops. The outer For-Each element will loop through the 'orderHeader' variable while the inner For-each element will loop through the 'orderDetails' loop.

Here is an example of the 'orderHeader' RowSet data. The rows have been color-coded to illustrate the relationship of the 'OrderNum' column with the data in the 'orderDetails' RowSet:

${orderHeader} RowSet Variable		
${orderHeader[OrderNum]}	${orderHeader[TotShipped]}	${orderHeader[TotCharge]}
25565	3	50
25566	2	100
25567	3	50

Here is an example of the 'orderDetails' RowSet data:

${orderDetails} RowSet Variable			
${orderDetails[OrderNum]}	${orderDetails[PartNumber]}	${orderDetails[TotPieces]}	${orderDetails[TotCharge]}
25565	WC0324	1	20
25565	CBJS01	1	20
25565	GBVVVDS	1	10
25566	DVBF066	2	100
25567	CBJS01	2	40
25567	GBVVVDS	1	10

Use the following instructions to create an XML file using the Write XML IF element:

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Write XML task to the Project Outline.
2. On the Basic tab of the Write XML task, specify the Output File value:

   Output File

   The "File Paths" on page 161 and file name of the XML file to write.
3. In the Write XML task window, from the **Add** button in the sub-menu, click **Element**. The first Element in the Project Outline will become the root node in the XML document.

4. On the Basic tab of the Element, specify a value for the following attributes:

   Name

   The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

   Enclose in CDATA

   Whether or not the text in the Value attribute should be wrapped in CDATA tags.

5. In the Element window, from the **Add** button in the sub-menu, click **For-Each**. The XML Write task's For-Each element iterates through each row in a RowSet variable. The first For-Each (outer loop) element in this example loops through the 'orderHeader' RowSet variable.
6. On the Basic tab of the For-Each element, specify the Input RowSet Variable value:

   Input RowSet Variable

   The name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}.

7. In the For-Each window, from the **Add** button in the sub-menu, click **Element**.
8. On the Basic tab for the Element, specify the Name value:

   Name

   The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

9. In the Element window, from the **Add** button in the sub-menu, click **Attribute**.
10. On the Basic tab of the Attribute element, specify values for the following attributes:

    Name

    The attribute name as it will appear in the output XML file. For example, <element attributeName="attributeValue" />.

    Value

    The value of this attribute. This may be expressed by a combination of constant values and RowSet column references. For example ${RowSetVariable[OrderNum]}, where RowSetVariable is the name of the variable of type RowSet andOrderNum is the column index name of that RowSet. Please note that only RowSets which are in use by a parent For-Each element may be used.

11. Form the Project Outline, select the 'order' element created in step 9. In the 'order' Element window, from the **Add** button in the sub-menu, click **For-Each**. The second For-Each element (inner loop) in this example loops through the 'orderDetails' RowSet variable.
12. On the Basic tab of the For-Each element, specify the Input RowSet Variable value:

    Input RowSet Variable

    The name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}.

13. From the Project Outline, select the element above the attribute, and from the **Add** button in the sub-menu, click **If**.
14. On the Basic tab of the If element, specify a value for the following attributes:

Test Condition

The comparison between the value of one RowSet variable to another. In this example, the data in the 'OrderNum' column is being compared with the 'orderHeader' and 'orderDetails' RowSets. If the value of the two variables are equal, the next element in the Write XML task will be written to the XML file.
Example Test Condition: ${orderHeader[OrderNum]} eq ${orderDetails[OrderNum]}

15. In the IF window, from the **Add** button in the sub-menu, click **Element**.
16. On the Basic tab of the Element, specify a value for the following attributes:

    Name

    The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

17. In the Element window, from the **Add** button in the sub-menu, click **Attribute**.
18. On the Basic tab of the Attribute element, specify values for the following attributes:

    Name

    The attribute name as it will appear in the output XML file. For example, <element attributeName="attributeValue" />.

    Value

    The value of this attribute. This may be expressed by a combination of constant values and RowSet column references. For example ${RowSetVariable[OrderNum]}, where RowSetVariable is the name of the variable of type RowSet and OrderNum is the column index name of that RowSet. Please note that only RowSets which are in use by a parent For-Each element may be used.

19. Form the Project Outline, select the 'part' element created in step 17. In the 'part' Element window, from the **Add** button in the sub-menu, click **Element**.
20. On the Basic tab of the Element, specify a value for the following attributes:

    Name

    The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

    Value

    The value of this attribute. This may be expressed by a combination of constant values and RowSet column references. For example ${RowSetVariable[OrderNum]}, where RowSetVariable is the name of the variable of type RowSet andOrderNum is the column index name of that RowSet. Please note that only RowSets which are in use by a parent For-Each element may be used.

21. Form the Project Outline, select the 'part' element created in step 16. In the 'part' Element window, from the **Add** button in the sub-menu, click **Element**.
22. On the Basic tab of the Element, specify a value for the following attributes:

    Name

    The element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.

    Value

    The value of this attribute. This may be expressed by a combination of constant values and RowSet column references. For example ${RowSetVariable[OrderNum]}, where RowSetVariable is the name

of the variable of type RowSet andOrderNum is the column index name of that RowSet. Please note that only RowSets which are in use by a parent For-Each element may be used.

23. Click the **Save** button when finished.

Write XML Task

The Write XML task allows you to specify file and data parameters for translating a RowSet variable into a XML file

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Output File	Required field. Specify the path and file name of the XML file to write.
When File Exists	Specify the action to take when the XML file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
XML Header	Specify the XML Header information that will be written to the XML document before the root element. Header information contains lines such as the XML processing information, DTD, Schema definitions, stylesheet definitions, etc. The default header is <?xml version="1.0" encoding="UTF-8" ?>, but may be overwritten. In order to completely remove the header, specify the ${system.emptyString} variable as the header value. Default Value: <?xml version="1.0" encoding="UTF-8" ?>
Tidy Output	Specify whether or not to use indentation so that the output is more legible. Default Value: true
Trim	Specify how the leading and trailing white spaces in the fields should be trimmed. This setting may also be overridden by the individual element and attribute settings. Default Value: none
Null Substitute	Specify the value that should be written to the output file when any field in any row of the input RowSet has a null value. The default value in an empty string. This value can be overridden by the individual columns.
Encoding	Specify the encoding to use when writing the output file. It is strongly recommended that this value be the same as the encoding specified in the XML header. Default Value: UTF-8
Data Format Tab	
Number Format	Specify the pattern to use for formatting the number fields (tinyint, smallint, int, bigint, real, float, double, decimal and numeric) in the output file. For e.g. ###,### (2,345) or $###,###.00 ($2,345.46). This value can be overridden by the individual elements and attributes.
Date Format	Specify the pattern for formatting the date fields in the output file. For e.g. MM/dd/yyyy (08/02/2007). This value can be overridden by the individual elements and attributes. Default Value: yyyy-MM-dd

Time Format	Specify the pattern to use for formatting the time fields in the input files. For e.g. hh:mm:ss a (08:12:56 PM). This value can be overridden by the individual elements and attributes. Default Value: HH:mm:ss
Timestamp Format	Specify the pattern to use for formatting the timestamp fields in the input files. For e.g. MMM dd, yyyy hh:mm:ss a (Aug 02, 2007 08:12:56 PM). This value can be overridden by the individual elements and attributes. Default Value: yyyy-MM-dd HH:mm:ss.SSS
Locale	Specify the locale to which the locale sensitive data such as numeric and date/time data should be formatted. The locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). If needed, the locale may be overridden on the individual elements and attributes. Default Value: en_US
XML Validation Tab	
Validation	Specify the type of validation to be performed. By default, validation is 'none' which means no validation is performed. Valid options are - none, schema, dtd Default Value: none
Schema URL	Specify the URL path to the schema source. Use this attribute only if the schema source to validate against is not already defined in the XML document, or to override the schema. Leaving this value blank will validate the document against the schema defined in the XML document. This attribute is ignored if validation is not set to schema.
When Validation Fails	Specify the action to take when a validation error occurs. By default, all validation errors will be logged to the job log and the project will continue. Note that any fatal errors encountered by the parser means that the XML document is unreliable and the project will fail regardless of this setting. Valid options are - ignore, log, error Default Value: error
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the output XML file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Element

Allows you specify XML elements and their parameters to your XML file.

Field	Definition
Basic Tab	
Name	Required field. Specify the element name as it will appear in the output XML file. An element is an XML tag. For example, <tagName>.
Value	Specify the value that will appear in this element. This may be expressed by a combination of constant values and RowSet column references, such as ${rowset[1]}. Only RowSets which are in use by a parent ForEach element may be used.
Skip if Empty	Specify whether or not this element should be skipped (not written to the output file) if the element does not contain any attributes or child elements. If any attributes or child elements exists, then this value will be ignored. Default Value: false
Enclose in CDATA	Specify whether or not this element's value should be enclosed in a CDATA section. For example, <![CDATA[value. Default Value: false
Type Conversion Tab	
Type	Specify the data type of this element For e.g. integer, date or decimal. If left blank, the input RowSet will be queried to obtain the type element. If the type cannot be determined from the RowSet, it defaults to VARCHAR. The data type specified here can be different than the actual data type in the input RowSet. If the data type is overridden, the task performs appropriate data type conversions when reading the data from the input RowSet. Default Value: Same as input.
Pattern	Specify the pattern to use for formatting the data in this element. This will have effect if and only if the data type of this column is numeric, date, time or timestamp. Default Value: Inherited from the parent Task element.
Locale	Specify the locale to which the data in this element is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). Please note that this setting will only be used if and only if this element is defined as a numeric or date/time type element. Default Value: Inherited from the parent Task element.

Data Options Tab	
Trim	Specify how the leading and trailing white spaces in this element should be trimmed. Default Value: Inherited from the parent Task element.
Null Substitute	Specify the value that should be written to the output file when this element of the input RowSet has a null value. Default Value: Inherited from the parent Task element.

Attribute

Allows you to add attributes to XML elements and specify the attribute's parameters.

Field	Definition
Basic Tab	
Name	Required field. Specify the attribute name as it will appear in the output XML file. For example, <element attributeName="attributeValue" />.
Value	Required field. Specify the value of this attribute. This may be expressed by a combination of constant values and RowSet column references. For example ${rowsetVariable[2]}, where rowsetVariable is the name of the variable of type RowSet and 2 is the column index of that RowSet. Please note that only RowSets which are in use by a parent For-Each element may be used.
Type Conversion Tab	
Type	Specify the data type of this element For e.g. integer, date or decimal. If left blank, the input RowSet will be queried to obtain the type element. If the type cannot be determined from the RowSet, it defaults to VARCHAR. The data type specified here can be different than the actual data type in the input RowSet. If the data type is overridden, the task performs appropriate data type conversions when reading the data from the input RowSet. Default Value: Same as input.
Pattern	Specify the pattern to use for formatting the data in this element. This will have effect if and only if the data type of this column is numeric, date, time or timestamp. Default Value: Inherited from the parent Task element.
Locale	Specify the locale to which the data in this element is formatted. The Locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). Please note that this setting will only be used if and only if this element is defined as a numeric or date/time type element. Default Value: Inherited from the parent Task element.
Data Options Tab	

Trim	Specify how the leading and trailing white spaces in this element should be trimmed. Default Value: Inherited from the parent Task element.
Null Substitute	Specify the value that should be written to the output file when this element of the input RowSet has a null value. Default Value: Inherited from the parent Task element.

For-Each

The For-Each element allows you to loop through data in a RowSet variable.

Field	Definition
Basic Tab	
Name	Required field. Specify the name of a variable of type RowSet which contains data to write to a file. For example, ${variableName}
Sorted	Specify whether or not the RowSet is sorted by the key column, allowing more efficient operation. Default Value: unsorted

If

The XML If element is used to write XML elements based on Primary Key/Foreign Key or Header/Detail relationships. The test condition requires a value from one RowSet variable to be compared against the value from another RowSet variable.

Field	Definition
Basic Tab	
Test Condition	Required field. Specify the comparison to perform. Only two comparison operators are supported, 'ne' and 'eq.'
Case Sensitive	Specify whether or not this comparison should ignore the difference between capital and lower case letters. Default Value: true

Modify RowSet

The Modify RowSet task allows you to add, modify, or delete columns from a "RowSet" on page 121 that was generated by tasks that read the contents of a file or database (for example, SQL or Read CSV tasks). The results of the Modify RowSet task are saved to an Output RowSet variable.

You have the option of modifying the existing columns and their index order, or you can define new columns with an index order of your choosing. Modifying existing columns is useful when the RowSet data needs slight modifications to meet the desired requirements. Identifying all new columns is preferred when the Input RowSet requires several changes to RowSet data and/or drastic changes to the column Index order.

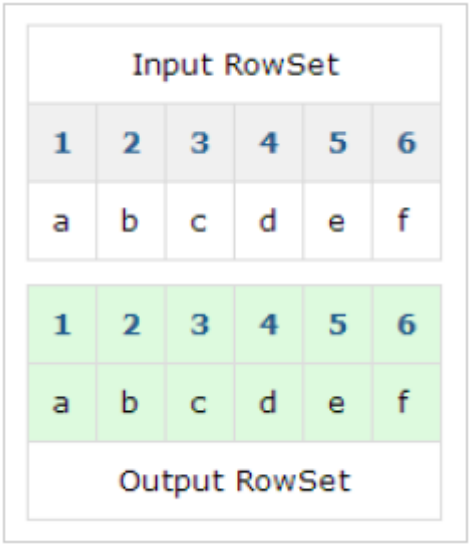
RowSet Processing Explained

Each column in a RowSet is identified by an Index number, beginning at 1. The processing example below illustrates how Managed File Transfer executes the New Column, Modify Column, and Remove Column elements when using existing columns.

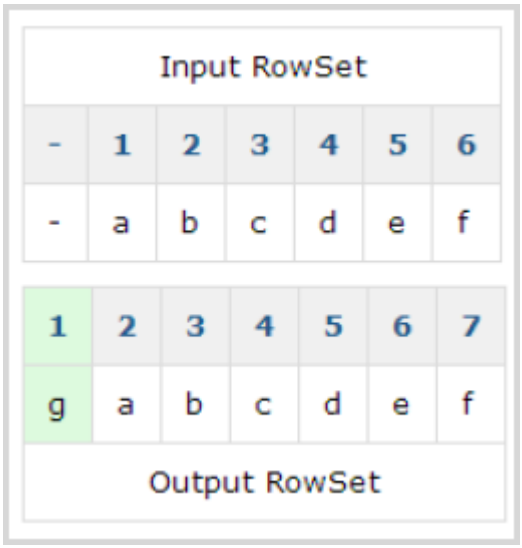
The example Input RowSet variable contains 1 row of data, 6 columns (Indexes), and will execute the following elements:

1. A new column will be inserted into the Output RowSet at Index 1.
2. The column at Index 3 will be modified with a new value.
3. The column at Index 5 will be removed.
4. A new column will be created at Index 5.

1. When Managed File Transfer begins the Modify RowSet task, all the columns from the Input RowSet variable are mapped to the new Output RowSet variable.



2. The newColumn:1 element is processed. The new column is inserted into the Output RowSet at Index 1 with a value of 'g'. The Indexes and values in the Output RowSet have been shifted to the right, but still maintain their mapped links to the Input RowSet.



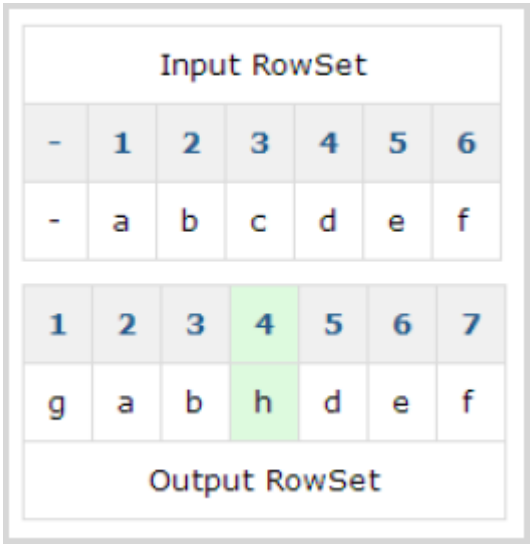
Input RowSet

-	1	2	3	4	5	6
-	a	b	c	d	e	f

1	2	3	4	5	6	7
g	a	b	c	d	e	f

Output RowSet

3. The modifyColumn:3 from the Input RowSet variable is processed. Column 4 of the Output RowSet has a new value of 'h'. This is because the value from the Input RowSet column 3 was mapped to the value of the Output RowSet column 4.



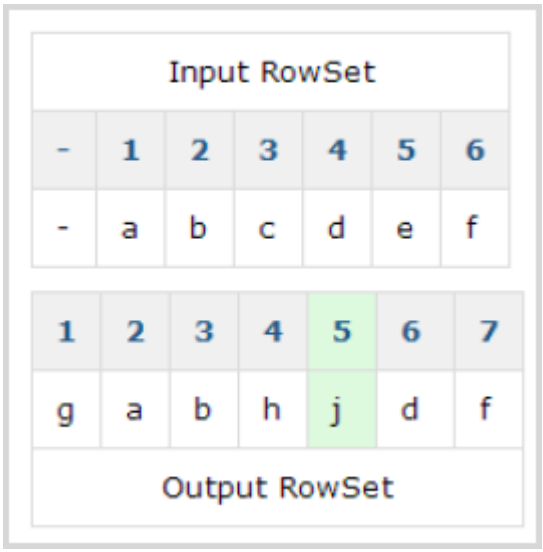
Input RowSet

-	1	2	3	4	5	6
-	a	b	c	d	e	f

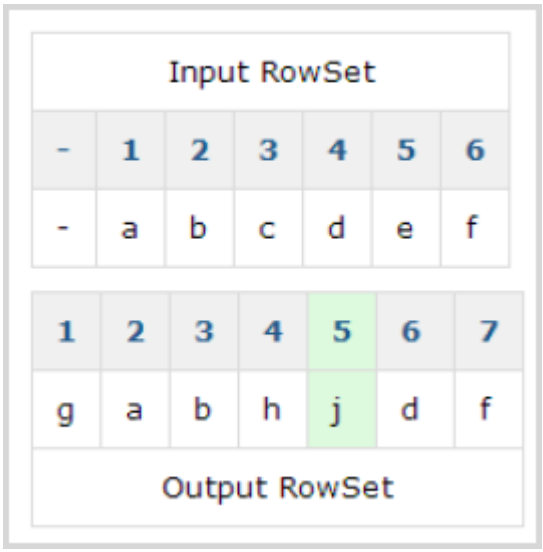
1	2	3	4	5	6	7
g	a	b	h	d	e	f

Output RowSet

4. The removeColumn:5 element is processed. Column 5 from the Input RowSet will not be included in the Output RowSet.



5. Finally, the newColumn:5 element is processed. A new Column at Index 5 has been inserted with a value of 'j'. The existing Indexes and values have been shifted to the right.



Example 1: Modify a RowSet Using Existing Columns

In this example, a Read CSV task creates a RowSet variable named myData that contains 6 columns of data. The following graphic illustrates the data contained in the RowSet:

Example Data:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
34594	Heather	Banks	1998-01-19	BB001	72000

34593	Tina	Young	2010-04-01	BB001	65000
34590	Kathy	Harris	2007-09-30	KH001	105000
34592	Mark	Walker	2012-11-15	KH001	87500
34591	John	Davis	2001-06-15	KH001	85000

The Modify RowSet task will be used to add a new column at Index 4, modify the value of the data in column 3, and remove column 5. Follow the steps below to use data from a RowSet, modify existing columns, and output the results to a new RowSet:

Note: Before adding a Modify RowSet task, you must have an Output RowSet variable from another task. The Output RowSet variable is used as the Input RowSet variable on the Modify RowSet task.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Modify RowSet task to the Project Outline.
2. On the Basic tab of the Modify RowSet task, specify the following values:

   Input RowSet Variable

   Specify the name of a variable of type RowSet which contains the data to modify. For example, ${myData}.

   Output RowSet Variable

   Specify the name of the variable that will contain the modified data. This will be a variable type of RowSet. If this variable exists it will be overwritten, otherwise it will be created.

   Start With Existing Columns

   Choose if you want to start with all columns from the input RowSet (true) or would rather specify which columns you want specifically (false). Choose true.
3. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add New Column**.
4. Specify the Index where the new column will be added, and the column value that will be written to the Output RowSet variable. In the example, a new column will be created at Index 4. The column will contain the value "Chicago."
5. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Modify Column**.
6. Specify the Index for the column to modify, and enter a new column value. In the example, the string data in column 3 will be converted to uppercase text (i.e. from 'James' to 'JAMES').
7. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Remove Column**.
8. Specify the Index for the column you want to remove.
9. Click the **Save** button when finished.

   The modifiedData RowSet Variable will contain 6 columns.

${modifiedData} RowSet Variable					
${modifiedData[1]}	${modifiedData[2]}	${modifiedData[3]}	${modifiedData[4]}	${modifiedData[5]}	${modifiedData[6]}

34594	Heather	BANKS	Chicago	1998-01-19	72000
34593	Tine	YOUNG	Chicago	2010-04-01	65000
34590	Kathy	HARRIS	Chicago	2007-09-30	105000
34592	Mark	WALKER	Chicago	2012-11-15	87500
34591	John	DAVIS	Chicago	2001-06-15	85000

Example 2: Modify RowSet Using Existing Columns

In this example, a Read CSV task creates a RowSet variable named myData that contains 6 columns of data. The following graphic illustrates the CSV data contained in the RowSet:

Example data:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
34594	Heather	Banks	1998-01-19	bb001	72000
34593	Tina	Young	2010-04-01	bb001	65000
34590	Kathy	Harris	2007-09-30	kh001	105000
34592	Mark	Walker	2012-11-15	kh001	87500
34591	John	Davis	2001-06-15	kh001	85000

The Modify RowSet task will be used to modify the column at Index 5, and remove columns 1 and 2. Also, any rows that contain a number greater that 80000 at Index 6 will be excluded in the Output RowSet variable. Follow the steps below to use data from a RowSet, modify existing columns, and output the results to a new RowSet:

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read CSV task to the Project Outline.
2. On the Basic tab of the Read CSV task, specify the following values:

   Input File

   Specify the path and file name of a single file to read the data from.

   Output Row

   Set VariableSpecify the name of a variable which will contain the data read from the specified input file(s). The variable will be of type RowSet and may be used in subsequent tasks that accept a RowSet input variable. The variable will be created if it does not exist. For this example, the variable myData was used.
3. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Modify RowSet task to the Project Outline.

   1.

   2. On the Basic tab of the Modify RowSet task, specify the following values:

Input RowSet VariableSpecify the name of a variable of type RowSet which contains the data to modify. For example, ${myData}.

Output RowSet VariableSpecify the name of the variable that will contain the modified data. This will be a variable type of RowSet. If this variable exists it will be overwritten, otherwise it will be created.

Start With Existing ColumnsChoose if you want to start with all columns from the input RowSet (true) or would rather specify which columns you want specifically (false). Choose true.

Exclude Row IfSpecify a condition that will exclude a row if it is satisfied and prevent it from being included in the output variable. In this example any row that contains an amount greater than 80000 in column 6 will be excluded.

1. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Modify Column**.
2. Specify the Index for the column to modify, and enter a new column value. In the example, the string data in column 5 will be converted to uppercase text (i.e. from 'bb001' to 'BB001').
3. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Remove Column**.
4. Specify the Index for the column you want to remove. In the example, the column at Index 1 will be removed.
5. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Remove Column**.
6. Specify the Index for the column you want to remove. In the example, the column at Index 2 will be removed.
7. When the Project executes, the modifiedData RowSet Variable will contain 4 columns. Rows that contained an amount greater than 80000 from column 6 of the Input RowSet are removed.
   The following image illustrates the Project Outline for the Modify RowSet task:

4. On the Basic tab of the Modify RowSet task, specify the following values:

   Input RowSet Variable

   Specify the name of a variable of type RowSet which contains the data to modify. For example, ${myData}.

   Output Row

   Set VariableSpecify the name of the variable that will contain the modified data. This will be a variable type of RowSet. If this variable exists it will be overwritten, otherwise it will be created.

   Start With Existing Columns

   Choose if you want to start with all columns from the input RowSet (true) or would rather specify which columns you want specifically (false). Choose true.

   Exclude Row If

   Specify a condition that will exclude a row if it is satisfied and prevent it from being included in the output variable. In this example any row that contains an amount greater than 80000 in column 6 will be excluded.

5. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Modify Column**.
6. Specify the Index for the column to modify, and enter a new column value. In the example, the string data in column 5 will be converted to uppercase text (i.e. from 'bb001' to 'BB001').

7. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Remove Column**.
8. Specify the Index for the column you want to remove. In the example, the column at Index 1 will be removed.
9. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add Remove Column**.
10. Specify the Index for the column you want to remove. In the example, the column at Index 2 will be removed.
11. When the Project executes, the modifiedData RowSet Variable will contain 4 columns. Rows that contained an amount greater than 80000 from column 6 of the Input RowSet are removed.

Example Output RowSet Data:

${modifiedData} RowSet Variable			
${modifiedData[1]}	${modifiedData[2]}	${modifiedData[3]}	${modifiedData[4]}
Banks	1998-01-19	BB001	72000
Young	2010-04-01	BB001	65000

Example 3: Modify RowSet Using New Columns with a SQL Task

In this example, an SQL query creates a RowSet variable named myData with 6 columns of data. The following graphic illustrates the data contained in the RowSet:

Example data:

${myData} RowSet Variable					
${myData[1]}	${myData[2]}	${myData[3]}	${myData[4]}	${myData[5]}	${myData[6]}
34594	Heather	Banks	1998-01-19	BB001	72000
34593	Tina	Young	2010-04-01	BB001	65000
34590	Kathy	Harris	2007-09-30	KH001	105000
34592	Mark	Walker	2012-11-15	KH001	87500
34591	John	Davis	2001-06-15	KH001	85000

The Modify RowSet task will be used to create a new RowSet variable that only contains columns 1,3, and 6 from the original RowSet. Follow the steps below to use the data from the original RowSet, create columns and specify their value, and then output the results to a new RowSet.

Note: Before adding a Modify RowSet task, you must have an Output RowSet variable from another task. The Output RowSet variable is used as the Input RowSet variable on the Modify RowSet task.

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Modify RowSet task to the Project Outline.
2. On the Basic tab of the Modify RowSet task, specify the following values:

Input RowSet Variable

Specify the name of a variable of type RowSet which contains the data to modify. For example, ${myData}.

Output RowSet Variable

Specify the name of the variable that will contain the modified data. This will be a variable type of RowSet. If this variable exists it will be overwritten, otherwise it will be created.

Start With Existing Columns

Choose if you want to start with all columns from the input RowSet (true) or would rather specify which columns you want specifically (false). Choose false.

3. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add New Column**.
4. Specify the Index where the new column will be added, and the column value that will be written to the Output RowSet variable. In the example, a new column will be created at Index 1 and will contain the value of column 1 from input RowSet variable.
5. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add New Column**.
6. Specify the Index where the new column will be added, and the column value that will be written to the Output RowSet variable. In the example, a new column will be created at Index 2 and will contain the value of column 3 from input RowSet variable.
7. In the Modify RowSet task window, from the **Add** button in the sub-menu, click **Add New Column**.
8. Specify the Index where the new column will be added, and the column value that will be written to the Output RowSet variable. In the example, a new column will be created at Index 3 and will contain the value of column 6 from input RowSet variable.
9. Click the **Save** button when finished.
10. The modifiedData RowSet variable will contain 3 columns.

Example Output RowSet Data:

${modifiedData} RowSet Variable		
${modifiedData[1]}	${modifiedData[2]}	${modifiedData[3]}
34594	Banks	72000
34593	Young	65000
34590	Harris	105000
34592	Walker	87500
34591	Davis	85000

Modify RowSet Task

The Modify RowSet task allows you to add, modify, or delete columns from a "RowSet" on page 121 that was generated by tasks that read the contents of a file or database (for example, SQL or Read CSV tasks).

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input RowSet Variable	Specify the name of a variable of type RowSet which contains the data to modify. For example, ${variableName}.
Output RowSet Variable	Specify the name of the variable that will contain the modified data. This will be a variable type of RowSet. If this variable exists it will be overwritten, otherwise it will be created.
Start With Existing Columns	Specify whether the output RowSet initially contains the column layout from the input RowSet (true), or if all new columns must be created (false). Default Value: true
Exclude Row If	Specify a condition that will exclude a row if it is satisfied and prevent it from being included in the output variable.
Include Row If	Specify a condition that will include a row if it is satisfied and allow it to be included in the output variable.
Advanced Tab	
Start At Row	Specify which row from the input RowSet should be the starting point for processing.
Maximum Rows	Specify the maximum number of rows that should be written to the output variable.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

New Column

The New Column Element allows you to add a new column to the RowSet variable.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of the column.
Value	Specify the value for this variable.
Advanced Tab	
Type	Specify the data type of this column. For e.g. integer, date or decimal. Default Value: VARCHAR
Size	Specify the size (maximum number of characters) of the column. The value specified here determines the field boundaries.

Modify Column

The Modify Column element allows you to modify the value of an existing column in a RowSet variable.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.
Name	Specify the name of the column.
Value	Specify the value for this variable.
Advanced Tab	
Type	Specify the data type of this column. For e.g. integer, date or decimal. Default Value: VARCHAR
Size	Specify the size (maximum number of characters) of the column. The value specified here determines the field boundaries.

Remove Column

The Remove Column element allows you to remove a column from an existing RowSet variable.

Field	Definition
Basic Tab	
Index	Specify the index of the column in the input file(s). The first column starts with index 1.

Email Tasks

Email tasks can send and retrieve emails.

Send Email Task

The Send Email task can be used to send email using standard SMTP (Simple Mail Transfer Protocol). Email can be sent to multiple recipients and can also include one or more attachments. This task can be used for a variety of purposes, including sending business documents (for example, spreadsheets, PDFs, etc.) to trading partners, sending alerts when Projects encounter problems, or sending SMS text messages.

Emails can be optionally encrypted and digitally signed using S/MIME standards. Encrypting the email will protect the contents and can only be deciphered by a recipient with the appropriate Private Key. Digital signatures may also be added to allow the recipient to verify your identity. Refer to the "Quick Start for Secure Email" on page 719 to learn more about the Sign Message and Encrypt Message attributes on the Advanced tab.

Example 1: Send Email

A department has requested a status report to be sent to them via email on a weekly basis. The following task creates the email, attaches the status report and then sends the email.

1. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Send Email task to the Project Outline.
2. On the Basic tab of the Send Mail task, specify values for the following attributes:

   SMTP Server

   The "SMTP Servers Resource" on page 78

   From

   The email address of the sender.

   To

   The email addresses of the recipients. Multiple email addresses should be separated by a comma.

   Subject

   The subject of the email.

   MessageThe message body text.
3. Click the **Add** button in the sub-menu and select the **Add Attachment** option. You can browse for the "File Paths" on page 161 by clicking the  button.
4. When the file is selected, click the **Save** button.

Example 2: Send an SMS or MMS Message

The Send Email task can be used to send a *SMS* text message by sending an email to a recipient's cellular number at their wireless carrier's domain. For example, sending an email to 4029444242@vtext.com will send an SMS text message to a wireless telephone number carried by Verizon Wireless. The following list contains the SMS email addresses for the for the most popular cellular phone carriers:

- AT&T: phonenumber@txt.att.net

- Cingular: phonenumber@cingularme.com
- Nextel: phonenumber@messaging.nextel.com
- Sprint: phonenumber@messaging.sprintpcs.com
- T-Mobile: phonenumber@tmomail.net
- Verizon: phonenumber@vtext.com
- Virgin Mobile: phonenumber@vmobl.com
  The Send Email task can also send a *MMS* message with attachments to wireless carriers that support that feature. Typically, a wireless carrier's domain for MMS messages is different than their SMS domain. Not all carriers support all file types. The following list contains the MMS email address for the most popular cellular phone carriers:
- AT&T: phonenumber@mms.att.net
- Cingular: phonenumber@mms.mycingular.com
- Nextel: phonenumber@messaging.nextel.com
- Sprint: phonenumber@pm.sprint.com
- T-Mobile: phonenumber@tmomail.net
- Verizon: phonenumber@vzwpix.com
- Virgin Mobile: phonenumber@vmpix.com

Note: Message and data rates may apply.

Use the following instructions to send a MMS text message to a cellular device:

1. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Send Email task to the Project Outline.
2. On the Basic tab of the Send Mail task, specify values for the following attributes:

   SMTP Server

   The "SMTP Servers Resource" on page 78 that will send the message to the wireless carrier.

   From

   The email address of the sender.

   To

   The telephone number and domain of the recipients. Multiple telephone numbers and domains should be separated by a comma.

   Subject

   The subject of the email.

   Message

   The message body text.
3. Click the **Add** button in the sub-menu and select the **Add Attachment** option. You can browse for the "File Paths" on page 161 by clicking the ... button.
4. When the file is selected, click the **Save** button.

Send Email Task

The Send Email task can be used to send email using standard SMTP (Simple Mail Transfer Protocol).

Field	Definition
Basic Tab	
Label	Specify a label for this task.
SMTP Server	Select a pre-configured SMTP server from the drop-down list.
From	Specify the email address of the sender. Emails will appear as sent from this email address. Only one 'From' email address is allowed.
To	Specify the email addresses of the recipients. Multiple email addresses should be separated by a comma.
Subject	Specify the subject of the email.
Message	Specify the message body text.
Advanced Tab	
CC	Specify the email addresses that should receive a carbon copy (CC) of this email. Multiple email addresses should be separated by a comma.
BCC	Specify the email addresses that should receive a blind carbon copy (BCC) of this email. Multiple email addresses should be separated by a comma.
Reply To	Specify the email addresses that should be replied to.
Request DSN	Specify the DSN (Deliver Status Notification) level on which to request a receipt from the mail server. If supported by the mail server, the receipt will be delivered to the address specified in the 'from' attribute. Default Value: The SMTP server's default notification.
Request Read Receipt	Specify whether or not to request a receipt from the recipient(s). Default Value: false
Allow Invalid Addresses	Specify whether or not the server should continue sending the email even if one or more invalid recipient addresses are specified. Default Value: false
Encryption Tab	
Encrypt Message	Specify whether or not to encrypt the message. The message will be encrypted using each recipient's trusted certificate following the S/MIME standard. Default Value: false
Sign Message	Specify whether or not to sign the message. A digital signature will be added using the sender's private key following the S/MIME standard. Default Value: false
Output Variables Tab	

Sent Attachments Variable	If desired, specify the name of a variable which will contain the attachment files sent with this email. The variable will be of type File List. It will be created if it does not exist, or overwritten otherwise.
SMTP Server	
Refer to the "SMTP Servers Resource" on page 78 page for the Mail Box Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

From

The From element allows you specify the sender's email address.

Field	Definition
Basic Tab	
Address	Specify the internet email address.
Name	Specify the name of the person at this address.
Charset	Specify a charset setting for special character encoding.
Private Key Alias	Specify the name of the key alias in the default private key store to use when adding a digital signature to the message.

To

The To element allows you specify the recipient's email address.

Field	Definition
Basic Tab	
Address	Specify the internet email address.
Name	Specify the name of the person at this address.
Charset	Specify a charset setting for special character encoding.
Trusted Key Alias	Specify the name of the key alias in the trusted key store to use when encrypting the message to this recipient.

Cc

The Cc element allows you specify additional recipients in the CC address field.

Field	Definition
Basic Tab	
Address	Specify the internet email address.
Name	Specify the name of the person at this address.
Charset	Specify a charset setting for special character encoding.
Trusted Key Alias	Specify the name of the key alias in the trusted key store to use when encrypting the message to this recipient.

Bcc

The Bcc (Blind Carbon Copy) element allows you specify additional recipients in the BCC address field. The recipients in the To and CC fields will not see the recipients in the BCC field.

Field	Definition
Basic Tab	
Address	Specify the internet email address.
Name	Specify the name of the person at this address.
Charset	Specify a charset setting for special character encoding.
Trusted Key Alias	Specify the name of the key alias in the trusted key store to use when encrypting the message to this recipient.

Reply-to

The Reply-to element species the recipient address when a user replies to a message.

Field	Definition
Basic Tab	
Address	Specify the internet email address.
Name	Specify the name of the person at this address.
Charset	Specify a charset setting for special character encoding.

Specify Subject

The Specify Subject element allows you to specify a message in the subject field of an email.

Field	Definition
Basic Tab	
Text	Specify the subject of this email.
Charset	Specify a charset setting for special character encoding.

Specify Message

The Specify Message element allows you to specify add a message in to an email.

Field	Definition
Basic Tab	
Text	Specify the body text of this email message
Content Type	Specify the content type setting for the body text of this email message. 'text/plain', 'text/xml', 'text/html' are examples of some valid content types. Default Value: text/plain
Charset	Specify a charset setting for special character encoding.

Add Attachment

The Add Attachment element allows you to add file attachments to an email.

Field	Definition
Basic Tab	

File	Specify the path and file name of a single file to attach to the email.
Input Files Variable	Specify the name of a variable of type File List which contains files to attach. For example, ${variableName}

Retrieve Email Task

The Retrieve Email task can access a standard POP-3 or IMAP "Mail Boxes Resource" on page 79 and retrieve emails stored on it. Messages can be filtered using a variety of criteria including the from-address, to-address, subject and message.

The attachments and message body contents for any emails (which are retrieved), can be stored in a specified Destination Directory. Subsequent tasks may then access the output "File Lists and File Sets" on page 116 variables to process the attachments (specified on the "Downloaded Attachments Variable") or message body files (specified on the "Downloaded Message Body Files Variable").

The details (for example, subject, from address, sent date, recipients, etc) for each retrieved message can be stored in the Email List output variable. This variable will also store the file path locations of where the attachments and message bodies were saved. The Email List variable can then be used in a "For-Each Loop" on page 152 loop to process each message individually. Refer to the "Email Lists" on page 122 topic for more information.

Processing Signed and Encrypted Emails

Before retrieving digitally signed email messages, the sender's public certificate will first need to be imported into Managed File Transfer so the sender can be authenticated. For more information about retrieving digitally signed emails, please refer to the "Quick Start for Secure Email" on page 719.

Before retrieving S/MIME encrypted Email messages, you need to first create an SSL Certificate in the Default Private Key Store. Then you should export the public portion of the certificate and give it to the intended sender. The sender can use your public certificate to encrypt any emails they send to you. For more information about decrypting emails, please refer to the "Quick Start for Secure Email" on page 719.

Note: Email messages may contain one or more message bodies. For example, if the sender's mail client is setup to send both text and html formats, the retrieved email will have two message body files. The name of those files will be messagebody.txt and messagebody.html respectively. If you choose to save message bodies on the Retrieve Email task, then both of those bodies will be stored in the Destination Directory.

Example 1: Retrieve Email

Follow the steps below to retrieve emails that contain a From address of "example@informatica.com" and save their attachments to a directory:

Note: On the Advanced tab, there is an option to delete the message after it is retrieved, which by default is set to false. Changing it to true will delete the message from the mail box server after it is retrieved.

1. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Retrieve Email task to the Project Outline.
2. On the Basic tab of the Retrieve Mail task, specify values for the following attributes:

   Mail Box

   The "Mail Boxes Resource" on page 79 resource.

Destination Directory

The "File Paths" on page 161 where the attachments should be saved.

Save Attachments

Whether or not to save the attachments to the destination directory.

3. Click the **Add** button in the sub-menu and select the Message Filter menu item.
4. On the Basic tab of the Message Filter element, specify values for the following attributes:
   - Match - Specify the type of matching to use. Valid options are 'all' and 'any'. The option 'all' means that all filter criteria must be met for an email message to be processed, whereas 'any' means that one or more filter criteria must be met for an email message to be processed.
5. Click the **Add** button in the sub-menu and select the Add a From Address Filter menu item.
6. On the Basic tab of the From Address Filter, specify values for the following attributes:

   Condition

   Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.

   Value

   Specify the search term.

   Case Sensitive

   Specify whether or not to use case sensitive matching.
7. Click the **Save** button when finished.

Retrieve Email Task

The Retrieve Email task can access a standard POP-3 or IMAP "Mail Boxes Resource" on page 79 and retrieve emails stored on it.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Mail Box	Select a pre-configured Mail Box from the drop-down list.
Mail Folder	Specify the name of the mail folder to open on the mail box server. Default Value: INBOX
Destination Directory	Specify the directory on the local system where the attachments and message body files should be saved to.
Save Attachments	Specify whether or not attachments of the email message should be downloaded. Default Value: true
Save Message Body	Specify whether or not the body of the email message should be saved to a file. Default Value: false

When File Exists	Specify the action to take when an attachment being downloaded already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Delete Messages	Specify whether or not to delete processed email messages from the mail box server. Default Value: false
Private Key Alias	Specify the private key alias to use when decrypting emails.
Output Variables Tab	
Email List Variable	If desired, specify the name of a variable which will contain an EmailList variable. It will be created if it does not exist, or overwritten otherwise.
Downloaded Attachments Variable	If desired, specify the name of a variable which will contain the downloaded attachments. The variable will be of type File List. It will be created if it does not exist, or overwritten otherwise.
Downloaded Message Body Files Variable	If desired, specify the name of a variable which will contain the downloaded message body files. The variable will be of type File List. It will be created if it does not exist, or overwritten otherwise.
Number of Messages Retrieved Variable	If desired, specify the name of a variable which will contain the number of messages retrieved. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Mailbox Server	
Refer to the "Mail Boxes Resource" on page 79 page for the Mail Box Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Message Filter

The Message Filter element allows you to specify the type of match to use in the filter.

Field	Definition
Basic Tab	
Match	Specify the type of matching to use. Valid options are 'all' and 'any'. The option 'all' means that all filter criteria must be met for an email message to be processed, whereas 'any' means that one or more filter criteria must be met for an email message to be processed. Default Value: all

From Address

The From Address element allows you to filter messages by the sender email address.

Field	Definition
Basic Tab	
Condition	Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.
Value	Specify the search term.
Case Sensitive	Specify whether or not to use case sensitive matching. Default Value: false

To Address

The To Address element allows you to filter messages by the recipient email address.

Field	Definition
Basic Tab	
Condition	Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.
Value	Specify the search term.
Case Sensitive	Specify whether or not to use case sensitive matching. Default Value: false

Cc Address

The CC Address element allows you to filter messages by the carbon copied recipients email addresses.

Field	Definition
Basic Tab	

Condition	Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.
Value	Specify the search term.
Case Sensitive	Specify whether or not to use case sensitive matching. Default Value: false

Subject

The Subject element allows you to filter messages by the contents of the email subject.

Field	Definition
Basic Tab	
Condition	Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.
Value	Specify the search term.
Case Sensitive	Specify whether or not to use case sensitive matching. Default Value: false

Message Body

The Message Body element allows you to filter emails by the contents of the message.

Field	Definition
Basic Tab	
Condition	Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.
Value	Specify the search term.
Case Sensitive	Specify whether or not to use case sensitive matching. Default Value: false

Message ID

The Message ID element allows you to filter emails by the MIME Message ID.

Field	Definition
Basic Tab	
Condition	Specify the condition to use for including or excluding emails. Valid options are 'equals', 'not equals', 'contains', 'not contains', and 'regex'.

Value	Specify the search term.
Case Sensitive	Specify whether or not to use case sensitive matching. Default Value: false

Add a Nested Message Filter

The Nested Message Filter element allows you to further filter messages after an initial filter is applied. For example, a message filter retrieves email messages that contain a From Address of "example@informatica.com." A nested filter takes the messages returned from the first filter and applies a second filter to return messages where the Subject contains the word "Reports."

Field	Definition
Basic Tab	
Match	Specify the type of matching to use. Valid options are 'all' and 'any'. The option 'all' means that all filter criteria must be met for an email message to be processed, whereas 'any' means that one or more filter criteria must be met for an email message to be processed. Default Value: all

Perform a PGP Encryption

File encryption tasks transform the plaintext file contents using an algorithm known as cipher. The transformation makes the file unreadable to anyone except those who possess the special knowledge.

Informatica Managed File Transfer provides OpenPGP compliant file encryption and decryption tasks for use within Projects.

PGP Decrypt Task

The PGP Decrypt task decrypts one or more files, using a private key stored in the OpenPGP Key Ring, reverting the files back into plain text form. The digital signature of an encrypted file is verified automatically when the file is decrypted.

Decrypting a Single File Using a PGP Decrypt Task

Perform the following steps to decrypt a single using a PGP Decrypt Task:

1. From within the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Decrypt task to the Project Outline.
2. On the Basic tab of the Write PGP Decrypt task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Passphrase attribute, specify the passphrase of your private key. This is the passphrase you used when you first created your key pair.

- For the Input File attribute, specify the name of the file to decrypt.
- For the Output File attribute, specify the directory and file name for the decrypted file.

3. Click the **Save** button to save the task.

Decrypting a Set of Files Using a PGP Decrypt Task

Perform the following steps to decrypt a set of files using a PGP Decrypt Task:

1. From within the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Decrypt task to the Project Outline.
2. On the Basic tab of the PGP Decrypt task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Passphrase attribute, specify the passphrase of your private key. This is the passphrase you used when you first created your key pair.
   - For the Input Files Variable attribute, specify a variable to process a list of files that you received from your trading partner.
   - For the Output Directory attribute, specify the directory to store the decrypted files.
3. Click the **Save** button to save the task.

PGP Decrypt Task Fields

The PGP Decrypt task can decrypt one or more files, reverting them back into plain text form.

The following table describes the fields in the **Basic Tab** of a PGP Decrypt Task:

Field	Description
Label	Specify a label for the task.
OpenPGP Key Ring	Select a pre-configured OpenPGP key ring from the drop-down list.
Passphrase	Specify the passphrase for this secret key (also knows as private or decryption key
Is Passphrase Encrypted?	Specify whether the passphrase is in encrypted form. Default is false.
Input File	Specify the path and file name of a single file to be decrypted.
Input Files Variable	Specify the name of a variable of type File List that contains the files to decrypt. For example, ${variableName}
Output File	Specify the path and file name of the decrypted output file. Specify the path and file name only if you decrypt a single file.
Output Directory	Specify the directory where the decrypted files should be saved.
When Output File Exists	Specify the action to take when an output file already exists. Default is rename. The default value changes the destination file name to a new name so the existing file does not change.

The following table describes the fields in the **Advanced Tab** of a PGP Decrypt Task:

Field	Description
File Name Prefix	Specify a string to attach to the beginning of the decrypted file names.
File Name Suffix	Specify a string to attach to the end of the decrypted file names.
Verify Signature	Specify whether Managed File Transfer must verify whether a signature exists in the TrustStore during decryption. **Note:** Managed File Transfer verifies signature only when the signature is added using the OpenPGP encryption. If users embed the digital signature in the files, the signature is not available in the TrustStore, and the job fails. Default is false.
Require Signature	Specify whether a signature is required on the encrypted file. Default is false.
Signature Key ID	Specify a key ID to ensure that the digitally signed files are signed with a specific key. When you do not specify a key ID, any key in the OpenPGP Key Ring is used to verify the signature.

The following table describes the fields in the **Output Variables Tab** of a PGP Decrypt Task:

Field	Description
Output Files Variable	You can specify the name of a variable that contains the verified files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Processed Input Files Variable	You can specify the name of a variable that contains the signed input files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Public Key Ring	You can specify the secret key ring that contains the sender's public keys. Specify the secret key ring only if no PGP key ring resource was specified or if you want to override the secret key ring that you specified in the PGP key ring resource.
Secret Key Ring	You can specify the secret key ring that contains the secret key. The secret key is also known as private or decryption key. Specify the secret key ring only if no PGP key ring resource was specified or if you want to override the secret key ring that you specified in the PGP key ring resource.

The following table describes the fields in the **Control Tab** of a PGP Decrypt Task:

Field	Description
Version	The version of the task.
Log Level	Specify the level of logging to use while executing this task. You can select **silent**, **normal**, **verbose**, or **debug**. The default value is inherited from the parent module.

Field	Description
Execute Only If	Specify a condition that must be satisfied before a task can be executed. The task will be skipped if the specified condition is not met.
Disabled	Whether the task is disabled. Default is false.

The following table describes the fields in the **On ErrorTab** of a PGP Decrypt Task:

Field	Description
On Error	Specify the action to take when the task errors out. You can select **abort**, **continue**, **call:[module]**, or **setVariable:[name]=[value]**. When you select **call:[module]**, replace `[module]` with the name of the module in the project, for example, `call:ErrorModule`. When you select **setVariable:[name]=[value]**, replace `[name]` with a variable name and `[value]` with the variable value, for example, `setVariable:error=true`. The default value is inherited from the parent module.

PGP Encrypt Task

The PGP Encrypt Task can encrypt one or more files, using a Public Key stored in an OpenPGP Key Ring, rendering the files unreadable until an authorized user decrypts them with the secret key. The files can also be digitally signed by adding a secret key to the file.

Encrypting a Single File Using a PGP Encrypt Task

Perform the following steps to encrypt a single file using a PGP Encrypt Task:

1. From within the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Encrypt task to the Project Outline.
2. On the Basic tab of the PGP Encrypt task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Input File attribute, specify the name of the file to encrypt.
   - For the Output File attribute, specify the directory and file name for the encrypted file.
3. To add a public key to encrypt the file with, click the **Next** button and choose **Add a Public Key** option from the menu.
4. To additionally sign the file, select the PGP Encrypt task by clicking it in the project outline.

   Note: Perform this step only if your trading partner requires digital signatures.
5. Click the **Add** button and choose Add a Secret Key from the context menu.
6. Click the  button to open the **PGP Key Chooser**, and select the private key.
7. Specify a passphrase for your private key. This is the passphrase you used when you first created your key pair.
8. Click the **Save** button to save the task.

Encrypting a Set of Files Using a PGP Encrypt Task

Perform the following steps to encrypt a set of files using a PGP Encrypt Task:

1. From within the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Encrypt task to the Project Outline.
2. On the **Basic** tab of PGP Encrypt Task, specify the following attributes:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Input Files Variable attribute, specify the file list variable that contains a list of files to encrypt and sign.
   - For the Output Directory attribute, specify the directory to place the encrypted files. If you leave the field blank, the encrypted file is created in the same directory as the input file.
3. To add a public key to encrypt the file with, click the **Add** button and choose **Add a Public Key** option from the menu.
4. To additionally sign the file, select the PGP Encrypt task by clicking it in the project outline.

   Note: Perform this step only if your trading partner requires digital signatures.
5. Click the **Add** button and choose Add a Secret Key from the context menu.
6. Click the  button to open the PGP Key Chooser and select the private key.
7. Specify a passphrase for your private key. This is the passphrase you used when you first created your key pair.
8. Click the **Save** button to save the task.

PGP Encrypt Task Fields

The PGP Encrypt Task can encrypt one or more files, rendering them unreadable until an authorized user decrypts them with the correct key.

The following table describes the fields in the **Basic Tab** of a PGP Encrypt Task:

Field	Description
Label	Specify a label for the task.
OpenPGP Key Ring	Select a pre-configured OpenPGP key ring from the drop-down list.
Input File	Specify the path and file name of the file to be verified.
Input Files Variable	Specify the name of a variable of type File List that contains the files to verify. For example, ${variableName}
Output File	Specify the path and file name of the verified output file. Specify the path and file name only if you verify a single file.
Output Directory	Specify the directory where the verified files should be saved.
When Output File Exists	Specify the action to take when the zipped file already exists. Default is rename. The default value changes the destination file name to a new name so the existing file does not change.

The following table describes the fields in the **Advanced Tab** of a PGP Encrypt Task:

Field	Description
Armor Output Files	Specify whether you want to armor the files when encrypting. Armoring converts the encrypted files into ASCII format using Base64 encoding. This makes the encrypted files safe for mailing, but about 33 percent larger. Default is false.
Compress Output Files	Specify whether you want to compress the files during encryption. Compressing the files results in smaller output files. Default is true.
Use Integrity Packet	Specify whether you want to use an integrity packet when encrypting. This option is provided for compatibility reasons with older PGP implementations. Default is true.
User Version3 Signature	Specify whether you want to sign the files using version 3 signatures. Default is false. By default, the files are signed using version 4 signatures. This attribute is provided for compatibility with older PGP softwares.
File Name Prefix	Specify a string to attach at the beginning of the encrypted file names.
File Name Suffix	Specify a string to attach at the end of the encrypted file names.

The following table describes the fields in the **Algorithms Tab** of a PGP Encrypt Task:

Field	Description
Symmetric Key Algorithm	Specify the symmetric key algorithm to use. The default value is automatically determined from the key.
Hash Algorithm	Specify the hash algorithm to use. The default value is automatically determined from the key.
Compression Algorithm	Specify the compression algorithm to use. The default value is automatically determined from the key.

The following table describes the fields in the **Output Variables Tab** of a PGP Encrypt Task:

Field	Description
Output Files Variable	You can specify the name of a variable that contains the verified files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Processed Input Files Variable	You can specify the name of a variable that contains the signed input files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.

Field	Description
Public Key Ring	Specify the public key ring that contains a copy of the sender's public keys. Specify the public key ring only if no PGP key ring resource was specified or if you need to override the public key ring that you specified in the PGP key ring resource.
Secret Key Ring	Specify the secret key ring that contains your secret key. The secret key is used if you are signing the files during encryption. Specify the secret key ring only if no PGP key ring resource was specified or if you need to override the secret key ring that you specified in the PGP key ring resource.

The following table describes the fields in the **Control Tab** of a PGP Encrypt Task:

Field	Description
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. You can select **silent**, **normal**, **verbose**, or **debug**. The default value is inherited from the parent module.
Execute Only If	Specify a condition that must be met before the task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether the task is disabled. Default is false.

The following table describes the fields in the **On Error Tab** of a PGP Encrypt Task:

Field	Description
On Error	Specify the action to take when the task errors out. You can select **abort**, **continue**, **call:[module]**, or **setVariable:[name]=[value]**. When you select **call:[module]**, replace `[module]` with the name of the module in the project, for example, `call:ErrorModule`. When you select **setVariable:[name]=[value]**, replace `[name]` with a variable name and `[value]` with the variable value, for example, `setVariable:error=true`. The default value is inherited from the parent module.

Public Key

Use the Public Key element to specify the public key used to encrypt the file or the set of files.

The following table describes the fields in the **Basic Tab** of a Public Key element:

Field	Description
Email Address	Specify the user's email address on the key. The email address is used to identify the key in the key ring that you need to use. Use **Email Address**, **Key ID**, or **Name** to find the key.
Key ID	Specify the ID of the key. The ID is used to identify the key in the key ring that you need to use. Use **Email Address**, **Key ID**, or **Name** to find the key.
Name	Specify the user name on the key. The user name is used to identify the key in the key ring that you need to use. Use **Email Address**, **Key ID**, or **Name** to find the key.

Secret Key

Use the Secret Key element to digitally sign a file or a set of files.

The following table describes the fields in the **Basic Tab** of a Secret Key element:

Field	Description
Email Address	Specify the user's email address on the key. The email address is used to identify the key in the key ring that you need to use. Use **Email Address**, **Key ID**, or **Name** to find the key.
Key ID	Specify the ID of the key. The ID is used to identify the key in the key ring that you need to use. Use **Email Address**, **Key ID**, or **Name** to find the key.
Name	Specify the user name on the key. The user name is used to identify the key in the key ring that you need to use. Use **Email Address**, **Key ID**, or **Name** to find the key.
Passphrase	Specify the passphrase for the secret key. You must specify the passphrase to access the secret key. If you did not specify the passphrase for the secret key, select the **system.emptystring** variable from the variable dropdown.
Is Passphrase Encrypted	Specify whether the passphrase is in encrypted form. Default is false.

PGP Sign Task

Digitally signing a file embeds a digital signature in the file without encrypting it. A digitally signed file assures the recipient that you were the original sender of the file. You can sign a single file or a set of files using the PGP Sign Task.

Signing a File Using a PGP Sign Task

Perform the following steps to sign a file using a PGP Sign Task:

1. From the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Sign task to the Project Outline.

2. On the Basic tab of the PGP Sign task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Input File attribute, specify the name of the file to sign.
   - For the Output File attribute, specify the directory and file name for the signed file.
3. Click the **Add** button and choose **Add a Secret Key** from the context menu.
4. Click the button to open the PGP Key Chooser and select the private key.
5. Specify a passphrase for your private key. This is the passphrase you used when you first created your key pair.
6. Click the **Save** button to save the task.

Signing a Set of Files Using a PGP Sign Task

Perform the following steps to sign a set of files using the PGP Sign Task:

1. From the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Sign task to the Project Outline.
2. Open the File Encryption folder and click the PGP Sign task.
3. On the Basic tab of the PGP Sign task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Input File attribute, specify the file list variable that contains a list of files to sign.
   - For the Output File attribute, specify the directory for the signed files.
4. Click the **Add** button and choose **Add a Secret Key** from the context menu.
5. Click the button to open the PGP Key Chooser and select the private key.
6. Specify a passphrase for your private key. This is the passphrase you used when you first created your key pair.
7. Click the **Save** button to save the task.

PGP Sign Task Fields

The PGP Sign task embeds a digital signature in the file without encrypting it.

The following table describes the fields in the **Basic Tab** of a PGP Sign Task:

Field	Description
Label	Specify a label for the task.
OpenPGP Key Ring	Select a pre-configured OpenPGP key ring from the drop-down list.
Input File	Specify the path and file name of the file to be signed.
Input Files Variable	Specify the name of a variable of type File List that contains the files to sign. For example, ${variableName}

Field	Description
Output File	Specify the path and file name of the signed output file. This is valid only if you are signing a single file.
Output Directory	Specify the directory where the signed files should be saved.
When Output File Exists	Specify the action to take when the output file already exists. Default is rename. The default value changes the destination file name to a new name. Therefore, the existing file does not change.

The following table describes the fields in the **Advanced Tab** of a PGP Sign Task:

Field	Description
Armor Output Files	Specify whether you want to armor the files when encrypting. Armoring converts the encrypted files into ASCII format using Base64 encoding. This makes the encrypted files safe for mailing, but about 33 percent larger. Default is false.
Compress Output Files	Specify whether you want to compress the files during encryption. Compressing the files results in smaller output files. Default is true.
User Version3 Signature	Specify whether you want to sign the files using version 3 signatures. Default is false. By default, the files are signed using version 4 signatures. This attribute is provided for compatibility with older PGP softwares.
File Name Prefix	Specify a string to attach at the beginning of the signed file names.
File Name Suffix	Specify a string to attach at the end of the signed file names.

The following table describes the fields in the **Algorithms Tab** of a PGP Sign Task:

Field	Description
Hash Algorithm	Specify the hash algorithm to use. The default value is automatically determined from the key.
Compression Algorithm	Specify the compression algorithm to use. The default value is automatically determined from the key.

The following table describes the fields in the **Output Variables Tab** of a PGP Sign Task:

Field	Description
Output Files Variable	You can specify the name of a variable that contains the verified files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Processed Input Files Variable	You can specify the name of a variable that contains the signed input files. The variable is of type File List and can be used in subsequent tasks that accept a File List input variable. The variable is created if it does not exist.
Secret Key Ring	Specify the secret key ring that contains your secret key. Specify the secret key ring only if no PGP key ring resource was specified or if you need to override the secret key ring that you specified in the PGP key ring resource.

The following table describes the fields in the **Control Tab** of a PGP Sign Task:

Field	Description
Version	The version of the task.
Log Level	Specify the level of logging to use while executing this task. You can select **silent**, **normal**, **verbose**, or **debug**. The default value is inherited from the parent module.
Execute Only If	Specify the secret key ring that contains the sender's public keys. Specify the secret key ring only if no PGP key ring resource was specified or if you need to override the secret key ring that you specified in the PGP key ring resource.
Disabled	Whether the task is disabled. Default is false.

The following table describes the fields in the **On ErrorTab** of a PGP Sign Task:

Field	Description
On Error	Specify the action to take when the task errors out. You can select **abort**, **continue**, **call:[module]**, or **setVariable:[name]=[value]**. When you select **call:[module]**, replace `[module]` with the name of the module in the project, for example, `call:ErrorModule`. When you select **setVariable:[name]=[value]**, replace `[name]` with a variable name and `[value]` with the variable value, for example, `setVariable:error=true`. The default value is inherited from the parent module.

Secret Key

Use the Secret Key element to digitally sign the file(s).

Field	Definition
Basic Tab	

Email Address	Specify the user's email address on the key. The email address is used to identify which key in the key ring to use. Either Email Address or Key ID or Name is required in order to find the correct key.
Key ID	Specify the ID of the key. The Key ID is used to identify which key in the key ring to use. Either Email Address or Key ID or Name is required in order to find the correct key.
Name	Specify the user name on the key. The user name is used to identify which key in the key ring to use. Either Email Address or Key ID or Name is required in order to find the correct key.
Passphrase	Specify the passphrase for this secret key. The passphrase is required in order to access this secret key. If the secret key does not have a passphrase, select the special 'system.emptystring' variable from the variable dropdown.
Is Passphrase Encrypted	Specify whether or not the passphrase is in encrypted form. Default Value: false

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

PGP Verify Task

If a file is signed, it should be verified before it is used. You can verify a single file or a set of files using the PGP Verify Task. When the PGP Verify Task is executed, files that cannot be verified will create a project error, and the project will be aborted by default. You can specify the action to take when an unverified file is encountered by selecting an error action on the **On Error** tab.

Verifying a File Using a PGP Verify Task

Perform the following steps to verify a file using a PGP Verify Task:

1. From within the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Verify Task to the Project Outline.
2. On the **Basic** tab of the PGP Verify task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Input File attribute, specify the name of the file to verify.
   - For the Output File attribute, specify the directory and file name for the verified file.
3. Click the **Save** button to save the task.

Verifying a Set of Files Using a PGP Verify Task

Perform the following steps to verify a set of files using a PGP Verify Task:

1. From within the Project Designer page, expand the File Encryption folder in the Component Library, and then drag the PGP Verify Task to the Project Outline.
2. On the **Basic** tab of the PGP Verify Task, specify the following values:
   - Select the Key Ring that contains the OpenPGP keys.
   - For the Input File attribute, specify the file list variable that contains a list of files to verify.
   - For the Output File attribute, specify the directory a for the verified files.
3. Click the **Save** button to save the task.

PGP Verify Task Fields

The following table describes the fields in a PGP Verify Task:

Field	Definition
Basic Tab	
Label	Specify a label for this task.
OpenPGP Key Ring	Select a pre-configured OpenPGP key ring from the drop-down list.
Input File	Specify the path and file name of a single file to be verify.
Input Files Variable	Specify the name of a variable of type File List which contains the files to verify. For example, ${variableName}
Output File	Specify the path and file name of the verified output file. This is only valid if you are verifying a single file.
Output Directory	Specify the directory where the verified files should be saved.
When Output File Exists	Specify the action to take when an output file already exists. The default value is 'rename' which changes the file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
File Name Prefix	Specify a string to attach to the beginning of the verified file names.
File Name Suffix	Specify a string to attach to the end of the verified file names.
Output Variables Tab	
Output Files Variable	If desired, specify the name of a variable which will contain the verified file(s). The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Processed Input Files Variable	If desired, specify the name of a variable which will contain the signed input file(s). The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
OpenPGP Key Ring	
Public Key Ring	Specify the secret key ring that contains the sender's public keys. This is only necessary if no PGP key ring resource was specified or if it is desired to override the secret key ring specified in the PGP key ring resource.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module

Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Local File System Tasks

Local File System tasks perform a wide range of actions on files and directories. These tasks can access "File Paths" on page 161 on the local system or network locations. The basic functions like "Copy Task" on page 364, "Delete Task" on page 369, "Move Task" on page 367, "Rename Task" on page 370 and "Make Directory Task" on page 372 are useful for organizing files on the file system.

The "Create File List Task" on page 380 can get file counts and build lists of files (based on filters) for analysis and processing. The "Merge Files Task" on page 377 can create one output file that contains the contents of multiple input files. The "Search and Replace Task" on page 373 can be used to search the contents of a file for a string value and automatically replace it with specified text.

Copy Task

The Copy task can copy one or more files into a destination directory on the local file system or network share. If a "File Lists and File Sets" on page 116 is being used, it will copy all of the files and folders in the File Set into the destination directory. By default it will create any sub-directories that do not already exist. Setting the attribute **Flatten Destination Directory** to true will place all files in the File Set directly into the destination directory specified without creating sub-directories.

Example 1: Copy a File

Follow the steps below to copy a single file from one directory to another:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Copy task to the Project Outline.
2. On the Basic tab of the Copy task, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and name of a single file to be copied.

Destination Directory

The directory to which the specified source files should be copied to.

3. Click the **Save** button when finished.

Example 2: Copy Multiple Files

Follow the steps below to copy multiple files from one directory to another:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Copy task to the Project Outline.
2. On the Basic tab of the Copy task, specify values for the following attributes:

   Source Files Variable

   Specify the name of a variable of type File List which contains the files to copy.

   Destination Directory

   Specify the directory to which the specified source files should be copied.

3. Click the **Save** button when finished.

Copy Task

The Copy task can copy one or more files into a destination directory on the local file system or network share.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Source File	Specify the path and name of a single file to be copied. This value must be a file, not a directory.
Source Files Variable	Specify the name of a variable of type File List which contains the files to copy. For example, ${variableName}.
Destination File	Specify the path and name of the destination file. It is invalid to specify this value if you are copying multiple files.
Destination Directory	Specify the directory to which the specified source files should be copied. You must specify this attribute if you are copying multiple files using one or more File Set elements, or a Source Files Variable.
When File Exists	Specify the action to take when a destination file already exists. The default value is ''rename'' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Flatten Destination Directory	Specify whether or not to copy all source files directly into the specified destination directory, without creating any sub directories. The default value is false, which creates sub directories to match the source directories. Default Value: false

Preserve Dates	Specify whether or not the last-modified date of the copies should remain consistent with the source files. The default behavior is to leave them as they are set by the file system. Default Value: false
File Name Prefix	Specify the string to prepend to the output file names.
File Name Suffix	Specify the string to append to the output file names.
Output Variables Tab	
Processed Source Files Variable	If desired, specify the name of a variable which will contain the file(s) in the source location. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Bytes Copied Variable	If desired, specify the name of a variable which will contain the number of bytes copied. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Number of Files Copied Variable	If desired, specify the name of a variable which will contain the number of files copied. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Destination Files Variable	If desired, specify the name of a variable which will contain the file(s) in the destination location. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Move Task

The Move task can move file(s) from one directory into another directory on the local file system or network share. This task also gives you the ability to rename a single file by changing the name in the **Destination File** attribute.

Note: It is recommended to use Copy+Delete tasks instead of Move tasks when you move files from or to shared folders.

Example 1: Move a File

Follow the steps below to move a file from one directory to another:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Move task to the Project Outline.
2. On the Basic tab of the Move task, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 of a single file to be moved.

   Destination Directory

   The directory to which the files are to be moved.
3. Click the **Save** button when finished.

Example 2: Move Multiple Files

Follow the steps below to move multiple files from one directory to another:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Move task to the Project Outline.
2. On the Basic tab of the Move task, specify values for the following attributes:

   Source Files Variable

   Specify the name of a variable of type File List which contains the files to move.

   Destination Directory

   The directory to which the files are to be moved.
3. Click the **Save** button when finished.

Move Task

The Move task can move file(s) from one directory into another directory on the local file system or network share.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Source File	Specify the path and file name of a single file to be moved.

Source Files Variable	Specify the name of a variable of type File List which contains the files to move. For example, ${variableName}
Destination File	Specify the path and file name of where the file should be moved. Specify only if you are moving a single file.
Destination Directory	Specify the directory to which the files are to be moved.
When File Exists	Specify the action to take when the destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Advanced Tab	
Flatten Destination Directory	Specify whether or not to save all moved files directly in the specified destination directory, without creating any sub-folders. Default Value: false
File Name Prefix	Specify the string to prepend to the output file names.
File Name Suffix	Specify the string to append to the output file names.
Output Variables Tab	
Number of Files Moved Variable	If desired, specify the name of a variable which will contain the number of files moved. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Destination Files Variable	If desired, specify the name of a variable which will contain the moved file(s). The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Delete Task

The Delete task can delete one or more files, or a directory, from a local file system or from an authorized network share.

Example 1: Delete a File

Follow the steps below to delete a file from a file path:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Delete task to the Project Outline.
2. On the Basic tab of the Delete task, specify the File value:

   File

   The file path and name of the file to be deleted.
3. Click the **Save** button when finished.

   Note: If a directory is specified all files and sub-directories in that directory will be deleted.

Example 2: Delete Multiple Files

Follow the steps below to delete files from a File Set:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Delete task to the Project Outline.
2. Click the **Add** button and select the Add a File Set menu item.
3. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the FTP server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
4. Click the **Save** button when finished.

Delete Task

The Delete task can delete one or more files, or a directory, from a local file system or from an authorized network share.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
File	Specify the path and name of the file to be deleted. e.g. /folder/subfolder/file.ext
Input Files Variable	Specify the name of a variable of type File List which contains the files to delete. For example, ${variableName}
Directory	Specify a single directory to delete. WARNING: The specified directory and all of its contents will be removed.

Output Variables Tab	
Number of Files Deleted Variable	If desired, specify the name of a variable which will contain the number of files deleted. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Rename Task

The Rename task can change the name of one or more files on the local file system or network share.

Example 1: Rename a File

Follow the steps below to rename a single file:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Rename task to the Project Outline.
2. On the Basic tab of the Rename task, specify values for the following attributes:

   Input File

   The "File Paths" on page 161 of a single file to rename.

   New Name

   The new name for the file.
3. Click the **Save** button when finished.

Example 2: Rename Multiple Files

Follow the steps below to rename files in a File Set:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Rename task to the Project Outline.
2. The fields on the Basic tab are optional when you are renaming files in a File Set. Select the **Advanced** tab.
3. On the Advanced tab of the Rename task, specify values for the following attributes:

   File Name Prefix

   The string to prepend to the file names.
4. Click the **Add** button, and then choose Add A File Set.
5. On the File Set element, Specify the following values:

   Base Directory

   Specify the starting directory for this File Set that contains the files to rename.
6. Click the **Save** button when finished. When the project executes, all the files in the C:\EmployeeData \Decrypted directory will prepended with "Procesed_".
7. **Note:** If a "File Lists and File Sets" on page 116 is being used that contains multiple files from multiple file paths, only the file names will be modified and the directory names will stay the same.

Rename Task

The Rename task can change the name of one or more files on the local file system or network share.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a single file to rename.
Input Files Variable	Specify the name of a variable of type File List which contains the files to rename. For example, ${variableName}
New Name	Specify a new name for the file. New Name can only be used if a single file is being renamed.
When File Exists	Specify the action to take when the destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched.
Advanced Tab	
Search Pattern	Specify a pattern to search and replace in the file name(s). Both regular expressions and wildcard search patterns can be used and can be changed using the Pattern Type attribute.
Pattern Type	Specify the type of pattern to use when using search and replace on the file names. Default Value: wildcard

Replace With	Specify the pattern to replace in the file names. If using regular expressions and groups of the file names were captured, use the syntax $1, $2, etc... to reuse the captured segments. If using wildcard search and replace, use character * and ? to reuse the values the * and ? represented in the search for value.
Case Sensitive	Specify whether or not to use case sensitive matching when searching and replacing sections of the file names. Default Value: false
File Name Prefix	Specify the string to prepend to the file names.
File Name Suffix	Specify the string to append to the end of the file names.
Output Variables Tab	
Number of Files Renamed Variable	If desired, specify the name of a variable which will contain the number of file names successfully modified by this task. The variable will be created if it does not exist.
Output Files Variable	If desired, specify the name of a variable which will contain the renamed files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Make Directory Task

The Make Directory task can create a directory based on the information provided. If the directory specified contains parent directories that do not exist, they will be created automatically.

Example 1: Make a New Directory

Follow the steps below to make a directory in a "File Paths" on page 161:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Make Directory task to the Project Outline.
2. On the Basic tab of the Make Directory task, specify the Directory Path value:

   Directory Path

   The directory file path to be created.
3. Click the **Save** button when finished.

Make Directory Task

The Make Directory task can create a directory based on the information provided.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Directory Path	Specify the directory path to be created.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Search and Replace Task

The Search and Replace task can search one or more files for a string value (pattern) and replace that pattern with characters specified in the **Replace With** attribute. By providing a "File Lists and File Sets" on page 116 element, multiple files can be processed in the same task. A single file can also be added by simply utilizing the **Input File** attribute.

By default, the **Case Sensitive Search** attribute on the Advanced tab is set to true. Setting it to false will ignore the case when applying the search pattern.

The Search and Replace Task contains the Number of Replacements and Number of Files Processed output variables. Those variables can be used to conditionally execute subsequent Tasks.

Example 1: Search and Replace

Follow the steps below to search for a pattern and replace it with other characters:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Search and Replace task to the Project Outline.
2. On the Basic tab of the Search and Replace task, specify values for the following attributes:

   Input File

   The "File Paths" on page 161 of a file to scan and modify.

   Output File

   The file path of the output file where the modified data should be written. This is only applicable when modifying a single file.

   Search For

   The string (pattern) to search for within the input file(s). All values will be searched for as their string literals. Regular expressions are not allowed. The backslash character '\' is an escape character that can be used to search for special characters. Below is a list of escape sequences that are permitted.
   \n - New line.

   \r - Carriage return.

   \t - Tab.

   \\ - Represents a single \.

   \xFF - A hex value. Replace FF with a valid 2-byte hex value.

   \u0000 - A Unicode value. Replace 0000 with a valid Unicode value.

   Replace With

   The replacement string to be written in place of the **Search For** match. In order to simply delete the **Search For** characters, use the ${system.emptyString} variable as the Replace With value. Escape sequences are permitted. For a list of valid escape sequences please refer to the list above under the **Search For** attribute.
3. Click the **Save** button when finished.
4. **Note:** You may only want to replace the pattern a predetermined number of times. The **Max Number of Replacements** attribute on the Advanced tab controls how many times the value will be replaced.

Example 2: Search and Replace Multiple Files

Follow the steps below to search files in a File Set for a pattern and replace it with other characters:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Search and Replace task to the Project Outline.
2. On the Basic tab of the Search and Replace task, specify values for the following attributes:

Output Directory

Specify the directory location on the local file system where the modified files should be written.

Search For

The string (pattern) to search for within the input file(s). All values will be searched for as their string literals. Regular expressions are not allowed. The backslash character '\' is an escape character that can be used to search for special characters. Below is a list of escape sequences that are permitted.
\n - New line.

\r - Carriage return.

\t - Tab.

\\ - Represents a single \.

\xFF - A hex value. Replace FF with a valid 2-byte hex value.

\u0000 - A Unicode value. Replace 0000 with a valid Unicode value.

Replace With

The replacement string to be written in place of the **Search For** match. In order to simply delete the **Search For** characters, use the ${system.emptyString} variable as the Replace With value. Escape sequences are permitted. For a list of valid escape sequences please refer to the list above under the **Search For** attribute.

Max Number of Replacements attribute on the Advanced tab controls how many times the value will be replaced.

3. Click the **Add** button and choose Add a File Set.
4. On the File Set element, specify the following attributes:

   Base Directory

   Specify the starting directory for this File Set. If no filters are defined, all files in this directory will be included.
5. Click the **Save** button when finished. When the project executes, all the files in the C:\EmployeeData folder will be searched for tab ('\t') string and replaced with a unit separator string ('\x1f').

Search and Replace Task

The Search and Replace task can search one or more files for a string value (pattern) and replace that pattern with characters specified in the **Replace With** attribute.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input File	Specify the path and file name of a file to scan and modify.
Input Files Variable	Specify the name of a variable of type File List which contains the files to scan and modify. For example, ${variableName}
Output File	Specify the path and file name of the output file where the modified data should be written. This is only applicable when modifying a single file.

Output Directory	Specify the directory location on the local file system where the modified files should be written.
When File Exists	Specify the action to take when the output file already exists. The default action is rename, which will auto-rename the output file leaving the existing file untouched. Default Value: rename
Search For	Specify the search pattern to use to search for and replace characters in the input file(s). All values will be searched for as their string literals. Regular expressions are not allowed. The following escaped characters are permitted \n (new line), \r (carriage return), \t (tab), \x (hex characters), and \u (unicode characters). Also, in order to search for a literal backslash character, the backslash must be escaped such as \\.
Replace With	Specify the replacement string to be written in place of the Search For match. Escaped characters \n, \r, and \t are permitted. In order to simply delete the Search For characters, use the ${system.emptyString} variable as the Replace With value.
Advanced Tab	
Case Sensitive Search	Specify whether or not to search the file(s) in case sensitive mode. The default setting is true which improves the search performance, but will not match strings that do not have the same case. Default Value: true
Encoding	Specify the file encoding. This is required if the files are using a different encoding than the platform's default. For example, UTF-8 or US-ASCII. Default Value: The platform's default encoding
Max Number of Replacements	Specify the maximum number of replacements to make on each file. Use this attribute to limit the replacements to a certain number of times. Each file will allow this many replacements. The default value is 0 which does not set a limit to the number of replacements Default Value: 0 - no limit
Output Variables Tab	
Output Files Variable	If desired, specify the name of a variable which will contain the modified output files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Processed Files Variable	If desired, specify the name of a variable which will contain the processed input files. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Processed Variable	If desired, specify the name of a variable which will contain the number of files successfully processed by this task. The variable will be created if it does not exist.
Number of Replacements Variable	If desired, specify the name of a variable which will contain the number of replacements made in all files processed by this task. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Merge Files Task

The Merge Files task accepts a list of files as input and merges their contents into a single output file on the local file system or network share. The input files can be specified using a combination of "File Lists and File Sets" on page 116 and by choosing single files (selectable through the **Add** button).

When the files are merged together, the first byte of the next file to merge is immediately appended to the end of the last file. By default, nothing is written between the files. A **File Delimiter** should be specified if separation is desired between the merged files. Below are a list of some common delimiters:

- \n - New line feed
- \t - Horizontal tab
- \r - Carriage return
- \f - Form feed

Example 1: Merge Files

Follow the steps below to merge two files together:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Merge Files task to the Project Outline.
2. On the Basic tab of the Merge Files task, specify the Output File value:

   Output File

   The output "File Paths" on page 161 that will contain the contents of all the merge files.
3. On the Advanced tab of the Merge Files task, specify the delimiter:

   File Delimiter

   A delimiter to be written between each appended file.
4. Click the **Add** button in the sub-menu and choose the **File** menu item.

5. On the Basic tab of the File element, specify the Path value:

   Path

   The full path of the file to be added to the list of merge files.

6. Click the **Add** button in the sub-menu and choose the **Add Same** menu item. Repeat step number 6 for each to merge.
7. Click the **Save** button when finished.

Example 2: Merge Multiple Files Using a File Set

Follow the steps below to merge multiple files from a File Set into a single file:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Merge Files task to the Project Outline.
2. On the Basic tab of the Merge Files task, specify the Output File value:

   Output File

   The output "File Paths" on page 161 that will contain the contents of all the merge files.

3. On the Advanced tab of the Merge Files Task, specify the delimiter:

   File Delimiter

   A delimiter to be written between each appended file.

4. Click the **Add** button in the sub-menu and choose the **File Set** menu item.
5. On the Basic tab of the File Set element, specify the Path value:

   Base Directory

   Specify the starting directory for this File Set. If no filters are defined, all files in this directory will be included.

6. Click the **Add** button in the sub-menu and choose the **Add Same** menu item. Repeat step number 6 for each to merge.
7. Click the **Save** button when finished.

Merge Files Task

The Merge Files task accepts a list of files as input and merges their contents into a single output file on the local file system or network share.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input Files Variable	Specify the name of a variable of type File List which contains the files to merge. For example, ${variableName}
Output File	Specify the output file that will contain the contents of all the merge files.

When File Exists	Specify what to do when the output file already exists. Default Value: rename
Advanced Tab	
Error If File Not Found	If a specified file cannot be found when the the task attempts to merge the file, if true, an error will be thrown and the task will terminate. Default Value: true
File Delimiter	Specify a delimiter to be written between each appended file. By default, nothing is written between the files, not even a line break.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the merged output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Processed Input Files Variable	If desired, specify the name of a variable which will contain all files that were successfully merged. The variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

File

The File element allows you to specify the path to the file that will be added to the list of merged files.

Field	Definition
Basic Tab	
Path	The full path of the file to be added to the list of merge files.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Create File List Task

The Create File List task will create a **File List Variable** based on the filters specified in the "File Lists and File Sets" on page 116. This variable will contain the "File Paths" on page 161 of the files found. That variable can then be used in other tasks by specifying that name in the **Input Files Variable** attribute. The **Number of Files Found Variable** will contain a count of the files, which is useful in other tasks by using the **Execute Only If** condition and checking to see if the number of files found is greater than zero.

Example 1: Create File List

Follow the steps below to create a File List variable:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
2. On the Basic tab of the Create File List task, specify the File List Variable value:

   File List Variable

   The name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists, then it will be overwritten.
3. Click the **Add** button in the sub-menu and select the **File Set** menu item. For more information please refer to the topic on "File Lists and File Sets" on page 116.
4. Click the **Save** button when finished.

Create File List Task

The Create File List task will create a **File List Variable** based on the filters specified in the File Set.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
File List Variable	If desired, specify the name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists it will be overwritten, otherwise it will be created.
Number of Files Found Variable	If desired, specify the name of a variable which will contain the number of files found. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module

Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

FTP Tasks

FTP tasks are provided in Managed File Transfer for connecting to standard and secure FTP servers for exchanging files. Managed File Transfer provides comprehensive FTP features to satisfy enterprise-level requirements including:

- Support for "FTP Task" on page 381, "FTPS Task" on page 397 "SFTP Task" on page 413, "SCP Task" on page 427, and "Execute SSH Command Task" on page 249.
- Comprehensive support of the FTP command set
- Get, Put, Delete and Move files
- Create, Change and Rename directories
- Execute custom commands
- Append files
- Transfer multiple files per connection
- Auto-detect Binary and ASCII modes
- Make Passive and Active connections
- Indicate the number of connection retry attempts and timeout values
- Auto suffix and prefix file names with constants, timestamps or variables
- Override file names and other properties at execution time using variables
- Auto-resume a file transfer without resending the entire file
- Connect to HTTP, SOCKS, or Managed File Transfer Gateway proxy servers

FTP Task

The FTP task can connect to FTP servers to send and retrieve files. It can perform get, put, rename, delete, create directory, and many more commands that are common to FTP clients. Either a single file or multiples files (through the use of a "File Lists and File Sets" on page 116) can be transferred at a time.

Active And Passive Modes

In Active mode, the FTP server will attempt to connect back to a port on the Managed File Transfer FTP client in order perform the data transfer. The challenge with Active mode is that your firewall may block the FTP server from trying to open a port back into your network.

In Passive mode, the FTP server does not need to connect back to a port on the Managed File Transfer FTP client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the FTP server, you may want to change the Use Passive Mode setting to **Yes** on the "FTP Servers Resource" on page 55 Connection tab.

Transfer Auto-Resume for FTP

If the FTP connection breaks or is lost, Managed File Transfer can automatically re-establish a connection and resume where it left off. The Auto-Resume feature uses the Connection Retry Attempts and Connection Retry Interval settings specified in the "FTP Servers Resource" on page 55 or at the task level.

If the connection is broken during a file transfer, files with an ASCII data type will be resent in their entirety to ensure data integrity. Files with a Binary data type will resume transferring the file. The connection retry attempts, transfers and the commands that are performed will be recorded in the job log when using Verbose and Debug log levels. The Transfer Auto-Resume is not available on the Append Files element.

Session Persistence

By default, when the FTP task is finished, the connection with the server (session) will be disconnected and closed. When using an FTP Task in a Loop or as part of a multi-step workflow, the FTP session can be kept open and reused rather than closing and reopening the session for each FTP Task to the same server. To keep a session open or to hand off the open session to the next FTP task in a Project, use the Input Session ID and Output Session ID variables on the Advanced tab of the FTP Task. If this is the first FTP session in the Project and other tasks will use this connection, only specify the Output Session ID (for example, FTPSession). The next task that uses the session would specify ${FTPSession} in the Input Session ID field. When no additional tasks in the Project need the open session, it should be closed using the "Close Session Task" on page 432 (using the Session ID value of ${FTPSession}).

Checksum Verification

Checksum verification can be added to the FTP task to ensure that the source file is exactly the same as the destination file after a transfer completes successfully. This option is available on the Put, Get, Mget, Manual Get, and Manual Put elements. Both the CRC32 and MD5 algorithms are supported with the default and recommended algorithm being MD5. Errors may occur if the transfer was performed in ASCII mode, if the FTP server doesn't support checksum verification or if the calculated values do not match.

Timestamp Preservation

Timestamp preservation is available in the FTP task when using the Put or Manual Put elements. Typically, timestamps are updated each time a file moves, however in some instances the file's timestamp may need to be preserved. If supported by the server, the preserve timestamp option can retain the timestamp from when the file was originally placed in the source location (not when it was placed on the destination server).

SOCKS, HTTP, and Informatica Managed File Transfer Gateway Proxy

Managed File Transfer connects to a proxy server as a client and the proxy server redirects the traffic to the target FTP server. Proxy settings for FTP connections are defined at the "FTP Servers Resource" on page 55

level or per FTP Task. The FTP Task can use SOCKS, HTTP, or Managed File Transfer Gateway proxy protocols when making a connection to a proxy server. The SOCKS connection in Managed File Transfer supports both version 4 and 5. The HTTP proxy, otherwise known as an HTTP tunneling proxy, provides an HTTP tunnel through which a transport can be established. When using a proxy server, obtain the correct proxy type and connection credentials from the proxy server administrator.

Example 1: FTP Get File

Follow the steps below to get a single file from an "FTP Servers Resource" on page 55:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
2. On the Basic tab of the FTP task, specify a value for the FTP Server:

   FTP Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Get Files menu item.
4. On the Basic tab of the Get Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to download.

   Destination File

   The destination file when downloading a single file.
5. Click the **Save** button when finished.

Note: If you want to FTP multiple files, then leave the Source File blank and click the **Add** button in the sub-menu and select the Add a File Set menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Example 2: FTP Get a File Manually

Follow the steps below to use a Manual Get to download a single file from an "FTP Servers Resource" on page 55:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
2. On the Basic tab of the FTP task, specify a value for the FTP Server:

   FTP Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Get a File Manually menu item.
4. On the Basic tab of the Get a File Manually element, specify values for the following attributes:

   Source File

   The path and file name of a single file to download. Unlike the regular Get, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the GET request.

   Destination File

   The destination file when downloading a single file.

5. Click the **Save** button when finished.

Example 3: FTP Put File

Follow the steps below to upload a single file to an "FTP Servers Resource" on page 55:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
2. On the Basic tab of the FTP task, specify a value for the FTP Server:

   FTP Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Put Files menu item.
4. On the Basic tab of the Put Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to upload.

   Destination File

   The destination file when uploading a single file.
5. Click the **Save** button when finished.

Note: If you want to FTP multiple files, then leave the Source File blank and click the **Add** button in the sub-menu and select the Add a File Set menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Example 4: FTP Put a File Manually

Follow the steps below to Manually Put (upload) a single file to an "FTP Servers Resource" on page 55:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
2. On the Basic tab of the FTP task, specify a value for the FTP Server:

   FTP Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Put a File Manually menu item.
4. On the Basic tab of the Put a File Manually element, specify values for the following attributes:

   Source File

   Specify the path and file name of a single file to upload.

   Destination File

   Specify the destination file. Unlike the regular Put action, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the PUT request.
5. Click the **Save** button when finished.

Example 5: FTP Create File List

"File Lists and File Sets" on page 116 allow you to iterate over a list of files and complete specific tasks sequentially. Follow the steps below to create a File List from a directory on a FTP server:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
2. On the Basic tab of the FTP task, specify a value for the FTP Server:

   FTP Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Create a File List menu item.
4. On the Basic tab of the Create a File list element, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created.

   Number of Files Found Variable

   The name of a variable which will contain the number of files found. The variable may be used in subsequent tasks.
5. Click the **Add** button and select the Add a File Set menu item.
6. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the FTP server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
7. Click the **Save** button when finished.

Example 6: FTP Get Multiple Files Using a Wildcard Filter

Follow the steps below to get a multiple files from an "FTP Servers Resource" on page 55 using a Wildcard Filter:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTP task to the Project Outline.
2. On the Basic tab of the FTP task, specify a value for the FTP Server:

   FTP Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Create a Files List menu item.
4. On the Basic tab of the Create a File list element, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created.

   Number of Files Found Variable

   The name of a variable which will contain the number of files found. The variable may be used in subsequent tasks.

5. Click the **Add** button and select the Add a File Set menu item.
6. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the FTP server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
7. Click the **Add** button and select the Add a Wildcard Filter menu item. Note: Wildcard filters do not have any attributes that can be changed.
8. Click the **Next** button and choose Exclude Files.
9. On the Basic tab of the Exclude element, specify the values for the following attributes:

   Pattern

   The pattern to match. An asterisk (*) matches any number of characters and a question mark (?) matches a single character.

   Case Sensitive

   Specify whether or not the pattern is case sensitive.
10. Click the **Add** button and select the Get Files menu item.
11. On the Basic tab of the Get Files element, specify values for the following attributes:

    Source Files Variable

    The name of a variable of type Remote File List which contains the files to retrieve from the remote server. (Created in step 5.)

    Destination Directory

    Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
12. Click the **Save** button when finished.

FTP Task

The FTP task allows you to specify the FTP server that will be used for your Project.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
FTP Server	Select a pre-configured FTP server from the drop-down list.
Advanced Tab	
Input Session ID	Specify the reference to a valid FTP Session that was created using the Output Session ID of an FTP Task (e.g. ${FTPSession}).
Output Session ID	Specify an ID for this FTP Session. A variable with the specified session ID will be created. The session ID can be referenced in the subsequent FTP tasks.

FTP Server Tab	
Refer to the "FTP Servers Resource" on page 55 page for the FTP Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Get Files

The Get Files element allows you to download files from an FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. A file name is required, it may not be a directory name only.
Source File Variable	Specify the name of a variable of type Remote File List which contains the files to retrieve from the remote server. For example, ${variableName}.
Destination File	Specify the destination file when downloading a single file. This value is only used when downloading only a single file. Specifying this attribute when downloading multiple files will result in a compilation error.
Destination Directory	Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename

Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Put Files

The Put Files element allows you to upload files to an FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.

Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Append Files

The Append Files element appends a local file to a file on the FTP server using the current file type setting.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Change Directory

The Change Directory element changes the present directory on the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Working Directory	Specify a directory to set as the new working directory. The path may be absolute or relative to the current working directory. The special value ".." may be used to set the working directory to the parent of the current working directory.

Create Directory

The Create Directory element creates a new directory on the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Directory	Specify the directory to create. The directory path may be specified as absolute or relative to the current working directory. All non-existent directories specified in this path will be created.

Rename Files

The Rename Directory element renames a directory on the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
From	Specify the path and name of the file or directory to be renamed. The path may be specified as absolute or relative to the current working directory.
To	Specify the new path and name. The path may be specified as absolute or relative to the current working directory. This attribute is only valid if a single file is being renamed.
Advanced Tab	
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to rename on the remote server. For example, ${variableName}.
File Name Prefix	Specify the string to prepend to the name of the file(s) being renamed.
File Name Suffix	Specify the string to append to the name of the file(s) being renamed.
Search Pattern	Specify a pattern to search and replace in the file name(s). Both regular expressions and wildcard search patterns can be used and can be changed using the Pattern Type attribute.

Pattern Type	Specify the type of pattern to use when using search and replace on the file names. Default Value: wildcard
Replace With	Specify the pattern to replace in the file names. If using regular expressions and groups of the file names were captured, use the syntax $1, $2, etc... to reuse the captured segments. If using wildcard search and replace, use character * and ? to reuse the values the * and ? represented in the search for value.
Case Sensitive	Specify whether or not to use case sensitive matching when searching and replacing sections of the file names. Default Value: false

Delete Files

The Delete Files element removes (deletes) files from the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file to delete. The path may be specified as absolute or relative to the current working directory.
Directory	Specify the path and name of a single directory to delete. WARNING: The directory and everything in it will be deleted.
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to delete from the remote server. For example, ${variableName}.

Move Files

The Move Files element moves a file from one directory on the FTP server to another directory on the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to move. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type Remote File List which contains the files to move on the remote server. For example, ${variableName}.
Destination File	Specify the path and file name to which the source file is to be moved. This is valid only when moving a single file.
Destination Directory	Specify the directory to which the files should be moved. The directory may be an absolute path or relative to the current working directory.

Advanced Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files in the destination directory on the remote system that were successfully moved. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Moved Variable	If desired, specify the name of a variable which will contain the number of files successfully moved. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

List Files

The List Files element creates a variable of type File List which contains a list of files on the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File List Variable	If desired, specify the name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists it will be overwritten, otherwise it will be created.
Number of Files Found Variable	If desired, specify the name of a variable which will contain the number of files found. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Set File Permissions

The Set File Permissions element specifies whether a file can be read, written, or modified.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file of which to change permissions.
Directory	Specify the path and name of a single directory of which to change permissions. All files and sub directories will also be affected.

Input Files Variable	Specify the name of a variable of type Remote File List which contains the files of which to change permissions from the remote server. For example, ${variableName}.
Permissions	Specify the permissions to apply to the files and/or directories. The syntax is similar to the UNIX file permission setting which consists of three bits. Each bit represents a group and the value of the bit (0-7) represents the permission level. For example, the value of 7 means RWX (read/write/execute) permissions. So 777 means RWX for all groups (owner, group, and all users).

Execute Command

The Execute Command element allows you send FTP commands to the FTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Command	Specify the command to execute. The command will be sent as is to the FTP server.

MGet Files (Get Multiple Files)

The MGet element allows you to download multiple files from the FTP server to the local machine.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source Files	Specify the path and/or filter pattern. Leave blank to download all files in the current working directory.
Destination Directory	Specify the directory to which the files should be downloaded.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.

Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Manual Get

The Manual Get element allows you download a file from FTP servers that do not support full file directory paths.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. Unlike the regular Get, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the GET request.
Destination File	Specify the destination file.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	

Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded file on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Manual Put

The Manual Put element allows you upload a file to FTP servers that do not support full file directory paths.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload.
Destination File	Specify the destination file. Unlike the regular Put action, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the PUT request.
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct upload mode. Default Value: auto

Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Processed Source Files Variable	If desired, specify the name of a variable which will contain the file on the local system that was successfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

FTPS Task

The FTPS task allows you to securely transfer files using FTP over *SSL*. For more information about *FTPS* please refer to the "Quick Start for FTPS" on page 714 section. The FTPS task can perform Get, Put, Rename, Delete, Create Directory, and many more commands that are common to FTPS clients.

Active And Passive Modes

In Active mode, the FTP server will attempt to connect back to a port on the Managed File Transfer FTP client in order perform the data transfer. The challenge with Active mode is that your firewall may block the FTP server from trying to open a port back into your network.

In Passive mode, the FTP server does not need to connect back to a port on the Managed File Transfer FTP client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the FTP server, you may want to change the Use Passive Mode setting to **Yes** on the "FTPS Servers Resource" on page 59 Connection tab.

Transfer Auto-Resume for FTPS

If the FTPS connection breaks or is lost, Managed File Transfer can automatically re-establish a connection and resume where it left off. The Auto-Resume feature uses the Connection Retry Attempts and Connection Retry Interval settings specified in the "FTPS Servers Resource" on page 59 or at the task level.

If the connection is broken during a file transfer, files with an ASCII data type will be resent in their entirety to ensure data integrity. Files with a Binary data type will resume transferring the file. The connection retry attempts, transfers and the commands that are performed will be recorded in the job log when using Verbose and Debug log levels. The Transfer Auto-Resume is not available on the Append Files element.

Session Persistence

By default, when the FTPS task is finished, the connection with the server (session) will be disconnected and closed. When using an FTPS Task in a Loop or as part of a multi-step workflow, the FTPS session can be kept open and reused rather than closing and reopening the session for each FTPS Task to the same server. To keep a session open or to hand off the open session to the next FTPS task in a Project, use the Input Session ID and Output Session ID variables on the Advanced tab of the FTPS Task. If this is the first FTPS session in the Project and other tasks will use this connection, only specify the Output Session ID (for example, FTPSSession). The next task that uses the session would specify ${FTPSSession} in the Input Session ID field. When no additional tasks in the Project need the open session, it should be closed using the "Close Session Task" on page 432 (using the Session ID value of ${FTPSSession}).

Checksum Verification

Checksum verification can be added to the FTPS task to ensure that the source file is exactly the same as the destination file after a transfer completes successfully. This option is available on the Put, Get, Mget, Manual Get, and Manual Put elements. Both the CRC32 and MD5 algorithms are supported with the default and recommended algorithm being MD5. Errors may occur if the transfer was performed in ASCII mode, if the FTPS server doesn't support checksum verification or if the calculated values do not match.

Timestamp Preservation

Timestamp preservation is available in the FTPS task when using the Put or Manual Put elements. Typically, timestamps are updated each time a file moves, however in some instances the file's timestamp may need to be preserved. If supported by the server, the preserve timestamp option can retain the timestamp from when the file was originally placed in the source location (not when it was placed on the destination server).

SOCKS, HTTP, and Informatica Managed File Transfer Gateway Proxy

Managed File Transfer connects to a proxy server as a client and the proxy server redirects the traffic to the target FTPS server. Proxy settings for FTPS connections are defined at the "FTPS Servers Resource" on page 59 level or per FTPS Task. The FTPS Task can use SOCKS, HTTP, or Managed File Transfer Gateway proxy protocols when making a connection to a proxy server. The SOCKS connection in Managed File Transfer supports both version 4 and 5. The HTTP proxy, otherwise known as an HTTP tunneling proxy, provides an HTTP tunnel through which a transport can be established. When using a proxy server, obtain the correct proxy type and connection credentials from the proxy server administrator.

Example 1: FTPS Get Files

Follow the steps below to get a single file from an "FTPS Servers Resource" on page 59:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTPS task to the Project Outline.
2. On the Basic tab of the FTPS task, specify a value for the following attribute:

   FTPS Server

   A pre-configured FTPS server from the drop-down list.
3. Click the **Add** button in the sub-menu and select the Get Files menu item.
4. On the Basic tab of the Get Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to download.

   Destination File

   The destination file when downloading a single file.
5. Click the **Save** button when finished.

Note: If you want to FTP multiple files, then leave the Source File blank and click the **Add** button in the sub-menu and select the Add a File Set menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Example 2: FTPS Get a File Manually

Follow the steps below to use a Manual Get to download a single file from an "FTPS Servers Resource" on page 59:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTPS task to the Project Outline.
2. On the Basic tab of the FTPS Task, specify a value for the FTPS Server:

   FTPS Server

   A pre-configured FTPS server from the drop-down list.
3. Click the **Add** button and select the Get a File Manually menu item.
4. On the Basic tab of the Get a File Manually element, specify values for the following attributes:

   Source File

   The path and file name of a single file to download. Unlike the regular Get, the specified file name/path will not be altered in any manner and will be sent to the FTPS server as is in the GET request.

   Destination File

   The destination file when downloading a single file.
5. Click the **Save** button when finished.

Example 3: FTPS Put Files

Follow the steps below to upload a single file to an "FTPS Servers Resource" on page 59:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTPS task to the Project Outline.
2. On the Basic tab of the FTPS task, specify a value for the following attribute:

   FTPS Server

   A pre-configured FTPS server from the drop-down list.
3. Click the **Add** button in the sub-menu and select the Put Files menu item.
4. On the Basic tab of the Put Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to upload.

   Destination File

   The destination file on the FTPS server when uploading a single file.
5. Click the **Save** button when finished.

Note: If you want to FTPS multiple files, then leave the Source File blank and click the **Add** button in the sub-menu and select the Add a File Set menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Example 4: FTPS Put a File Manually

Follow the steps below to Manually Put (upload) a single file to an "FTPS Servers Resource" on page 59:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTPS task to the Project Outline.
2. On the Basic tab of the FTPS task, specify a value for the FTPS Server:

   FTPS Server

   A pre-configured FTPS server from the drop-down list.
3. Click the **Add** button and select the Put a File Manually menu item.
4. On the Basic tab of the Put a File Manually element, specify values for the following attributes:

   Source File

   Specify the path and file name of a single file to upload.

   Destination File

   Specify the destination file. Unlike the regular Put action, the specified file name/path will not be altered in any manner and will be sent to the FTPS server as is in the PUT request.
5. Click the **Save** button when finished.

Example 5: FTPS Create File List

"File Lists and File Sets" on page 116 allow you to iterate over a list of files and complete specific tasks sequentially. Follow the steps below to create a File List from a directory on a FTPS server:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTPS task to the Project Outline.
2. On the Basic tab of the FTPS task, specify a value for the FTPS Server:

   FTPS Server

   A pre-configured FTPS server from the drop-down list.
3. Click the **Add** button and select the Create a File List menu item.
4. On the Basic tab of the Create a File list element, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created.

   Number of Files Found Variable

   The name of a variable which will contain the number of files found. The variable may be used in subsequent tasks.
5. Click the **Add** button and select the Add a File Set menu item.
6. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the FTPS server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
7. Click the **Save** button when finished.

Example 6: FTPS Get Multiple Files Using a Wildcard Filter

Follow the steps below to get a multiple files from an "FTPS Servers Resource" on page 59 using a Wildcard Filter:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the FTPS task to the Project Outline.
2. On the Basic tab of the FTPS task, specify a value for the FTPS Server:

   FTPS Server

   A pre-configured FTP server from the drop-down list.
3. Click the **Add** button and select the Create a Files List menu item.
4. On the Basic tab of the Create a File list element, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created.

   Number of Files Found Variable

   The name of a variable which will contain the number of files found. The variable may be used in subsequent tasks.

5. Click the **Add** button and select the Add a File Set menu item.
6. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the FTPS server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
7. Click the **Add** button and select the Add a Wildcard Filter menu item. Note: Wildcard filters do not have any attributes that can be changed.
8. Click the **Add** button and choose ExcludeFiles.
9. On the Basic tab of the Exclude element, specify the values for the following attributes:

   Pattern

   The pattern to match. An asterisk (*) matches any number of characters and a question mark (?) matches a single character.

   Case Sensitive

   Specify whether or not the pattern is case sensitive.
10. Click the **Add** button and select the Get Files menu item.
11. On the Basic tab of the Get Files element, specify values for the following attributes:

    Source Files Variable

    The name of a variable of type Remote File List which contains the files to retrieve from the remote server. (Created in step 5.)

    Destination Directory

    Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
12. Click the **Save** button when finished.

FTPS Task

The FTPS task allows you to specify the FTPS server that will be used for your Project.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
FTPS Server	Specify or select a pre-configured FTPS server from the drop-down list.
Advanced Tab	
Input Session ID	Specify the reference to a valid FTPS Session that was created using the Output Session ID of an FTPS Task (e.g. ${FTPSSession}).
Output Session ID	Specify an ID for this FTPS Session. A variable with the specified session ID will be created. The session ID can be referenced in the subsequent FTPS tasks.

FTP Server Tab	
Refer to the "FTPS Servers Resource" on page 59 page for the FTPS Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Get Files

The Get Files element allows you to download files from an FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type Remote File List which contains the files to retrieve from the remote server. For example, ${variableName}.
Destination File	Specify the destination file when downloading a single file. This value is only used when downloading only a single file. Specifying this attribute when downloading multiple files will result in a compilation error.
Destination Directory	Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename

Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Verify Checksum	SSpecify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the succesfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Put Files

The Put Files element allows you to upload files to an FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.

Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Append Files

The Append Files element appends a local file to a file on the FTPS server using the current file type setting.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Change Directory

The Change Directory element changes the present directory on the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Working Directory	Specify a directory to set as the new working directory. The path may be absolute or relative to the current working directory. The special value ".." may be used to set the working directory to the parent of the current working directory.

Create Directory

The Create Directory element creates a new directory on the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Directory	Specify the directory to create. The directory path may be specified as absolute or relative to the current working directory. All non-existent directories specified in this path will be created.

Rename Files

The Rename Directory element renames a directory on the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
From	Specify the path and name of the file or directory to be renamed. The path may be specified as absolute or relative to the current working directory.
To	Specify the new path and name. The path may be specified as absolute or relative to the current working directory. This attribute is only valid if a single file is being renamed.
Advanced Tab	
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to rename on the remote server. For example, ${variableName}.
File Name Prefix	Specify the string to prepend to the name of the file(s) being renamed.
File Name Suffix	Specify the string to append to the name of the file(s) being renamed.

Search Pattern	Specify a pattern to search and replace in the file name(s). Both regular expressions and wildcard search patterns can be used and can be changed using the Pattern Type attribute. Click here for additional information.
Pattern Type	Specify the type of pattern to use when using search and replace on the file names. Default Value: wildcard
Replace With	Specify the pattern to replace in the file names. If using regular expressions and groups of the file names were captured, use the syntax $1, $2, etc... to reuse the captured segments. If using wildcard search and replace, use character * and ? to reuse the values the * and ? represented in the search for value.
Case Sensitive	Specify whether or not to use case sensitive matching when searching and replacing sections of the file names. Default Value: false

Delete Files

The Delete Files element removes (deletes) files from the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file to delete. The path may be specified as absolute or relative to the current working directory.
Directory	Specify the path and name of a single directory to delete. WARNING: The directory and everything in it will be deleted.
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to delete from the remote server. For example, ${variableName}.

Move Files

The Move Files element moves a file from one directory on the FTPS server to another directory on the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to move. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type Remote File List which contains the files to move on the remote server. For example, ${variableName}.

Destination File	Specify the path and file name to which the source file is to be moved. This is valid only when moving a single file.
Destination Directory	Specify the directory to which the files should be moved. The directory may be an absolute path or relative to the current working directory.
Advanced Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files in the destination directory on the remote system that were successfully moved. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Moved Variable	If desired, specify the name of a variable which will contain the number of files successfully moved. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

List Files

The List Files element creates a variable of type File List which contains a list of files on the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File List Variable	If desired, specify the name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists it will be overwritten, otherwise it will be created.
Number of Files Found Variable	If desired, specify the name of a variable which will contain the number of files found. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Set File Permissions

The Set File Permissions element specifies whether a file can be read, written, or modified.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file of which to change permissions.

Directory	Specify the path and name of a single directory of which to change permissions. All files and sub directories will also be affected.
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files of which to change permissions from the remote server. For example, ${variableName}.
Permissions	Specify the permissions to apply to the files and/or directories. The syntax is similar to the UNIX file permission setting which consists of three bits. Each bit represents a group and the value of the bit (0-7) represents the permission level. For example, the value of 7 means RWX (read/write/execute) permissions. So 777 means RWX for all groups (owner, group, and all users).

Execute Command

The Execute Command element allows you send FTPS commands to the FTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Command	Specify the command to execute. The command will be sent as is to the FTP server.

MGet (Get Multiple Files)

The MGET element allows you to download multiple files from the FTPS server to the local machine.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source Files	Specify the path and/or filter pattern. Leave blank to download all files in the current working directory.
Destination Directory	Specify the directory to which the files should be downloaded.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.

Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Manual Get

The Manual Get element allows you download a file from FTPS servers that do not support full file directory paths.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. Unlike the regular Get, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the GET request.
Destination File	Specify the destination file.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	

Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct download mode. Default Value: auto
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded file on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Manual Put

The Manual Put element allows you upload a file to FTPS servers that do not support full file directory paths.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload.
Destination File	Specify the destination file. Unlike the regular Put action, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the PUT request.
Transfer Options Tab	
Data Type	Specify the data type to use when transferring the files. The default value is 'auto' which uses the file extensions and/or the content type of the file to determine the correct upload mode. Default Value: auto

Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Please note that not all FTP servers support checksum verification, in which case you must turn off checksum verification to be able to transfer files. Also, transferring files in ASCII mode may result in checksum mismatch. Please make sure to explicitly set the Data Type to binary or image. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Some FTP servers implemented a proprietary command called XCRC for getting the checksum of the remote file. Most recent FTP standards recommend implementing a command called MD5, which uses the MD5 algorithm for calculating the checksums. Depending on the algorithm you choose, an appropriate command will be sent to the FTP server to request the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: MD5
Output Variables Tab	
Processed Source Files Variable	If desired, specify the name of a variable which will contain the file on the local system that was successfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

SFTP Task

The SFTP task allows you to securely transfer files using SSH File Transfer Protocol (Version 3). For more information about *SFTP* please refer to the "Quick Start for SFTP" on page 712 section.

Transfer Auto-Resume for SFTP

If the SFTP connection breaks or is lost, Managed File Transfer can automatically re-establish a connection and resume where it left off. The Auto-Resume feature uses the Connection Retry Attempts and Connection Retry Interval settings specified in the "SFTP Servers Resource" on page 66 or at the task level. The Transfer Auto-Resume feature is not available on the Append Files element.

Session Persistence

By default, when the SFTP task is finished, the connection with the server (session) will be disconnected and closed. When using an SFTP Task in a Loop or as part of a multi-step workflow, the SFTP session can be kept open and reused rather than closing and reopening the session for each SFTP Task to the same server. To keep a session open or to hand off the open session to the next SFTP task in a Project, use the Input Session ID and Output Session ID variables on the Advanced tab of the SFTP Task. If this is the first SFTP session in

the Project and other tasks will use this connection, only specify the Output Session ID (for example, SFTPSession). The next task that uses the session would specify ${SFTPSession} in the Input Session ID field. When no additional tasks in the Project need the open session, it should be closed using the "Close Session Task" on page 432 (using the Session ID value of ${SFTPSession}).

Timestamp Preservation

Timestamp preservation is available in the SFTP task when using the Put or Manual Put elements. Typically, timestamps are updated each time a file moves, however in some instances the file's timestamp may need to be preserved. If supported by the server, the preserve timestamp option can retain the timestamp from when the file was originally placed in the source location (not when it was placed on the destination server).

SOCKS, HTTP, and Informatica Managed File Transfer Gateway Proxy

Managed File Transfer connects to a proxy server as a client and the proxy server redirects the traffic to the target SFTP server. Proxy settings for SFTP connections are defined at the "SFTP Servers Resource" on page 66 level or per SFTP Task. The SFTP Task can use SOCKS, HTTP, or Managed File Transfer Gateway proxy protocols when making a connection to a proxy server. The SOCKS connection in Managed File Transfer supports both version 4 and 5. The HTTP proxy, otherwise known as an HTTP tunneling proxy, provides an HTTP tunnel through which a transport can be established. When using a proxy server, obtain the correct proxy type and connection credentials from the proxy server administrator.

Host Key Fingerprints

For added authentication, Host Key Fingerprints can be used by the client (Managed File Transfer), to verify the authenticity of the host SFTP server. If, when connecting to the SFTP server, the host key fingerprint entered into Managed File Transfer does not match the fingerprint on the server's private key, Managed File Transfer will error and then display a message that it does not trust the target server. This is to prevent connecting to the wrong server in a case where someone is trying to spoof the IP of the SFTP server in question resulting in the data going to a wrong and most likely malicious destination. Follow the steps below to add Host Key Fingerprint verification to a SFTP Task:

1. Contact the administrator of the host server to which the Managed File Transfer SFTP Task is connecting.
2. Ask them for the Fingerprint of the Private Key used in the SFTP session.
3. On the SFTP Task page, click the **SFTP Server** tab, open the SSH Keys fold and then type the fingerprint in the Host Key field.

SSH Algorithms

The options on the Algorithms fold allow customization of the supported algorithms for each SFTP connection. The entries in the left column are the available algorithms and the entries in the right column are the selected algorithms. By selecting one or more algorithms, only those will be used during the SFTP communication. If no algorithms are selected for a section, the defaults will be used. The Default Algorithms are listed on the Algorithms tab on the "SFTP Servers Resource" on page 66.

During the handshake process, the selected options are negotiated with the server, starting with the entry at the top of the list. The first cipher and mac and compression algorithms to match an algorithm supported by the server will be used for the connection. If your company prefers certain algorithms over others, use the arrow buttons to move that cipher to the Selected column and to set the order with the most preferred algorithm at the top. Press the CTRL key while clicking to select multiple entries.

Example 1: SFTP Get Files

Follow the steps below to get a single file from an "SFTP Servers Resource" on page 66:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SFTP task to the Project Outline.
2. On the Basic tab of the SFTP task, specify a value for the following attribute:

   SFTP Server

   A pre-configured SFTP server from the drop-down list.
3. Click the **Add** button in the sub-menu and select the **Get Files** menu item.
4. On the Basic tab of the Get Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to download.

   Destination File

   The destination file path when downloading a single file.
5. Click the **Save** button when finished.

Note: If you want to SFTP multiple files, then leave the **Source File** blank and click the **Action** link in the sub-menu and select the **Add a File Set** menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Example 2: SFTP Get a File Manually

Follow the steps below to use a Manual Get to download a single file from an "SFTP Servers Resource" on page 66:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SFTP task to the Project Outline.
2. On the Basic tab of the SFTP task, specify a value for the SFTP Server:

   SFTP Server

   A pre-configured SFTP server from the drop-down list.
3. Click the **Add** button and select the Get a File Manually menu item.
4. On the Basic tab of the Get a File Manually element, specify values for the following attributes:

   Source File

   The path and file name of a single file to download. Unlike the regular Get, the specified file name/path will not be altered in any manner and will be sent to the SFTP server as is in the GET request.

   Destination File

   The destination file when downloading a single file.
5. Click the **Save** button when finished.

Example 3: SFTP Put Files

Follow the steps below to upload a single file to an "SFTP Servers Resource" on page 66:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SFTP task to the Project Outline.
2. On the Basic tab of the SFTP task, specify a value for the following attribute:

   SFTP Server

   A pre-configured SFTP server from the drop-down list.
3. Click the **Add** button in the sub-menu and select the **Put Files** menu item.
4. On the Basic tab of the Put Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to upload.

   Destination File

   The destination file path on the SFTP server when uploading a single file.
5. Click the **Save** button when finished.

Note: If you want to SFTP multiple files, then leave the **Source File** blank and click the **Add** button in the sub-menu and select the **Add a File Set** menu item. Then follow the instructions in the "File Lists and File Sets" on page 116 topic.

Example 4: SFTP Put a File Manually

Follow the steps below to Manually Put (upload) a single file to an "SFTP Servers Resource" on page 66:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SFTP task to the Project Outline.
2. On the Basic tab of the SFTP task, specify a value for the SFTP Server:

   SFTP Server

   A pre-configured SFTP server from the drop-down list.
3. Click the **Add** button and select the Put a File Manually menu item.
4. On the Basic tab of the Put a File Manually element, specify values for the following attributes:

   Source File

   Specify the path and file name of a single file to upload.

   Destination File

   Specify the destination file. Unlike the regular Put action, the specified file name/path will not be altered in any manner and will be sent to the FTP server as is in the PUT request.
5. Click the **Save** button when finished.

Example 5: SFTP Create File List

"File Lists and File Sets" on page 116 allow you to iterate over a list of files and complete specific tasks sequentially. Follow the steps below to create a File List from a directory on a SFTP server:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SFTP task to the Project Outline.
2. On the Basic tab of the SFTP task, specify a value for the SFTP Server:

   SFTP Server

   A pre-configured SFTP server from the drop-down list.
3. Click the **Add** button and select the Create a File List menu item.
4. On the Basic tab of the Create a File list element, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created.

   Number of Files Found Variable

   The name of a variable which will contain the number of files found. The variable may be used in subsequent tasks.
5. Click the **Add** button and select the Add a File Set menu item.
6. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the SFTP server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
7. Click the **Save** button when finished.

Example 6: SFTP Get Multiple Files Using a Wildcard Filter

Follow the steps below to get a multiple files from an "SFTP Servers Resource" on page 66 using a Wildcard Filter:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SFTP task to the Project Outline.
2. On the Basic tab of the SFTP task, specify a value for the SFTP Server:

   SFTP Server

   A pre-configured SFTP server from the drop-down list.
3. Click the **Add** button and select the Create a Files List menu item.
4. On the Basic tab of the Create a File list element, specify values for the following attributes:

   File List Variable

   The name of a variable that will contain the list of files being created.

   Number of Files Found Variable

   The name of a variable which will contain the number of files found. The variable may be used in subsequent tasks.

5. Click the **Add** button and select the Add a File Set menu item.
6. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory on the SFTP server that contains the files to list.

   Recursive

   Specify whether or not to also download files from all sub-folders.
7. Click the **Add** button and select the Add a Wildcard Filter menu item. Note: Wildcard filters do not have any attributes that can be changed.
8. Click the **Next** button and choose Exclude Files.
9. On the Basic tab of the Exclude element, specify the values for the following attributes:

   Pattern

   The pattern to match. An asterisk (*) matches any number of characters and a question mark (?) matches a single character.

   Case Sensitive

   Specify whether or not the pattern is case sensitive.
10. Click the **Add** button and select the Get Files menu item.
11. On the Basic tab of the Get Files element, specify values for the following attributes:

    Source Files Variable

    The name of a variable of type Remote File List which contains the files to retrieve from the remote server. (Created in step 5.)

    Destination Directory

    Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
12. Click the **Save** button when finished.

SFTP Task

The SFTP task allows you to specify the SFTP server that will be used for your Project.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
SFTP Server	Select a pre-configured SFTP server from the drop-down list.
Advanced Tab	
Input Session ID	Specify the reference to a valid SFTP Session that was created using the Output Session ID of an SFTP Task (e.g. ${SFTPSession}).
Output Session ID	Specify an ID for this SFTP Session. A variable with the specified session ID will be created. The session ID can be referenced in the subsequent SFTP tasks.

Transfer Mode	Specify the mode to transfer files. Select one of the following options: - BINARY - ASCII Default is BINARY. **Note:** Connectivity to SFTP server version 4 is supported.
SFTP Server Tab	
Refer to the "SFTP Servers Resource" on page 66 page for the SFTP Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Get Files

The Get Files element allows you to download files from an SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. A file name is required, it may not be a directory name only.
Source File Variable	Specify the name of a variable of type Remote File List which contains the files to retrieve from the remote server. For example, ${variableName}.
Destination File	Specify the destination file when downloading a single file. This value is only used when downloading only a single file. Specifying this attribute when downloading multiple files will result in a compilation error.
Destination Directory	Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.

When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Put Files

The Put Files element allows you to upload files to an SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none

File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Append Files

The Append Files element appends a local file to a file on the SFTP server using the current file type setting.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	

Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Change Directory

The Change Directory element changes the present directory on the SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Working Directory	Specify a directory to set as the new working directory. The path may be absolute or relative to the current working directory. The special value ".." may be used to set the working directory to the parent of the current working directory.

Create Directory

The Create Directory element creates a new directory on the SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Directory	Specify the directory to create. The directory path may be specified as absolute or relative to the current working directory. All non-existent directories specified in this path will be created.

Rename Files

The Rename Directory element renames a directory on the SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
From	Specify the path and name of the file or directory to be renamed. The path may be specified as absolute or relative to the current working directory.

To	Specify the new path and name. The path may be specified as absolute or relative to the current working directory. This attribute is only valid if a single file is being renamed.
Advanced Tab	
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to rename on the remote server. For example, ${variableName}.
File Name Prefix	Specify the string to prepend to the name of the file(s) being renamed.
File Name Suffix	Specify the string to append to the name of the file(s) being renamed.
Search Pattern	Specify a pattern to search and replace in the file name(s). Both regular expressions and wildcard search patterns can be used and can be changed using the Pattern Type attribute.
Pattern Type	Specify the type of pattern to use when using search and replace on the file names. Default Value: wildcard
Replace With	Specify the pattern to replace in the file names. If using regular expressions and groups of the file names were captured, use the syntax $1, $2, etc... to reuse the captured segments. If using wildcard search and replace, use character * and ? to reuse the values the * and ? represented in the search for value.
Case Sensitive	Specify whether or not to use case sensitive matching when searching and replacing sections of the file names. Default Value: false

Delete Files

The Delete Files element removes (deletes) files from the SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file to delete. The path may be specified as absolute or relative to the current working directory.
Directory	Specify the path and name of a single directory to delete. WARNING: The directory and everything in it will be deleted.
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to delete from the remote server. For example, ${variableName}.

Move Files

The Move Files element moves a file from one directory on the FTP server to another directory on the SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to move. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type Remote File List which contains the files to move on the remote server. For example, ${variableName}.
Destination File	Specify the path and file name to which the source file is to be moved. This is valid only when moving a single file.
Destination Directory	Specify the directory to which the files should be moved. The directory may be an absolute path or relative to the current working directory.
Advanced Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files in the destination directory on the remote system that were successfully moved. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Moved Variable	If desired, specify the name of a variable which will contain the number of files successfully moved. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

List Files

The List Files element creates a variable of type File List which contains a list of files on the SFTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File List Variable	If desired, specify the name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists it will be overwritten, otherwise it will be created.
Number of Files Found Variable	If desired, specify the name of a variable which will contain the number of files found. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Set File Permissions

The Set File Permissions element specifies whether a file can be read, written, or modified.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file of which to change permissions.
Directory	Specify the path and name of a single directory of which to change permissions. All files and sub directories will also be affected.
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files of which to change permissions from the remote server. For example, ${variableName}.
Permissions	Specify the permissions to apply to the files and/or directories. The syntax is similar to the UNIX file permission setting which consists of three bits. Each bit represents a group and the value of the bit (0-7) represents the permission level. For example, the value of 7 means RWX (read/write/execute) permissions. So 777 means RWX for all groups (owner, group, and all users).

MGet (Get Multiple Files)

The MGet element allows you to download multiple files from the SFTP server to the local machine.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source Files	Specify the path and/or filter pattern. Leave blank to download all files in the current working directory.
Destination Directory	Specify the directory to which the files should be downloaded.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Manual Get

The Manual Get element allows you download a file from SFTP servers that do not support full file directory paths.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. Unlike the regular Get, the specified file name/path will not be altered in any manner and will be sent to the SFTP server as is in the GET request.
Destination File	Specify the destination file.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded file on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Manual Put

The Manual Put element allows you upload a file to SFTP servers that do not support full file directory paths.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload.

Destination File	Specify the destination file. Unlike the regular Put action, the specified file name/path will not be altered in any manner and will be sent to the SFTP server as is in the PUT request.
Transfer Options Tab	
Preserve Timestamp	Select the desired option for timestamp preservation. The timestamp preservation allows the destination files to have the same modification timestamp as the source files. Not all servers support the timestamp preservation feature. Default Value: none
Output Variables Tab	
Processed Source Files Variable	If desired, specify the name of a variable which will contain the file on the local system that was successfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

SCP Task

The Secure Copy (SCP) task allows you to securely exchange files with a server that supports SCP. The SCP task is much like the SFTP Task, using SSH File Transfer Protocol, except SCP only supports the following FTP commands: GET, MGET, and PUT (for a single file). If multiple files are required per SCP session, consider creating a "Loops" on page 148 to accomplish this task.

Session Persistence

By default, when the SCP task is finished, the connection with the server (session) will be disconnected and closed. When using an SCP Task in a Loop or as part of a multi-step workflow, the SCP session can be kept open and reused rather than closing and reopening the session for each SCP Task to the same server. To keep a session open or to hand off the open session to the next SCP task in a Project, use the Input Session ID and Output Session ID variables on the Advanced tab of the SCP Task. If this is the first SCP session in the Project and other tasks will use this connection, only specify the Output Session ID (for example, SCPSession). The next task that uses the session would specify ${SCPSession} in the Input Session ID field. When no additional tasks in the Project need the open session, it should be closed using the "Close Session Task" on page 432 (using the Session ID value of ${SCPSession}).

SOCKS, HTTP, and Informatica Managed File Transfer Gateway Proxy

Managed File Transfer connects to a proxy server as a client and the proxy server redirects the traffic to the target SCP server. Proxy settings for SCP connections are defined at the SCP Server resource level or per SCP Task. The SCP Task can use SOCKS, HTTP, or Managed File Transfer Gateway proxy protocols when making a connection to a proxy server. The SOCKS connection in Managed File Transfer supports both version 4 and 5. The HTTP proxy, otherwise known as an HTTP tunneling proxy, provides an HTTP tunnel through which a transport can be established. When using a proxy server, obtain the correct proxy type and connection credentials from the proxy server administrator.

Host Key Fingerprints

For added authentication, Host Key Fingerprints can be used by the client (Managed File Transfer), to verify the authenticity of the host SCP server. If, when connecting to the SCP server, the host key fingerprint entered into Managed File Transfer DOES NOT match the fingerprint on the server's private key, Managed File Transfer will error out saying it does not trust the target server. This is to prevent connecting to the wrong server in a case where someone is trying to spoof the IP of the SCP server in question resulting in the data going to a wrong and most likely malicious destination. Follow the steps below to add Host Key Fingerprint verification to a SCP Task:

1. Contact the administrator of the host server to which the Managed File Transfer SCP Task is connecting.
2. Ask them for the Fingerprint of the Private Key used in the SCP session.
3. On the SCP Task page, click the **SCP Server** tab, open the SSH Keys fold and then type the fingerprint in the Host Key field.

SSH Algorithms

The options on the Algorithms fold allow customization of the supported algorithms for each SCP connection. The entries in the left column are the available algorithms and the entries in the right column are the selected algorithms. By selecting one or more algorithms, only those will be used during the SCP communication. If no algorithms are selected for a section, the defaults will be used. The Default Algorithms are listed on the Algorithms tab on the SCP Server.

During the handshake process, the selected options are negotiated with the server, starting with the entry at the top of the list. The first cipher and mac and compression algorithms to match an algorithm supported by the server will be used for the connection. If your company prefers certain algorithms over others, use the arrow buttons to move that cipher to the Selected column and to set the order with the most preferred algorithm at the top. Press the CTRL key while clicking to select multiple entries.

Example 1: SCP Get File

Follow the steps below to get a single file from an SCP Server:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SCP task to the Project Outline.
2. On the Basic tab of the SCP task, specify a value for the following attribute:

   SCP Server

   A pre-configured SCP server from the drop-down list.
3. Click the **Add** button in the sub-menu and select the Get Files menu item.
4. On the Basic tab of the Get Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to download.

   Destination File

   The destination file when downloading a single file.
5. Click the **Save** button when finished.

Example 2: SCP Put File

Follow the steps below to upload a single file to an SCP Server:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the SCP task to the Project Outline.
2. On the Basic tab of the SCP task, specify a value for the following attribute:

   SCP Server

   A pre-configured SCP server from the drop-down list.
3. Click the **Add** button in the sub-menu and select the Put Files menu item.
4. On the Basic tab of the Put Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to upload.

   Destination File

   The destination file on the SCP server when uploading a single file.
5. Click the **Save** button when finished.

SCP Task

The SCP task allows you to specify the SCP server that will be used for your Project.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
SCP Server	Select a pre-configured SCP server from the drop-down list.
Advanced Tab	
Input Session ID	Specify the reference to a valid SCP Session that was created using the Output Session ID of an SCP Task (e.g. ${SCPSession}).
Output Session ID	Specify an ID for this SCP Session. A variable with the specified session ID will be created. The session ID can be referenced in the subsequent SCP tasks.
SCP Server Tab	
Refer to the "SFTP Servers Resource" on page 66 page for the SCP Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.

Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Get Files

The Get Files element allows you to download files from an SCP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. A file name is required, it may not be a directory name only.
Destination File	Specify the destination file when downloading a single file. This value is only used when downloading only a single file. Specifying this attribute when downloading multiple files will result in a compilation error.
Destination Directory	Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Put Files

The Put Files element allows you to upload files to an SCP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
Transfer Options Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

MGet (Get Multiple Files)

The MGet element allows you to download multiple files from the SCP server to the local machine.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source Directory	Specify the remote directory from which to download files. This value can be an absolute or relative path. Relative paths will be relative to the current working directory of the server. If left blank, files will download from the current working directory on the server.
Destination Directory	Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.

File Name Pattern	Specify the wildcard file name pattern to match files to download. For example, *.txt will download all files from the source directory that end with '.txt'.
Recursive	Specify whether or not sub-directories and files that match the given file name pattern will also be downloaded. Default Value: false
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Close Session Task

The FTP, FTPS, SFTP, SCP and Execute SSH Commands tasks can optionally keep a session alive after the task finishes by specifying an Output Session ID on them. This is useful to keep an existing connection alive inside of a loop or over multi-step workflows. The Close Session task closes the specified session after it is no longer needed. If a session is persisted and this task is not included in a Project, the session will automatically be disconnected and closed at the end of the Project.

Example 1: Close an FTP Session

Follow the steps below to close an open session:

1. From within the Project Designer page, expand the FTP folder in the Component Library, and then drag the Close Session task to the Project Outline.
2. On the Basic tab of the Close Session task, specify a value for the Session ID:

   Session ID

   The Output Session ID specified on the Advanced tab of an FTP, FTPS, SFTP, SCP and Execute SSH Commands Task.
3. Click the **Save** button when finished.

   For example, a Project gets a set of .CSV files from an FTP server, converts them to XML, and then uploads them back to the same FTP server in the same FTP session. The Close Session task closes the FTP session and the Project completes.

Close Session

The Close Session task closes a persisted FTP, FTPS, SFTP, or SCP session after it is no longer needed.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Session ID	Specify the Session ID to close (e.g. ${FTPSession}). The specified session variable may represent any of the FTP protocols, including FTP, FTPS, SFTP and SCP session.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Job Control Tasks

Job Control tasks contain functions that can be used in Projects to control execution flow.

Call Module Task

The Call Module task executes another module within a Project. A module is like a sub-routine that allows Chapter 5, “Task Reference” on page 227 and “Loops” on page 148 to be logically grouped together. The Call Module task executes the module and when the processes in this module complete, control will be returned to the point from which it was called. A module can be called and executed more than once before the Project ends.

Example 1: Call Module

Perform the following steps to call a module based on a condition. The module called must exist in the current Project.

1. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the Call Module task to the Project Outline.
2. On the Basic tab, specify the name of the module that will execute.
3. On the Control tab, specify the Execute Only If condition for when the module will be called.

Call Module Task

The Call Module task executes another module within a Project.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Module	Specify the name of the Module to be called. The value is required must be the name of only one Module. This value is case sensitive.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Call Project Task

Projects can be designed to call other *Projects* in the same Managed File Transfer installation. This is useful when you want to create reusable logic that multiple Projects can execute.

One example usage would be to create a Project that accepts a file name from a "User Defined Variables" on page 112 and encrypts the file with a public key. Then other Projects that need that same functionality can simply call that Project and pass in the file to encrypt.

By default, the **Run In Same Job** attribute is set to true. When this attribute is set to true, the specified Project is called and the current Project will wait until the called Project completes. The called Project will not generate a new job number, job log or workspace. When set to false, the specified Project is submitted for execution as a separate job, which will have its own job number, job log, workspace etc.

If you specify to run the Project in a separate job you should consider whether you want the calling Project to wait for the job to finish (interactive mode) or if the calling Project should kick off the other Project and immediately continue executing (batch mode). By default, the **Mode** attribute is set to interactive. When calling the Project is in "Execution from Administrator" on page 183 Mode, the Advanced tab allows you to specify the "Job Queue Manager" on page 217 and queue priority the called Project will execute in. If no Job Queue is selected from the calling Project, the called Project will execute in the Job Queue specified in its own Project. If the called Project does not have a specified Job Queue, the Project will execute in the default Job Queue.

When calling a Project you need to indicate whether or not all user-defined variables should be passed over to the Project being called. By default, the **Pass User Variables** attribute is set to false. User-defined variables are variables that belong to the parent Project, whether they are Project variables, or variables created "on the fly" by some other task. Variable sub-elements of the Call Project Task will always be passed to the called Project, regardless of this setting. This setting is only valid if **Run In Same Job** is set to true. If **Run In Same Job** is set to false, this value will be ignored.

The Return User Variables indicates whether or not the user variables created by the called project are returned back to this project. If set to true, after the called project finishes, all user defined variables (except RowSets) will be accessible to this project. This setting is valid only when Run In Same Job is set to true. If **Run In Same Job** is set to false, this value will be ignored.

Example 1: Call Project

Follow the steps below to call a Project:

1. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the Call Project task to the Project Outline.
2. On the Basic tab of the Call Project task, click the  icon beside the **Project** field to select the Project from a pop-up window.
3. Click the **Save** button when finished.

Call Project Task

The Call Project task allows you to call other Projects in the same Managed File Transfer installation.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Project	Specify the project to be called. The value must contain the full path to the project. For example, /My Folder/My Project. Project names and folders are case sensitive.

Run in Same Job	Specify whether or not the project should be executed in the same job as the calling project's job. When this attribute is set to true, the specified project is called and the current project will wait until the calling project completes. The calling project will not generate a new job number, job log or workspace. When set to false, the specified project is submitted for execution as a separate job, which will have its own job number, job log, workspace etc. Default Value: true
Pass User Variables	Specify whether or not to pass all user-defined variables to the project being called. User-defined variables are variables that belong to this project, whether they are project variables, or variables created "on the fly" by some other task. Variable sub-elements of the Call Project Task will always be passed to the called project, regardless of this setting. This setting is only valid if Run In Same Job is set to true. If Run In Same Job is set to false, this value will be ignored. Default Value: false
Return User Variables	Specify whether or not to return the user variables created by the called project back to this project. If set to true, after the called project finishes, all user defined variables (except RowSets) will be accessible to this project. This setting is valid only when Run In Same Job is set to true. Default Value: false
Mode	Specify the execution mode for the called project. Valid values are interactive and batch. This option is valid only if Run In Same Job is set to false. When Run In Same Job is set to true, this value is ignored, as the caller project must always wait until the called project finishes. Default Value: interactive
Advanced Tab	
Job Queue	Specify the job queue to run within when executed in batch mode. If not specified, default queue will be used.
Job Name	Specify a name which identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters. Spaces are allowed.
Queue Priority	Specify the priority the called project should get while it sits in the Job Queue. If Run In Same Job is set to true, this value is ignored. Default Value: 5 (Normal)
Run Priority	Specify the priority the called project should get when it is running. If Run In Same Job is set to true, the project will use the same run priority as the caller project and this value will be ignored. Default Value: 5 (Normal)
Output Variables Tab	
Job Number Output Variable	If desired, specify the name of a variable which will contain the job number of the called project. The variable will be created if it does not exist.
Message Output Variable	If desired, specify the name of a variable which will contain the resulting message of the called project. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Variable

Use the Variable element to pass the value of a variable to another Project.

Field	Definition
Basic Tab	
Name	Specify a name for this variable. The name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores(_) and periods(.).
Value	Specify the value for this variable.

Call Remote Project Task

The Call Remote Project task is very similar to the "Call Project Task" on page 434 except that it can be used to call Projects on another installation of Managed File Transfer.

Example 1: Call Remote Project

Follow the steps below to call a Project on another instance of Managed File Transfer:

1. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the Call Remote Project task to the Project Outline.
2. On the Basic tab of the Call Remote Project task, specify values for the following attributes:

   Informatica Managed File Transfer Server

   An Managed File Transfer Server Resource.

   Project

   The "File Paths" on page 161 and name of the Project to execute.
3. Click the **Save** button when finished.

Call Remote Project Task

The Call Remote Project task allows you to call other Projects in remote Managed File Transfer installations.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Informatica MFT Server	Select a pre-configured Informatica MFT Server from the drop-down list.
Project	Specify the project on the remote system that is to be executed.
Mode	Specify the mode to execute the project in. Interactive mode means the current process will wait until the called project is finished before continuing. Batch means the project will be submitted and the current process will immediately continue executing. Default Value: interactive
Job Queue	Specify the remote job queue to run within when executing in batch mode. If not specified, default queue will be used.
Job Name	Specify a name which identifies the Job. This name should be descriptive enough so Admin Users can quickly identify this Job from a report or list. The Job Name cannot exceed 50 characters. Spaces are allowed.
Priority	Specify the priority the remote project should have when being executed. Valid values are between 1 and 10 inclusive, with 1 being the lowest priority and 10 being the highest priority. Default Value: 5
Output Variables Tab	
Job Number Variable	If desired, specify the name of a variable which will contain the job number of the executed project. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Status Code Variable	If desired, specify the name of a variable which will contain the status code of the executed project. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Message Variable	If desired, specify the name of a variable which will contain the message of the executed project. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Informatica Managed File Transfer Server Tab	
Refer to the "Informatica MFT Server Resource" on page 92 page for the Informatica MFT server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module

Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Variable

Use the Variable element to pass the value of a variable to another Project on a remote Managed File Transfer installation.

Field	Definition
Basic Tab	
Name	Specify a name for this variable. The name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores(_) and periods(.).
Value	Specify the value for this variable.

Exit Module Task

The Exit Module task can be used to exit a Module at a particular point. If the module was called from another module, control will be routed back to the calling module and processing will continue.

Example 1: Exit Module

Perform the following steps to exit a module based on the value of a variable.

1. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the Exit Module task to the Project Outline.
2. On the Control tab of the Exit Module task, specify the Execute Only If condition for when the module should exit.
3. Click the **Save** button.

Exit Module Task

The Exit Module task can be used to exit a Module at a particular point.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Exit Project Task

The Exit Project task can be used to exit a Project at any given time. This task can be executed conditionally by using the "Execute Only If" attribute on the Control tab or by using an "IF Condition" on page 146.

Example 1: Exit Project

Perform the following steps to exit a Project based on the value of a variable.

1. From within the Project Designer page, expand the Job Control folder in the Component Library, and then drag the Exit Project task to the Project Outline.
2. On the Control tab of the Exit Project task, specify the Execute Only If condition for when the Project should exit.
3. Click the **Save** button.

Exit Project Task

The Exit Project task can be used to exit a Project at any given time.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Miscellaneous Tasks

Miscellaneous tasks contain a wide range of functions that can be used throughout Projects to support other tasks and to control execution flow.

Outdated Tasks

If improvements are made to a Task which may change its existing behavior, then a new version number of that Task will be created. Each version of a Task is numbered using a format of x.y, where x is the major version number and y is the minor version number of the Task. For instance, the version number 1.0 represents the first version of a Task. Version 2.0 represents the next major version of a Task and so on.

Even though a new version of a Task may be made available by Informatica in a product upgrade, existing Projects will continue to use the version of the Task(s) when those Projects were created. Those Projects will not automatically use the latest versions. This preserves the behavior of existing Projects, which allows you to upgrade Managed File Transfer without having to retest all of your Projects.

For example, to support Excel 2007 documents (.xlsx), changes were required to how the Read Excel and Write Excel Tasks functioned. So a new version 2.0 of the Excel Tasks were created, but any existing Projects will still use the 1.0 version of those Excel Tasks to preserve their behavior.

When adding a new Task to a Project, the Task will default to use its latest version. If the execution of a Task is not producing the desired outputs, you can choose an earlier version of a Task (if available) by using one of the following methods:

1. Create New Task using Prior Version
2. Convert existing Tasks to Newer or Prior versions

Create New Task using Prior Version

When adding a new Task to a Project, you can choose an earlier version of a Task.

- From within the Project Designer page, navigate to the **Miscellaneous** > **Outdated Tasks** folder in the Component Library, and then drag the outdated task to the Project Outline.

  Note: This method is for advanced users. It is recommended to make a "Copy Projects" on page 173 of your Project before changing the Version number for any Tasks in the Project.

Convert existing Tasks to Newer or Prior versions

When converting an existing Task, you can choose a different version.

1. Open the Project in which to change the Task version Number.
2. From the page toolbar, click  **Show XML**.
3. In the Project XML page, locate the version number for a Task and change it to the desired version. In the example below, the yellow highlight indicates where the Read Excel Task could be updated to 2.0 or where the Read Excel Task could be downgraded to 1.0.
4. When complete, click the **Validate and Save** button. The changes will be visible in the Project Designer.

Close RowSet Task

Although a RowSet is closed when a project finishes, you may want to close the RowSet before the Project finishes.

For instance, while the RowSet is open, it will maintain a lock on the file or database table. If the Project needs to perform an action on that file which requires write access, such as Move or Delete, it must first close the RowSet before it can perform that action and finish the Project successfully.

Example: Close RowSet

Only the first 5 records of a CSV file need to be read into a RowSet for further processing. After processing those records, the CSV file needs to be moved to an archive folder. If remaining records in the file were not processed, then a Close RowSet task must be used to release the lock on the CSV file before it can be moved.

1. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Close RowSet task to the Project Outline.
2. On the Basic tab of the Close RowSet task, specify the RowSet Variable that needs to be closed.
3. Place the Close RowSet task directly above the Move task in the project.
   a. Right-click the Close RowSet task in the Project Outline panel.
   b. From the drop-down menu, point to Edit and then move the task up or down to the appropriate location in the project (above the Move Task).
4. Click the **Save** button.

Close RowSet Field Definitions

The Close RowSet task allows you close a RowSet before a Project finishes.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
RowSet Variable	Specify the variable reference to a RowSet that needs to be closed. (e.g. ${myRowSet}).
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Create Workspace Task

Managed File Transfer can create a workspace directory for temporarily storing files while executing a Project. Please refer to the "Workspaces" on page 160 section for more information.

Create Workspace Field Definitions

Use the Create a Workspace task to store temporary files while executing a Project.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Delete Workspace Task

Managed File Transfer can create a workspace directory for temporarily storing files while executing a Project. In order to minimize disk space usage, you should delete a workspace when it is no longer needed. Please refer to the "Workspaces" on page 160 section for more information.

Delete Task Field Definitions

Use this task to delete the Project's workspace directory and any files contained within it.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Deny Trigger Event Task

The Deny Trigger Event task can be used by the following types of "Trigger Manager" on page 206 events:

- Before AS2 MDN Send – Can be used to validate the content of AS2 messages, and then return a failed MDN receipt
- Before Shared Drive Upload – Can prevent a file from being uploaded into Shared Drive
- Before Secure Mail Send – Can stop a file from being sent through Secure Mail
  This task is particularity useful when used in conjunction with the ICAP task to scan files for viruses, inappropriate content, or restricted information. The Deny Trigger Event task can only be used in Projects that are on the same server as the Trigger, and can only be run "Execution from Administrator" on page 183 (the Job be cannot be sent to batch) from the Trigger.

Example 1: Send a Failed MDN Receipt for Unauthorized File Attachments

An Admin User wants to scan and delete AS2 file attachments that contain viruses or unauthorized data. If files are found to contain unauthorized data, the Deny Trigger task will be used to send a failed MDN receipt to the sender of the files.

An Admin User creates a Trigger using the Before AS2 MDN Send event type. The Trigger will use the Call Project action to call a local Project that uses an ICAP resource to scan the file attachments. If any file attachment contains a virus or unauthorized data, the Project will delete the file and report a failure message to the Trigger, and the Trigger will send a failed AS2 MDN receipt.

Use the following instructions to scan AS2 file attachments:

1. Create the Scan AS2 Messages Project
2. Create the Before AS2 MDN Send Trigger

Step 1: Create the Scan AS2 Messages Project

1. From the main menu, select **Workflows** and then click the Projects link.
2. In the Projects page, drill-down to the folder in which to create the new Project.
3. Click the Create a Project link in the sub-menu.
4. Type the Project name and description, and then click **Save**.
5. The Managed File Transfer Project Designer will open.
6. Expand the Loops folder in the Component Library, and then drag the For-Each task to the Project Outline.
7. On the For-Each Loop, specify the following fields:

Items Variable - Specify the fileList variable. This is a "File Lists and File Sets" on page 116 variable that contains AS2 Message file attachments and will be supplied from the Trigger that you will create in Step 2 Create the Before AS2 MDN Send Trigger.

Current Item Variable - Specify a variable name which will be populated with the item at the current index. The variable can then be used in the tasks inside the loop or anywhere in the project. The value must be a valid identifier (e.g. myItem).

8. From within the Project Designer page, expand the Web folder in the Component Library, drag the ICAP task to the Project Outline, and then place it inside the For-Each Loop you created in step g.
9. On the ICAP task, specify the following fields:
ICAP Server

   Select a pre-configured ICAP server from the drop down list.

Source File

   Specify the Current Item Variable created in step g.
10. Click the ICAP Task **On Error** tab. Specify the following fields:
On Error - Specify The call:[module] option, and then replace [module] with the name of the module that will be called (which will be added in the next step).
11. From within the Project Designer page, expand the Project folder in the Component Library, drag the Module task to the Project Outline, and place it below the Main module.
12. On the Module task, specify the Module Name from step j.
13. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, drag the Deny Trigger Event task to the Project Outline, and place it below the Deny Trigger module.
14. On the Deny Trigger Event Task, specify the following fields:
Reason - The reason for sending a failed AS2 MDN receipt. This reason will appear in the Job Log and Audit Log.
15. From within the Project Designer page, expand the File System folder in the Component Library, drag the Delete task to the Project Outline, and place it below the Deny Trigger task.
16. On the Delete task, specify the following fields:
Specify the name of a variable of type File List which contains the files to delete. For example, ${fileList}
17. Click the **Save** button.

Step 2: Create the Before AS2 MDN Send Trigger

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. In the "Trigger Manager" on page 206 page, click the Add Trigger link in the page toolbar.
4. The Select Event Window appears. Select the Before AS2 MDN Send Event Type and then click the **Continue** button.
5. Specify a Name for the Trigger on the **General** tab, and then click the **Action** tab.
6. On the Action tab, specify the following fields:
Project

   Specify the Scan AS2 Messages Project (created in "Step 1: Create the Scan AS2 Messages Project" on page 445) to run. Click the button to navigate to the Project.

User

The Admin User account that is used to execute the Project.

Password

The Admin User password. If encryption on the password is required, click the **Encrypt...** button.

Variables

When the Before AS2 MDN Send event was selected in step d, the default fileList variable is populated. This variable is passed to the to the Scan AS2 Messages Project.

7. Click the **Save** button to add the Trigger.

Example 2: Deny a Shared Drive Upload

An Admin User wants to prevent Web Users from uploading files to Shared Drive that contain viruses or unauthorized data.

An Admin User creates a Trigger using the Before Shared Drive Upload event type. The Trigger will use the Call Project action to call a local Project that uses an ICAP resource to scan files. If the files contain a virus or unauthorized data, the Project reports a failure to the Trigger, and the Trigger will not allow the files to be uploaded. When Web Users attempt to upload multiple files at once, the Trigger is invoked for each file being uploaded.

Use the following instructions to prevent Web Users from uploading restricted content to Shared Drive:

1. Create the Shared Drive Deny Trigger Project
2. Create the Before Shared Drive Upload Trigger

Step 1: Create the Shared Drive Deny Trigger Project

1. From the main menu, select **Workflows** and then click the Projects link.
2. In the Projects page, drill-down to the folder in which to create the new Project.
3. Click the Create a Project link in the sub-menu.
4. Type the Project name and description, and then click **Save**.
5. The Managed File Transfer Project Designer will open.
6. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the ICAP task to the Project Outline.
7. On the ICAP task, specify the following fields:

   ICAP ServerSelect a pre-configured ICAP server from the drop down list.

Source File - Specify the file variable. This variable contains the name of the file supplied from the Trigger that you will create in "Step 2: Create the Before Shared Drive Upload Trigger" on page 448.

1. Click the ICAP Task **On Error** tab. Specify the following fields:
   On Error - Specify The call:[module] option, and then replace [module] with the name of the module that will be called (which will be added in the next step).
2. From within the Project Designer page, expand the Project folder in the Component Library, drag the Module task to the Project Outline, and place it below the Main module.
3. On the Module task, specify the Module Name from step h.
4. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, drag the Deny Trigger Event task to the Project Outline, and place it below the Deny Trigger module.
5. On the Deny Trigger Event Task, specify the following fields:
   Reason - The reason for denying the event. This reason will appear in the Job Log and Audit Log.
6. Click the **Save** button.
   The following image illustrates the Project Outline for the Deny Trigger task:

Step 2: Create the Before Shared Drive Upload Trigger

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.
3. In the "Trigger Manager" on page 206 page, click the Add Trigger link in the page toolbar.
4. The Select Event Window appears. Select the Before Shared Drive Upload Event Type and then click the **Continue** button.
5. Specify a Name for the Trigger on the **General** tab, and then click the **Action** tab.
6. On the Action tab, specify the following fields:

   Project

   Specify the Shared Drive Deny Trigger Project (created in "Step 1: Create the Shared Drive Deny Trigger Project" on page 447) to run. Click the button to navigate to the Project.

   User

   The Admin User account that is used to execute the Project.

   Password

   The Admin User password. If encryption on the password is required, click the **Encrypt...** button.

   Variables

   When the Before Shared Drive Upload event was selected in step d, the default file Variable is populated. This variable is passed to the to the Deny Trigger Project.
7. Click the **Save** button to add the Trigger.

Example 3: Deny a Secure Mail Message Before it is Sent

An Admin User wants to prevent Web Users from sending Secure Mail Messages that contain viruses or unauthorized data.

An Admin User creates a Trigger using the Before Secure Mail Send event type. The Trigger will use the Call Project action to call a local Project that uses an ICAP resource to scan the file attachments. If the file attachment contains a virus or unauthorized data, the Project reports a failure message to the Trigger, and the Trigger will not allow the Secure Mail Message to be sent.

Use the following instructions to prevent Web Users from sending restricted content through Secure Mail:

1. Create the Secure Mail Deny Trigger Project
2. Create the Before Send Secure Mail Trigger

Step 1: Create the Secure Mail Deny Trigger Project

1. From the main menu, select **Workflows** and then click the Projects link.
2. In the Projects page, drill-down to the folder in which to create the new Project.
3. Click the Create a Project link in the sub-menu.
4. Type the Project name and description, and then click **Save**.
5. The Managed File Transfer Project Designer will open.
6. Expand the Loops folder in the Component Library, and then drag the For-Each task to the Project Outline.
7. On the For-Each Loop, specify the following fields:
   Items Variable - Specify the package:attachmentList variable. This is a "File Lists and File Sets" on page 116 variable that contains the Secure Mail Package file attachments and will be supplied from the Trigger that you will create in "Step 2: Create the Before Shared Drive Upload Trigger" on page 448.

   Current Item Variable - Specify a variable name which will be populated with the item at the current index. The variable can then be used in the tasks inside the loop or anywhere in the project. The value must be a valid identifier (e.g. myItem).
8. From within the Project Designer page, expand the Web folder in the Component Library, drag the ICAP task to the Project Outline, and then place it inside the For-Each Loop you created in step g.
9. On the ICAP task, specify the following fields:
   ICAP Server

   Select a pre-configured ICAP server from the drop down list.
   Source File - Specify the Current Item Variable created in step g.
10. Click the ICAP Task **On Error** tab. Specify the following fields:
    On Error - Specify The call:[module] option, and then replace [module] with the name of the module that will be called (which will be added in the next step).
11. From within the Project Designer page, expand the Project folder in the Component Library, drag the Module task to the Project Outline, and place it below the Main module.
12. On the Module task, specify the Module Name from step j.
13. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, drag the Deny Trigger Event task to the Project Outline, and place it below the Deny Trigger module.
14. On the Deny Trigger Event Task, specify the following fields:
    Reason - The reason for denying the event. This reason will appear in the Job Log, Trigger Log, Audit Log, and Package Details View.
15. Click the **Save** button.
    The following image illustrates the Project Outline for the Deny Trigger task:

Step 2: Create the Before Send Secure Mail Trigger

1. Log in as an Admin User with the Trigger Manager role.
2. From the main menu, select **Workflows**, and then click the Triggers link.

3. In the "Trigger Manager" on page 206 page, click the Add Trigger link in the page toolbar.
4. The Select Event Window appears. Select the Before Secure Mail Send Event Type and then click the **Continue** button.
5. Specify a Name for the Trigger on the **General** tab, and then click the **Action** tab.
6. On the Action tab, specify the following fields:

   Project

   Specify the Deny Trigger Project to run (created in "Step 1: Create the Secure Mail Deny Trigger Project" on page 449). Click the ... button to navigate to the Project.

   User

   The Admin User account that is used to execute the Project.

   Password

   The Admin User password. If encryption on the password is required, click the **Encrypt...** button.

   Variables

   When the Before Secure Mail Send event was selected in step d, the default Package Variable is populated. This variable is passed to the to the Deny Trigger Project.
7. Click the **Save** button to add the Trigger.

When the Triggers are Invoked

The Triggers are invoked before an AS2 MDN receipt is sent, before a file is uploaded to Shared Drive, or before a Secure Mail Message is sent. The Trigger calls the Project and supplies the Project with a variable containing a list of files that will be sent. When the Project executes, the Project sends each attachment to the ICAP server. If a file is found to contain viruses, inappropriate content, or restricted content, the ICAP server returns an HTTP error response to the Project, and the Project's ICAP task will error. The ICAP task will then call the Project's Deny Trigger Module which executes the Deny Trigger Event task. The Deny Trigger Event task reports the reason for the failure to the Trigger, and the Trigger either prohibits Shared Drive uploads and Secure Mail messages, or reports an error on an AS2 MDN receipt.

Trigger Log

The Trigger Log will display the reason for the denial. The following example illustrates a denied Secure Mail Message:

Job Log

The reason the transfer is denied is recorded in the Job Log. The following example illustrates a denied Secure Mail Message:

```
6/11/15 7:48:38 PM            INFO      ICAP server returned status code '200'.
6/11/15 7:48:38 PM            ERROR     [9001 - Clearswift DLP Scan] File is
infected
6/11/15 7:48:38 PM            INFO      Routing the control to the module 'Deny
Trigger'
6/11/15 7:48:38 PM            INFO      Executing task 'denyTriggerEvent 1.0'
6/11/15 7:48:38 PM            INFO      DenyTriggerEvent reason: The Secure Mail
Package contained sensitive data.
6/11/15 7:48:38 PM            INFO      Finished task 'denyTriggerEvent 1.0'
6/11/15 7:48:38 PM            INFO      Exiting loop 'forEachLoop'
6/11/15 7:48:38 PM            INFO      Finished module 'Main'
6/11/15 7:48:38 PM            INFO      Finished project 'Deny Trigger Event'
6/11/15 7:48:38 PM            INFO      End Date and Time: 6/11/15 7:48:38 PM
```

View Package Details

The View Package Details screen (from the Secure Mail in the File Transfer Portal) will display the reason for the failure to the Web User.

Deny Trigger Event Field Definitions

Prevents a file from being sent when a Trigger is monitoring for AS2, Shared Drive, and Secure Mail transfers.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Reason	Specify the reason for denying the event
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Notify Consumer Task

Managed File Transfer can send custom notifications to consumers. The Notify Consumer Task is executed only if the *deny.event.auto.notifications* variable is created and set to `True`. For more information about creating the variable, see "Creating a Variable" on page 113.

Notify Consumer Task Definitions

Use this task to notify consumers when a file is ready for use.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Source File	Browse the repository to navigate to file path or enter the sourceFileVariable.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Print Task

The Print task writes information to the job log or to an output file if one is specified. The **Text** attribute can contain any static text and variables that should be printed. If an **Output File** attribute is specified it will write the text to that file. If an **Output File** is not specified then the text will be printed to the job log with a log level of INFO.

Example 1: Print the Value of Variables

Follow the steps below to print out the contents of a variable that has been previously defined:

1. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Print task to the Project Outline.
2. On the Basic tab of the Print task, specify the Text value:

   Text

   Any combination of static text and previously defined variables.
3. Click the **Save** button when finished.

Example 2: Printing the Values of a RowSet Variable Using a Loop

It is sometimes useful to troubleshoot Projects by using the Print task to print the values from a "RowSet" on page 121 variable to the Job Log. This is accomplished by adding a Print task within a "For-Each Loop" on page 152. Follow the steps below to print out the contents of a RowSet variable generated from a Read CSV task:

1. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Read CSV task to the Project Outline.
2. On the Basic tab of the Read CSV task, specify values for the Read CSV Task attributes:

   Input File

   The "File Paths" on page 161 and file name of a single file from which to read the data.

   Output Row

   Set VariableThe name of a variable which will contain the data read from the specified input file.
3. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For-Each Loop task to the Project Outline.
4. On the Basic tab of the For-Each Loop task, specify the values for the following attributes:

   Items Variable

   Specify the RowSet variable that contains the items to iterate over.

   Current Items Variable

   Specify a variable name which will be populated with the value of the row at the current index.
5. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Print task to the Project Outline.
6. On the Basic tab of the Print task, specify the Text value.

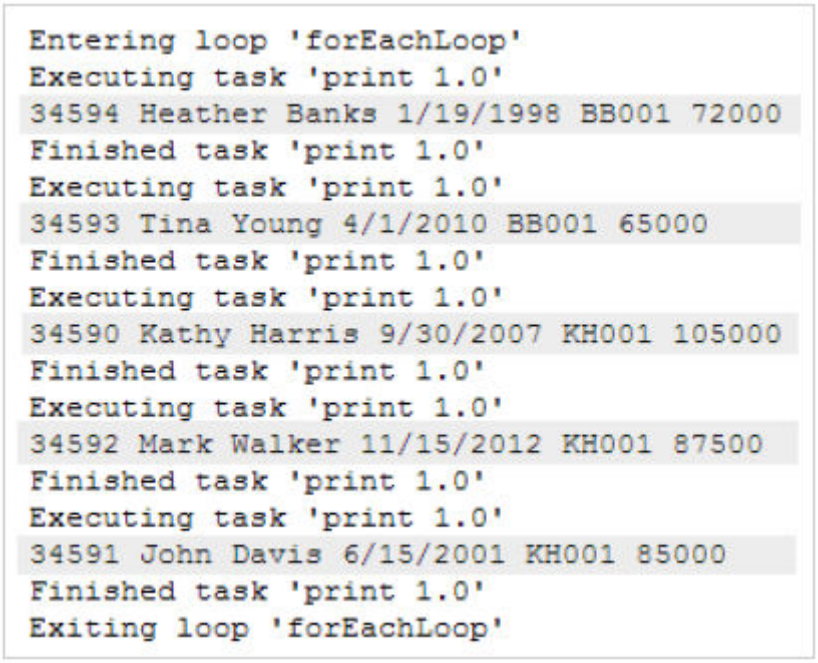
   Text

   Using the Current Items Variable, enter the values for the RowSet columns using the Column Index Numbers.
7. Click the **Save** button, and then click the **Execute Project** button. The Project will iterate through each Row in the RowSet and print the values from each column to the Job Log.

8. Once the Project has executed, click the **View Job Log** button.

   The Job Log will display the results of the Print task for each row in the RowSet variable (which is highlighted in the page shot below).

   The following image illustrates the Project Outline for the Print task using a Loop:



Example 3: Printing a File List to a File

Follow the steps below to crate a File List, and then print the File List to a file.

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
2. On the Basic tab of the Create File List task, specify values for the Create File List attributes:

   File List Variable

   The name of a variable that will contain the list of files being created. This will be a variable type of File List.

3. Click the **Add** button, and then choose File Set.
4. On the Basic tab of the File Set element, specify the values for the following attributes:

   Base Directory

   The starting directory for this File Set.

   Recursive

   Specify whether or not to process files from all sub-folders within the base directory.

5. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For-Each Loop task to the Project Outline.
6. On the Basic tab of the For-Each Loop task, specify the values for the following attributes:

Items Variable

Specify the File Set variable that contains the items to iterate over.

Current Items Variable

Specify a variable name which will be populated with the value of the row at the current index.

7. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Print task to the Project Outline.
8. On the Basic tab of the Print task, specify the Text value.

   Text

   Enter the Current Items Variable created in step 7. Optionally, use the "Expression Wizard" on page 130 to add the "System Variables" on page 114 '${system.carriageReturn}' after the file variable. The Carriage Return variable will add a line break at the end of each file name printed in the file.
9. On the Advanced tab of the Print task, specify the following attributes:

   Output File

   The path and file name of the output file that the message will be printed to.

   Append

   Specify whether or not to append data to the end of the specified file. Choose True.
10. Click the **Save** button, and then click the **Execute Project** button. The Project will iterate through each file in the File Set and output the file names (including the file path) to the file specified.

Print Task

The Print task writes information to the job log or to an output file if one is specified.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Text	Specify the text to be printed.
Advanced Tab	
Output File	Specify the path and file name of the output file that the message will be printed to. If no file is specified, the message will be printed to the job log as an 'INFO' type message.
Append	Specify whether or not to append data to the end of the specified file. If false, the output file will be overwritten. If an output file is not specified, this value will be ignored. Default Value: true
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module

Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Raise Error Task

The Raise Error task will write an error message and abort the Project when a user defined condition is met. This is useful for aborting a Project when files are not found or when other undesired results occur.

Example 1: Raise Error

In this example, if no files are found on a server (by checking the ${numberOFfiles} variable), then the task will raise an error and abort the Project.

1. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Raise Error task to the Project Outline.
2. On the Basic tab of the Raise Error task, specify the Message to write to the Job Log. If no Message is specified, the system variable "System Variables" on page 114 will be written to the Job Log.
3. On the Control tab of the Raise Error Task, specify the condition that must be met to run this task. In this case we will check if the number of files is equal to 0.
4. Click the **Save** button when finished.

Raise Error Task

The Raise Error task will write an error message and abort the Project when a user defined condition is met.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Message	Specify a custom error message. When left blank, the system variable system.job.error will be used, if it exists, to display the last error that might have occurred in the project. Otherwise, a standard message will be displayed indicating no message text was specified.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Set Variable Task

The Set Variable task can set a variable's value to static text, user-defined variables, data from a RowSet, or the contents of a file. When setting the value of a variable, either the Value or Input File attribute must be specified.

When using a RowSet variable, the Set Variable task must be inside a "For-Each Loop" on page 152. For example, specifying a Value of ${data[1]} inside a loop will set your Variable Name to the value of the current row's first column.

Example 1: Set the Value of a Variable

Follow the steps below to create a variable that contains static text:

1. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Set Variable task to the Project Outline.
2. On the Basic tab of the Set Variable task, specify values for the following attributes:

   Variable Name

   A name for this variable. The name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores(_) and periods(.).

   Value

   The new value for this variable.
3. Click the **Save** button when finished.

Example 2: Loading a Variable from a File

A variable can be loaded from a file on the local file system or network share. The Input File attribute (on the Advanced tab) should contain the path and file name . The contents of the file will be placed into the variable as 'string' data.

Note: The entire contents of the file is stored in memory. Informatica recommended to only load small files. If a large file is needed to load a variable, you should first determine whether Managed File Transfer is allocated enough memory to support it.

Follow the steps below to create a variable by reading data from a file:

1. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Set Variable task to the Project Outline.
2. On the Basic tab of the Set Variable task, specify values for the following attributes:

   Variable Name

   A name for this variable. The name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscores(_) and periods(.).
3. Select the **Advanced** tab.
4. On the Advanced tab, specify values for the following attributes:

   Input File

   Specify the path and file name of a file.
5. Click the **Save** button when finished.

Set Variable Task

The Set Variable task can set a variable's value to static text, user-defined variables, data from a RowSet, or the contents of a file.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Variable Name	Specify a name for this variable. The name must start with a letter (a-z or A-Z), and may only contain letters, digits (0-9), underscrores(_) and periods(.).
Value	Specify the new value for this variable. It can contain a combination of static text, string variables, and RowSet variables. When using a RowSet variable you must specify the column number or name. If your RowSet variable contains more than one row all other rows except for the first one will be ignored. For example: static text ${variableName} ${rowSetName[columnNumber]} ${rowSetName[columnName]}.
Advanced Tab	
Input File	Specify the path and file name of a file. The contents of the file will be placed into the variable. Since the entire contents of the file is stored in memory it is recommended to only use small file sizes. If a large file is required you should determine whether Managed File Transfer has enough memory to support it.
Encoding	Specify the file encoding. This is required if the files are using a different encoding than the platform's default. Default Value: The platform's default encoding
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module

Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Timestamp Task

Variables can be initialized to the current date, time or timestamp within a Project. These variables can then be used as attributes within tasks in Projects. Please refer to the "Dates, Times and Timestamps" on page 144 section for more information.

Timestamp Task

The Timestamp task initializes date and time variables to the current time.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Format

The Format element allows you to specify the output variable name and pattern in which the timestamp will be formatted.

Field	Definition
Basic Tab	
Output Variable	Specify the name of a variable which will contain the custom date/time. This variable will contain character date and may be used in most fields (other than fields expecting a File List or RowSet). For example, a common use for this variable would be part of an output file name (OutputFile_${timestampVar}.txt). The variable will be created if it does not exist. This timestamp value will not be available in the system variables system.currentDate, system.currentTime and system.currentTimestamp
Pattern	Specify the pattern in which this timestamp should be formatted.
Locale	Specify the locale to which the date/time data is to be formatted. The locale must be of the form [language]_[country], where language is the two character ISO language code and country is the two character ISO country code. The country part may be omitted if the data was formatted to just the specified language. Example locales are - en_US (English/United States), de (German). The default is 'en_US'.
Date Manipulation Tab	
Day of Month	Specify the value to which the day of month field of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the day of month should be rolled forward or backward by the specified amount. When nothing precedes the number, the day of month component of this timestamp is set (or made equal) to the specified number. For example, a value of 3 sets the date to 3, +3 adds 3 to the current date and -3 subtracts 3 from the current date. A special value of "L" can be used to set the date to the last day of the month.
Month	Specify the value to which the month (month of year) field of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the month should be rolled forward or backward by the specified amount. When nothing precedes the number, the month field of this timestamp is set (or made equal) to the specified number. For example, a value of 3 sets the month to 3 (march), +3 adds 3 to the current month and -3 subtracts 3 from the current month.
Year	Specify the value to which the year field of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the year should be rolled forward or backward by the specified amount. When nothing precedes the number, the year field of this timestamp is set (or made equal) to the specified number. For example, a value of 2007 sets the year to 2007, +3 adds 3 to the current year and -3 subtracts 3 from the current year.
Hour	Specify the value to which the hour (hour of day) field of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the hour field should be rolled forward or backward by the specified amount. When nothing precedes the number, the hour field of this timestamp is set (or made equal) to the specified number. For example, a value of 15 sets the hour to 3pm, +3 adds 3 to the current hour of day and -3 subtracts 3 from the current hour of day.

Minute	Specify the value to which the minute (minute of hour) field of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the minute field should be rolled forward or backward by the specified amount. When nothing precedes the number, the minute field of this timestamp is set (or made equal) to the specified number. For example, a value 0 sets the minute to 0, +3 adds 3 to the current minute of hour and -3 subtracts 3 from the current minute of hour.
Second	Specify the value to which the seconds (second of the minute) fields of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the seconds field should be rolled forward or backward by the specified amount. When nothing precedes the number, the seconds field of this timestamp is set (or made equal) to the specified number. For example, a value of 20 sets the seconds to 20, +10 adds 10 to the current seconds and -10 subtracts 10 from the current seconds.
Millisecond	Specify the value to which the milliseconds field of this timestamp is to be set, rolled forward or rolled backward. A valid value must be a whole number. The number may be prefixed with a "+" or '-' sign to indicate that the milliseconds field should be rolled forward or backward by the specified amount. When nothing precedes the number, the milliseconds component of this timestamp is set (or made equal) to the specified number. For example, a value of 0 sets the milli seconds to 0 (makes it a whole second), +500 adds 500 milliseconds to the current milliseconds -500 subtracts from the current milliseconds.
Day of Week	Specify the value to which the day of week field of this timestamp is to be set. A valid value must be in the rage of 1 through 7 where 1 means Sunday, 2 means Monday and 7 means Saturday. For example, a value of 3 sets day of week to Tuesday. This value in combination with dayOfWeekInMonth can be used to uniquely identify a day in a month (e.g. 3rd Friday of the month).
Week In Month	Specify the value to which the day of week in month field of this timestamp is to be set. A valid value must be in the range of -5 through 5. A value of 1 in this field together with a value of 3 in Day of Week field will evaluate to the 1st Tuesday of the month. Negative values in this field will count backwards from the end of the month. For example, A value of -1 in this field together with a value of 1 in the Day of Week field will evaluate to the last Sunday of the month. When a value of 0 is specified for this attribute, the week in month will be set to the last week of the previous month.

Notify Consumer Task

Managed File Transfer can send custom notifications to consumers. The Notify Consumer Task is executed only if the *deny.event.auto.notifications* variable is created and set to `True`. For more information about creating the variable, see "Creating a Variable" on page 113.

Notify Consumer Task Definitions

Use this task to notify consumers when a file is ready for use.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Source File	Browse the repository to navigate to file path or enter the sourceFileVariable.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Reports

Report tasks can be placed within Projects to run reports on an automated basis using the "Scheduling Projects" on page 187. A variety of report types are provided including audit log activity, analytics and management information. The reports are generated as PDF files, which can be distributed to recipients using email or file transfer tasks. Multiple reports can be combined into a single file using the Merge Report task.

Example 1: Create a Report

Perform the following steps to create a Blacklisted IP Addresses report:

1. From within the Project Designer page, expand the Reports folder in the Component Library, and then drag the Blacklisted IP Addresses task to the Project Outline.
2. On the Basic tab of the Blacklisted IP Addresses Report task, specify the following values:

   PDF File

   Specify the path and name of the PDF file.

   Title

   Specify a title for the report that will appear on the report header. If a title is not specified, the report will use the default title.

   Orientation

   Specify the page layout, either portrait or landscape.

   Date Range

   Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range.
3. Click the **Save** button when finished.

Example 2: Merge Reports

After two or more reports are created, the Merge Reports task can merge the reports into a single PDF file. Use the instructions in Example 1 to add more reports using the same PDF file destination directory, and then use the following instructions to merge the files:

1. From within the Project Designer page, expand the Reports folder in the Component Library, and then drag the Merge Reports task to the Project Outline.
2. On the Basic tab of the Merge Reports task, specify the following values:

   Output File

   Specify the path and name of the merged PDF file.
3. Click the **Add** button and select the File Set menu item.
4. On the Basic tab of the File Set element, specify values for the following attributes:

   Base Directory

   The directory that contains the files to merge.

   Recursive

   Specify whether or not to also merge files from all sub-folders.
5. Click the **Save** button when finished.

Report Tasks

Blacklisted IP Addresses

The Blacklisted IP Addresses report displays a list of blocked IP addresses and the date they were created.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00

To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Completed Jobs

The Completed Job report displays a list of completed Jobs, their status, and the Admin User who ran the job.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.

Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Status	Specify which statuses to get the Completed Jobs report for.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Completed Jobs Statistics

The Completed Jobs Statistics report displays the total number of Jobs processed during the specified date range.

Field	Definition
Basic Tab	

Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Group By	Specify the period that you want the job statistics to be broken down by. Default: hour
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Database Statistics

The Database Statistics report displays a list of each database table used by the Managed File Transfer system as well as the number of rows used by each table.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Expiring OpenPGP Keys

The Expiring OpenPGP Keys report displays a list of OpenPGP Keys that will be expiring within the specified date range.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: next_30_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Expiring SSL Certificates

The Expiring SSL Certificates report displays a list of SSL Certificates that will be expiring within the specified date range.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: next_30_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Global Activity Details

The Global Activity Details report displays all activity for the selected features based on the search term provided.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the date range for which to generate the report. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom.
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom.
Module	Specify which modules to include in the report.

Search Term	Specify items to search for. The Global Activity report search field uses the following wildcard searches: - Multiple character wildcard searching using "*" - A single character wildcard search for terms that match a single character replaced using "?". For example, to search for "text" or "test" you can use "te?t". Fuzzy searches using a tilde "~". A Fuzzy search finds words that are similar to the search term. For example, the search term "Proj~" will return results that contain the word "Project." - Multiple terms can be combined together with Boolean operators to form a more complex query. for example: - Searching for Project could result in 3400 hits (items contain the word Project) - Searching for Deny could result in 100 hits (items contain the word Deny) - Searching for Project and Deny results in 17 hits (results contain both words Project and Deny) - Searching for "Project Deny" (with quotes) results in 0 hits (There are no items that contain the words Project and Deny directly after each other)
User	Admin User or Web User that generated the log entries.
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Shared Drive Disk Usage

The Shared Drive Disk Usage report displays the Web Users who are permitted to use the Shared Drive feature, and their total amount of disk usage.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Job Count Summary

The Job Count Summary report displays a pie chart representation of the number of Jobs processed during the specified date range.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_30_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Merge Reports

The Merge Reports task allows you to combine multiple reports into a single PDF file.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Input Files Variable	Specify the name of a variable of type File List which contains the reports to merge. For example, ${variableName}
Output File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Secure Mail Activity

The Secure Mail Activity report displays a list of Secure Mail messages and the Web User(s) who created them, the recipient(s) of the message, the status, and the date the message was last modified.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Status	Specify which package statuses to get the Secure Mail activity report for.
Output Variables Tab	

Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Secure Mail Disk Usage

The Secure Mail Disk Usage report displays the Secure Mail disk usage for each Web User sorted by size.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Output Variables Tab	

Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Secure Mail Package Sizes

The Secure Mail Package Sizes report displays a list of Secure Mail Packages, their subject (from the Secure Mail Message) and their size.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Output Variables Tab	

Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Security Settings Audit

The Security Settings Audit report will analyze your Managed File Transfer product's security settings and determine if they comply with the Payment Card Industry Data Security Standards (PCI-DSS). For each security setting, the report will indicate if the setting meets the PCI-DSS standard using one of the following statuses:

- **Pass**

  The setting meets the PCI-DSS requirement.

- **Fail**

  The setting does not meet the PCI-DSS requirement. Recommend steps to correct the setting are provided.

- **Warning**

  Further research is required to ensure your system meets the specified requirement. Recommend steps to correct the setting are provided.

- **Not Applicable**

  A check on this setting is not required, typically due to Managed File Transfer features that you are not licensed to use.

- **Fatal**

  Indicates a configuration problem is preventing Managed File Transfer from accessing the appropriate data.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Service Activity By Module

The Service Activity by Module report displays the number of files and bytes transferred by the selected file transfer modules.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_30_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Module	Specify which modules to include in the report.
Transfer Type	Specify whether you want to see uploads, downloads or both.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false

On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Service Activity Summary

The Service Activity Summary report displays the number of uploads and downloads for the selected protocols.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_30_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Protocol	Specify which protocols to get the activity summary report for.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.

Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Service Errors

The Service Errors report displays all errors for the selected inbound services within the specified date range.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_30_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Module	Specify which modules to include in the Service Errors report.
Status	Specify which statuses to include in the Service Errors report.

Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Trigger Activity

The Trigger Activity report displays a list of executed Triggers, their status, and their associated event types.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait

Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Status	Specify which statuses to get the Trigger Activity report for.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Web User Logins

The Web User Logins report displays a list of each Web User login, the service they logged in to, and the status of the login attempt.

Field	Definition
Basic Tab	

Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Protocol	Specify which protocols to get the Login report for.
Status	Specify which statuses to get the Login report for.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Web User Transfer Count Activity

The Web User Transfer Count Activity report displays the number of file transfers per Web User.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Module	Specify which modules to include in the report.
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Transfer Type	Specify whether you want to see uploads, downloads or both.
Output Variables Tab	
Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.

Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Web User Transfer Size Activity

The Web User Transfer Size Activity report displays the total size of transferred files by Web User.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
PDF File	Specify the path and name of the PDF file.
When File Exists	Specify the action to take when the output file already exists. The default value is 'rename' which changes the output file name to a new name so the existing file remains untouched. Default Value: rename
Title	Specify an optional title to use instead of the default report title.
Orientation	Specify the page layout, either portrait or landscape. Default: portrait
Date Range	Specify the scope of your report, in days. You can select 'custom' to use the From Date and To Date fields to specify a custom date range. Default: last_7_days
From Date	Specify the date time you wish to start the report. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
To Date	Specify the date time you wish to run the report to. Only used if Date Range is custom. Date Format: YYYY-MM-DD or YYYY-MM-DD 00:00:00
Module	Specify which modules to include in the report.
Number of Rows	Specify the number of rows to include in the report. A value of 0 means that there is no limit. Default: 0
Transfer Type	Specify whether you want to see uploads, downloads or both.
Output Variables Tab	

Output File Variable	If desired, specify the name of a variable which will contain the PDF file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Web Tasks

Web tasks perform get and post functions to transfer data using the AS2, HTTP, HTTPS, Informatica HTTPS, and ICAP servers.

AS2 Task

The AS2 task is used to send (POST) messages using the AS2 1.2 specification. Messages sent using AS2 are typically structured data files like XML and EDI documents, but the transmission protocol can be used for all file types. AS2 Task can compress, sign, and encrypt messages before sending them over an SSL tunnel. The AS2 Task can also process Message Disposition Notifications (*MDN* receipts) to ensure the message was received. Asynchronous MDN receipts can be sent to an email address or url.

The AS2 task in Managed File Transfer supports the *EDIINT* header information defined in AS2 version 1.2. File attachments in the AS2 task can be single file, a source variable and/or a File Set. The AS2 task also supports the use of "AS2 Task Output" on page 124.

For more information, refer to the "Quick Start for AS2" on page 716.

Example 1: AS2 Task

Follow the steps below to select a single file and send (post) the file to an AS2 server. This example task sends the daily EDI formatted "2904 Report" to a defined AS2 resource and writes the signed message receipt to the Job log:

1. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the AS2 task to the Project Outline.
2. On the Basic tab of the AS2 task, specify values for the following attributes:

   Label

   A name to identify the Task in the Project Outline

   AS2 Server

   A pre-configured "AS2 Servers Resource" on page 72 from the drop-down list

   Source File

   Type the "File Paths" on page 161 and file name for the file or click the  icon to browse for the file

   Content Type

   Select a Content Type from the drop-down list

   Subject

   A subject name to identify the message
3. On the Receipt tab of the AS2 task, specify values for the following attributes:

   Request Receipt

   Select what type of receipt to receive from the drop-down list

   Destination

   Select the joblog option to write the receipt information to the Job log
4. Click the **Save** button.

AS2 Task

Send (POST) messages to an AS2 server using an AS2 task.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
AS2 Server	Select a pre configured AS2 server from the list.
Source File	Specify the path and file name of a single file to send. Enter a file name, it might not be a directory name.
Source Files Variable	Specify the name of a variable of type File List which contains the files to send to the AS2 server. For example, ${variableName}.

Content Type	Specify the content type of the source file(s) from the list or type in any valid MIME content type. Default Value: application/EDI-Consent
Subject	Specify the subject of the message.
Receipt Tab	
Request Receipt	Specify whether or not to request a receipt from the AS2 server. Default Value: none
Destination	Specify where to save the receipt. Valid options are: - File. The synchronous receipt is saved to the file specified in 'Receipt File' attribute. - Email. The asynchronous receipt is sent to the email address specified in the 'Receipt Email' attribute. Please verify with the AS2 Server that this option is supported. - URL. The asynchronous receipt is sent to the URL specified in the 'Receipt URL' attribute. You can specify 'https://[hostname]:[portnumber]/as2/mdn' as the url and the MDN receipts will appear in the Managed File Transfer AS2 audit log. - *[hostname]* is the host name or IP address of the Managed File Transfer server - *[portnumber]* is the port number of the File Transfer Portal. The default port is 443. If you are sending the MDN receipt to another server, verify the URL option is supported on the other AS2 server. **Discard. The receipt is discarded.**
File	Specify the location of the file to which the receipt, if any, should be saved. This is required if the 'Receipt Destination' is set to 'file'.
When File Exists	Specify the action to take when the receipt file already exists. Default Value: rename
Email Address	Specify the email address to which the receipt, if any, should be sent to. This is required and used only if the 'Receipt Destination' is set to 'email'.
Receipt URL	Specify the URL to which the receipt, if any, should be sent to. This is required and used only if the 'Receipt Destination' is set to 'url'.
Output Variables Tab	

Output Variable	If desired, specify the name of a variable which will contain an AS2TaskOutput variable. It will be created if it does not exist, or overwritten otherwise.
AS2 Server Tab	
Refer to the "AS2 Servers Resource" on page 72 page for the AS2 Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

AS2 Request Header

You can add the field-value pairs to the AS2 request header.

Field	Definition
Basic Tab	
Name	Specify the name of the header to include in the request. This is any standard AS2 header or a custom header that is specific to the AS2 server.
Value	Specify the value.

Informatica HTTPS Task

Managed File Transfer is packaged with an "Service Manager" on page 516 that allows "Web User Management" on page 589 to login to it from any web browser. Once logged in, that user can upload, download, copy, rename, and delete files from within their home directory. The Managed File Transfer HTTPS Task can perform these same functions from within your Project. Although you can specify the connection information on a per task basis, it is always recommended to create a "Informatica HTTPS Server Resource" on page 96.

Most Web User functions can be executed from within Managed File Transfer using the Informatica HTTPS task. Along with uploading and downloading files from a Managed File Transfer Web User account, the Informatica HTTPS Task can send Secure Mail packages to email recipients using the Send Package element. The Send Package element allows you to specify which files will be placed on a secure Managed File Transfer server for download by an authorized recipient. The process sends the recipient an email containing a link they use to securely access the files.

Checksum verification can be added to ensure that the source file is exactly the same as the destination file after a transfer completes successfully. This option is available on the Transfer Options tab in the Upload, Download, and Upload Raw Data elements. SHA1, CRC32 and MD5 algorithms are supported with the default and recommended algorithm being SHA1. If the calculated checksum values do not match, an error is written to the job log.

Example 1: Upload a File Using Informatica HTTPS

Follow the steps below to upload a file to a Managed File Transfer server using the Informatica HTTPS task:

1. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the Informatica HTTPS task to the Project Outline.
2. On the Basic tab of the Managed File Transfer HTTPS task, specify the Informatica HTTPS Server value:

   Informatica HTTPS Server

   A pre-defined "Informatica HTTPS Server Resource" on page 96.
3. Click the **Add** button in the sub-menu and from the drop-down menu, click **Upload Files**.
4. On the Basic tab of the Upload Files element, specify values for the following attributes:

   Source File

   The "File Paths" on page 161 and file name of a single file to upload.

   Destination File

   The destination file.
5. Click the **Save** button when finished.

Example 2: Send a Package Using Informatica Managed File Transfer HTTPS

The Send Package element connects to Managed File Transfer for securely sharing files with designated recipient(s) of the message. Files are sent to the Managed File Transfer server and then an email is sent to the recipient(s) allowing them to download the files and view the secure message. Each recipient receives a unique link to the package. The link is comprised of a 36-character UUID string.

The Send Package element allows placing multiple files in a package through the use of a "File Lists and File Sets" on page 116 sub-element. The maximum size of the files is governed by settings on the Managed File Transfer server.

The Send Package element provides several settings for Packages. These settings can limit the number of times each file can be downloaded per recipient, package expiration, password protection options and purging options.

Follow the steps below to send a Package from a Managed File Transfer server using the Managed File Transfer HTTPS task:

1. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the Informatica HTTPS task to the Project Outline.
2. On the Basic tab of the Managed File Transfer HTTPS task, specify the Informatica HTTPS Server value:

   Informatica HTTPS Server

   A pre-defined "Informatica HTTPS Server Resource" on page 96.
3. Click the **Add** button in the sub-menu and from the drop-down menu, click **Send Package**.
4. On the Basic tab of the Send Package element, specify values for the following attributes:

   To

   Specify the email addresses of the recipients. Multiple email addresses should be separated by a comma.

   Subject

   Specify the subject of the message.

   Source file

   Specify the path and file name of a single file to attach. A file name is required, it may not be a directory name only.
5. Click the Advanced Tab. On the Advanced tab, specify values for the following attributes:

   Expire Package After Days

   Specify the number of days after which the package will automatically expire. For no expiration, leave this field blank.

   Maximum Downloads

   Specify the number of times each recipient can download each file attached to the package. For unlimited downloads, leave this field blank.

   Reply Allowed

   Specify whether or not to allow replies. This setting only applies to URL Protected and Password Protected packages. If true, and allowed by the server, the recipient will be allowed to reply to this Secure Mail message.

   Send me A Copy

   Specify whether the Web User that sends this package should receive an email for this package.

   Read Receipt

   Specify whether the Web User that sends this package should receive an email notification the first time each recipient views the package.
6. Click the Package Security tab. On the Package Security tab, specify the following attributes:

   Protection Level

   Specify whether this package will be protected by a unique URL, with a password, or requires a certified registered user.
7. Click the **Save** button when finished.

Informatica HTTPS Task

The Informatica HTTPS task allows you to send and receive files to an Managed File Transfer HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
Informatica HTTPS Server	Select a pre-configured Informatica HTTPS Server from the drop-down list.
Informatica HTTPS Server Tab	
Refer to the "Informatica HTTPS Server Resource" on page 96 page for the Managed File Transfer HTTP Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Send Package

The Send Package element allows you to send Secure Mail Packages using a Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
To	Specify the email addresses of the recipients. Multiple email addresses should be separated by a comma.
Subject	Specify the subject of the message.

Message	Specify the message body text.
Source File	Specify the path and file name of a single file to attach. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to attach to the package. For example, ${variableName}.
Advanced Tab	
Expire Package After Days	Specify the number of days after which the package will automatically expire. For no expiration, leave this field blank. Default Value: Secure Mail server default
Maximum Downloads	Specify the number of times each recipient can download each file attached to the package. For unlimited downloads, leave this field blank. Default Value: Secure Mail server default
Reply Allowed	Specify whether or not to allow replies. This setting only applies to URL Protected and Password Protected packages. If true, and allowed by the server, the recipient will be allowed to reply to this Secure Mail message. Default Value: Secure Mail server default
Send Me A Copy	Specify whether the Web User that sends this package should receive an email for this package. Default Value: false
Read Receipt	Specify whether the Web User that sends this package should receive an email notification the first time each recipient views the package. Default Value: false
Package Security	
Protection Level	Specify whether this package will be protected by a unique URL, with a password, or requires a certified registered user. Default Value: Secure Mail server default
Password Generation	If the package is Password Protected, specify whether the password should be generated automatically or specified manually. Default Value: Secure Mail server default
Password	Specify a Password if the package is Password Protected and the Password Generation above is set to Manual.
Is Password Encrypted?	Specify if the password is encrypted. Default Value: false
Include Password in Email	Specify whether to include the specified or generated password in the email that is sent to the recipient. Default Value: Secure Mail server default
Output Variables Tab	

Number of Files Attacked Variable	If desired, specify the name of a variable which will contain the number of files attached to the package. The variable may be used in subsequent tasks and will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were successfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Message

The Message element allows you to add a message to your Secure Package.

Field	Definition
Basic Tab	
Text	Specify the body text of this email message

Download Files

The Download Files element allows you to download files from an Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to download. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type Remote File List which contains the files to retrieve from the remote server. For example, ${variableName}.
Destination File	Specify the destination file when downloading a single file. This value is only used when downloading only a single file. Specifying this attribute when downloading multiple files will result in a compilation error.
Destination Directory	Specify where on the local system the files should be downloaded. If the specified directory does not exist, it will be created.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.

Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Depending on the algorithm you choose, the appropriate request will be sent to the Informatica HTTPS Server to calculate the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: SHA1
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the successfully downloaded files on the local system. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.
Number of Files Downloaded Variable	If desired, specify the name of a variable which will contain the number of files downloaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully downloaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.

Upload Files

The Upload Files element allows you to upload files an Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Destination File	Specify the destination file. This is valid only when uploading a single file.
Destination Directory	Specify the directory on the remote system to which the files should be uploaded. The directory may be an absolute path or relative to the current working directory.
When File Exists	Specify the action to take when a destination file already exists. The default value is 'rename' which changes the destination file name to a new name so the existing file remains untouched. Default Value: rename
Transfer Options Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.

File Name Suffix	Specify a string to attach to the end of the destination file names.
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Depending on the algorithm you choose, the appropriate request will be sent to the Informatica HTTPS Server to calculate the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: SHA1
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Upload Raw Data

The Upload Raw Data element allows you to upload raw data to the Informatica HTTPS Server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to upload. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type File List which contains the files to upload to the remote server. For example, ${variableName}.
Transfer Options Tab	
Verify Checksum	Specify whether or not to enable checksum verification. Checksum verification ensures that the source file is exactly the same as the destination file after a successful transfer. Default Value: false
Checksum Algorithm	Specify the algorithm to use for checksum verification. Depending on the algorithm you choose, the appropriate request will be sent to the Informatica HTTPS Server to calculate the checksum. The same algorithm will be used for calculating the checksum of local files. Default Value: SHA1

Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files on the remote system that were successfully uploaded. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Uploaded Variable	If desired, specify the name of a variable which will contain the number of files uploaded. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Processed Source Files Variable	If desired, specify the name of a variable which will contain the files on the local system that were succesfully uploaded. This variable will be of type File List and may be used in subsequent tasks that accept a File List input variable. The variable will be created if it does not exist.

Change Directory

The Change Directory element changes the present directory on the Informatica HTTPS Server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Working Directory	Specify a directory to set as the new working directory. The path may be absolute or relative to the current working directory. The special value ".." may be used to set the working directory to the parent of the current working directory.

Create Directory

The Create Directory element creates a new directory on the Informatica HTTPS Server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Directory	Specify the directory to create. The directory path may be specified as absolute or relative to the current working directory. All non-existent directories specified in this path will be created.

Rename Files

The Rename Directory element renames a directory on the Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.

From	Specify the path and name of the file or directory to be renamed. The path may be specified as absolute or relative to the current working directory.
To	Specify the new path and name. The path may be specified as absolute or relative to the current working directory. This attribute is only valid if a single file is being renamed.
Advanced Tab	
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to rename on the remote server. For example, ${variableName}.
File Name Prefix	Specify the string to prepend to the name of the file(s) being renamed.
File Name Suffix	Specify the string to append to the name of the file(s) being renamed.
Search Pattern	Specify a pattern to search and replace in the file name(s). Both regular expressions and wildcard search patterns can be used and can be changed using the Pattern Type attribute.
Pattern Type	Specify the type of pattern to use when using search and replace on the file names. Default Value: wildcard
Replace With	Specify the pattern to replace in the file names. If using regular expressions and groups of the file names were captured, use the syntax $1, $2, etc... to reuse the captured segments. If using wildcard search and replace, use character * and ? to reuse the values the * and ? represented in the search for value.
Case Sensitive	Specify whether or not to use case sensitive matching when searching and replacing sections of the file names. Default Value: false
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files in the destination directory on the remote system that were successfully renamed. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Renamed Variable	If desired, specify the name of a variable which will contain the number of files successfully renamed. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Delete Files

The Delete Files element removes (deletes) files from the Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File	Specify the path and name of a single file to delete. The path may be specified as absolute or relative to the current working directory.

Directory	Specify the path and name of a single directory to delete. WARNING: The directory and everything in it will be deleted.
Input Files Variable	Specify the name of a variable of type Remote File List which contains the files to delete from the remote server. For example, ${variableName}.

Move Files

The Move Files element moves a file from one directory on the Informatica HTTPS Server to another directory on the Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
Source File	Specify the path and file name of a single file to move. A file name is required, it may not be a directory name only.
Source Files Variable	Specify the name of a variable of type Remote File List which contains the files to move on the remote server. For example, ${variableName}.
Destination File	Specify the path and file name to which the source file is to be moved. This is valid only when moving a single file.
Destination Directory	Specify the directory to which the files should be moved. The directory may be an absolute path or relative to the current working directory.
Advanced Tab	
File Name Prefix	Specify a string to attach to the beginning of the destination file names.
File Name Suffix	Specify a string to attach to the end of the destination file names.
Output Variables Tab	
Destination Files Variable	If desired, specify the name of a variable which will contain the files in the destination directory on the remote system that were successfully moved. This variable will be of type Remote File List and may be used in subsequent tasks that accept a Remote File List input variable. The variable will be created if it does not exist.
Number of Files Moved Variable	If desired, specify the name of a variable which will contain the number of files successfully moved. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

List Files

The List Files element creates a variable of type File List which contains a list of files on the Informatica HTTPS server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
File List Variable	If desired, specify the name of a variable that will contain the list of files being created. This will be a variable type of File List. If this variable exists it will be overwritten, otherwise it will be created.
Number of Files Found Variable	If desired, specify the name of a variable which will contain the number of files found. The variable may be used in subsequent tasks. The variable will be created if it does not exist.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

HTTP Task

The Hyper Text Transfer Protocol (*HTTP*) can be used to get or post data to a web server. By performing multiple get or post commands, the HTTP task can simulate an interactive user working from within their web browser. Although the range of possible uses will vary, a common HTTP task will perform a post command with user name and password parameters to log into a site. After the user is successfully logged in, it could then get or post data to the web server.

SOCKS, HTTP, and Informatica Managed File Transfer Proxy

Managed File Transfer connects to a proxy server as a client and the proxy server redirects the traffic to the target HTTP server. Proxy settings for HTTP connections are defined at the "HTTP Servers Resource" on page 81 level or per HTTP Task. The HTTP Task can use SOCKS, HTTP, or Managed File Transfer proxy protocols when making a connection to a proxy server. The SOCKS connection in Managed File Transfer supports both version 4 and 5. The HTTP proxy, otherwise known as an HTTP tunneling proxy, provides an HTTP tunnel through which a transport can be established. When using a proxy server, obtain the correct proxy type and connection credentials from the proxy server administrator.

Example 1: HTTP Post and Get

Follow the steps below to log into a site, post a file, and issue a get command to retrieve a file on a web server. This example assumes the file would only be accessible if the login is successful:

1. To start the Post example, from within the Project Designer page, expand the Web folder in the Component Library, and then drag the HTTP task to the Project Outline.
2. On the Basic tab of the HTTP task, specify the "HTTP Servers Resource" on page 81 value:
3. Click the **Add** button in the sub-menu and select the **Add a Post Method** menu item.
4. On the Basic tab of the Post Method element, specify the URI value:

URI

the URI (Uniform Resource Identifier), also known as *URL* (Uniform Resource Locator), (for example, /data/orders.xls). If left blank, the default URI of the server is requested.

Content Type

Specify the value to send in the Content-Type header field when making the request. When you post files (with or with out parameters) then the content type is set to 'multipart/mixed'.

5. Click the **Add** button in the sub-menu and select the **Add a Request Parameter** menu item.
6. On the Basic tab of the Request Parameter element, specify values for the following attributes:

   Name

   The name for this parameter.

   Value

   The value for this parameter.

7. Click the **Add** button in the sub-menu and select the Add Same menu item.
8. On the Basic tab of the Request Parameter element, specify values for the following attributes:

   Name

   The name for this parameter.

   Value

   The value for this parameter.

9. Select the Post element from the Project Outline. Click the **Add** button in the sub-menu and select the Add a File menu item.
10. On the Basic tab of the Add a File element, specify values for the following attributes:

    Name

    Specify the parameter (or part) name for this file name. The specified name will be sent to the server as a header in the Multi-Part data.

    Path

    Specify the location of the file to upload.

11. For the Get example, in the **Project Outline** window on the left side of the page right-click the **HTTP** task and select the **Add a Get Method** from the drop-down menu.
12. On the Basic tab of the Get Method element, specify the URI values:

    URI

    the URI (Uniform Resource Identifier), also known as *URL* (Uniform Resource Locator), (for example, /documents/data.txt). If left blank, the default URI of the server is requested (for example, www.example.com).

13. On the Response Body tab of the Get Method element, specify the Destination value:

    Destination

    Where the response body, if any, should be saved. By default, the response body will be saved to the job log.

14. On the Response Headers tab of the Get Method element, specify the File value:

Response Body File

The location of the file to which the response body, if any, should be saved. This is required if the **Response Body Destination** attribute is set to 'file'.

15. Click the **Save** button when finished.

Example 2: HTTP Web Service SOAP Request

Managed File Transfer has the ability to create Web Service SOAP messages by using the "Write XML Task" on page 318 and HTTP(S) Tasks. The Write XML task will be used to create a SOAP XML file with standard SOAP name spaces, Envelope, and Body elements. The HTTP task will use the Post Raw Data element to pass the SOAP XML file into the HTTP request. The HTTP task will then write the SOAP Response Body to an XML file.

Follow the steps below create an HTTP SOAP Request:

1. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Create Workspace task to the Project Outline.
2. From within the Project Designer page, expand the Data Translation folder in the Component Library, and then drag the Write XML task to the Project Outline.
3. On the Basic Tab of the Write XML task, specify an Output File name. The file will be temporarily stored in the Workspace created in step 3.
4. Use the "Write XML Task" on page 318 task to add the XML Elements and Attributes for the SOAP request to the Project.
5. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the HTTP task to the Project Outline.
6. On the Basic tab of the HTTP task, specify the "HTTP Servers Resource" on page 81 value:
7. Click the **Add** button in the sub-menu and choose the **Add a Post Raw Data** menu item.
8. On the Basic tab of the Post Raw Data Method element, specify the following values:

   URI

   Specify the URI (Uniform Resource Identifier), also known as URL (Uniform Resource Locator)

   Input File

   Specify the file that contains the data to be posted.

   Content Type

   Specify the value to send in the Content-Type header field when making the request.
9. On the Response Body tab, specify the following values:

   Destination

   Specify if and where the response body, if any, should be saved.

   File

   Specify the location of the file to which the response body, if any, should be saved. This is required if the 'Response Body Destination' is set to 'file'.

   When File Exists

   Specify the action to take when the response file already exists.

10. From within the Project Designer page, expand the Miscellaneous folder in the Component Library, and then drag the Delete Workspace task to the Project Outline.
11. Click the **Save** button when finished.

HTTP Task

The HTTP task can be used to get or post data to a web server.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
HTTP Server	Select a pre-configured HTTP server from the drop-down list.
Advanced Tab	
Follow Redirects	Specify whether or not to follow redirects. Default Value: true
Enable Cookies	Specify whether or not to enable cookies. Default Value: true
User Agent	Specify a custom value for the User-Agent request header. Default Value: Managed File Transfer/${currentProductVersion}
HTTP Server Tab	
Refer to the "HTTP Servers Resource" on page 81 page for the Mail Box Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Get Method

The Get Method element allows you to download files from an HTTP server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
URI	Specify the URI (Uniform Resource Identifier), also known as URL (Uniform Resource Locator), e.g., '/data/orders.xls' or '/cgi-bin/upload.cgi'. If left blank, the default URI of the server is requested. e.g., www.domainname.com.
Advanced Tab	
Follow Redirects	Specify whether or not to follow redirects. The default value is true. Default Value: Inherited from the task
Read Timeout	Specify the maximum amount of time, in seconds, to wait when waiting for a response from the server. A value of 0 (zero) is interpreted as infinite timeout. This defaults to the value specified on the HTTP task.
Validate Status Code	If true (default), the HTTP status code will be validated and any code not in the 200-299 range will cause the project to fail. If false, the HTTP status code will not be validated and will not cause the project to fail. This allows the response to be accessed later in the project. NOTE: By definition the status codes 204 and 304 do not contain a message body and are therefore do not apply to this setting.
If Modified Since	Specify the value to send in the 'If-Modified-Since' header when making the request. The HTTP server will look at this header and sends the response body if and only if the requesting URI was modified after the specified date. The value must be a date and may include a time also. The value must be entered in yyyy-MM-dd or yyyy-MM-dd HH:mm:ss format.
Response Body Tab	
Destination	Specify if and where the response body, if any, should be saved. By default, the response body will be saved to the job log.
File	Specify the location of the file to which the response body, if any, should be saved. This is required if the 'Response Body Destination' is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Response Headers Tab	
Destination	Specify if and where the response headers should be saved. By default, the response headers will be discarded.
File	Specify the location of the file to which the response headers should be saved. This is required if the 'Response Headers Destination' attribute is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Output Variables Tab	

Status Code Variable	If desired, specify the name of a variable which will contain the HTTP status code returned by the server. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Status Message Variable	If desired, specify the name of a variable which will contain the status message returned by HTTP server. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Response Body File Variable	If desired, specify the name of a variable which will contain the response body output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Response Headers File Variable	If desired, specify the name of a variable which will contain the headers file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.

Request Parameter

The Request Parameter element allows you to define query field-value pairs in your HTTP request.

Field	Definition
Basic Tab	
Name	Specify the name for this parameter.
Value	Specify the value for this parameter.
Advanced Tab	
Content Type	Specify the value of the Content-Type header that will be written to this parameter part of the MIME message. This setting will be ignored if the request is not multipart.
Content Disposition	Specify the value of the Content-Disposition header that will be written to this parameter part of the MIME message. This setting will be ignored if the request is not multipart. Default Value: form-data
Content ID	Specify the value of the Content-ID header that will be written to this parameter part of the MIME message. This is required if the Content Type of the post element is 'multipart/related', otherwise this is ignored.
Transfer Encoding	Specify the value of the Content-Transfer-Encoding header that will be written to this parameter part of the MIME message. This setting will be ignored if the request is not multipart.
Charset	Specify the charset that will be added to the Content-Type header of this parameter part of the MIME message. This setting will be ignored if the request is not multipart. Default Value: UTF-8

Request Header

The Request Header element allows you to add field-value pairs to the HTTP Request header.

Field	Definition
Basic Tab	
Name	Specify the name of the header you would like to include in the request. This could be any standard HTTP header or a custom header that is specific to the HTTP server.
Value	Specify the value for this header field.

Post Method

The Post Method element allows you to upload a file to a web server.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
URI	Specify the URI (Uniform Resource Identifier), also known as URL (Uniform Resource Locator), for e.g., '/data/orders.xls' or '/cgi-bin/upload.cgi'. If left blank, the default URI of the server is requested. For e.g., www.domainname.com.
Input Files Variable	Specify a file list to post to the HTTP server. The value must be a reference to a variable whose value is a file, file list or a collection of file lists.
File Field Name	Specify the parameter name (or part name) to set for the files being posted, if any.
Content Type	Specify the value to send in the Content-Type header field when making the request. The default value depends on the information being posted. If you are posting just parameters, then the content-type defaults to 'application/x-www-form-urlencoded'. If you are posting files (with or with out parameters) then the content type is set to 'multipart/mixed'.
Advanced Tab	
Follow Redirects	Specify whether or not to follow redirects. The default value is true. Default Value: Inherited from the task
Read Timeout	Specify the maximum amount of time, in seconds, to wait when waiting for a response from the server. A value of 0 (zero) is interpreted as infinite timeout. This defaults to the value specified on the HTTP task.
Validate Status Code	If true (default), the HTTP status code will be validated and any code not in the 200-299 range will cause the project to fail. If false, the HTTP status code will not be validated and will not cause the project to fail. This allows the response to be accessed later in the project. NOTE: By definition the status codes 204 and 304 do not contain a message body and are therefore do not apply to this setting.
Start Content ID	Specify the starting content ID of a 'multipart/related' MIME package. This is required if the Content Type of this post element is 'multipart/related', otherwise this is ignored.

Response Body Tab	
Destination	Specify if and where the response body, if any, should be saved. By default, the response body will be saved to the job log.
File	Specify the location of the file to which the response body, if any, should be saved. This is required if the 'Response Body Destination' is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Response Headers Tab	
Destination	Specify if and where the response headers should be saved. By default, the response headers will be discarded.
File	Specify the location of the file to which the response headers should be saved. This is required if the 'Response Headers Destination' attribute is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Output Variables Tab	
Status Code Variable	If desired, specify the name of a variable which will contain the HTTP status code returned by the server. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Status Message Variable	If desired, specify the name of a variable which will contain the status message returned by HTTP server. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Response Body File Variable	If desired, specify the name of a variable which will contain the response body output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Response Headers File Variable	If desired, specify the name of a variable which will contain the headers file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.

File

The File element allows you to add a file to your HTTP Post request.

Field	Definition
Basic Tab	
Name	Specify the parameter (or part) name for this file name. The specified name will be sent to the server as a header in the Multi-Part data.
Path	Specify the location of the file to upload.
Advanced Tab	

Content Type	Specify the value of the Content-Type header that will be written to this file part of the MIME message. This setting will be ignored if the request is not multipart.
Content Disposition	Specify the value of the Content-Disposition header that will be written to this file part of the MIME message. This setting will be ignored if the request is not multipart. Default Value: form-data
Content ID	Specify the value of the Content-ID header that will be written to this file part of the MIME message. This is required if the Content Type of the post element is 'multipart/related', otherwise this is ignored.
Transfer Encoding	Specify the value of the Content-Transfer-Encoding header that will be written to this file part of the MIME message. This setting will be ignored if the request is not multipart.
Charset	Specify the charset that will be added to the Content-Type header of this file part of the MIME message. This setting will be ignored if the request is not multipart.

Note: This task uses the File Set Elements. The field definitions for the File Set Elements can be found on the "File Lists and File Sets" on page 116 topic.

Post Raw Data Method

The Post Raw Data element allows you to post the contents of a file to a HTTP request.

Field	Definition
Basic Tab	
Label	Specify a label for this action.
URI	Specify the URI (Uniform Resource Identifier), also known as URL (Uniform Resource Locator), for e.g., '/data/orders.xls' or '/cgi-bin/upload.cgi'. If left blank, the default URI of the server is requested. For e.g., www.domainname.com.
Input File	Specify the file that contains the data to be posted.
Content Type	Specify the value to send in the Content-Type header field when making the request. Default Value: text/xml
Advanced Tab	
Follow Redirects	Specify whether or not to follow redirects. The default value is true. Default Value: Inherited from the task
Read Timeout	Specify the maximum amount of time, in seconds, to wait when waiting for a response from the server. A value of 0 (zero) is interpreted as infinite timeout. This defaults to the value specified on the HTTP task.
Validate Status Code	If true (default), the HTTP status code will be validated and any code not in the 200-299 range will cause the project to fail. If false, the HTTP status code will not be validated and will not cause the project to fail. This allows the response to be accessed later in the project. NOTE: By definition the status codes 204 and 304 do not contain a message body and are therefore do not apply to this setting.

Response Body Tab	
Destination	Specify if and where the response body, if any, should be saved. By default, the response body will be saved to the job log.
File	Specify the location of the file to which the response body, if any, should be saved. This is required if the 'Response Body Destination' is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Response Headers Tab	
Destination	Specify if and where the response headers should be saved. By default, the response headers will be discarded.
File	Specify the location of the file to which the response headers should be saved. This is required if the 'Response Headers Destination' attribute is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Output Variables Tab	
Status Code Variable	If desired, specify the name of a variable which will contain the HTTP status code returned by the server. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Status Message Variable	If desired, specify the name of a variable which will contain the status message returned by HTTP server. The variable may be used in subsequent tasks. The variable will be created if it does not exist.
Response Body File Variable	If desired, specify the name of a variable which will contain the response body output file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.
Response Headers File Variable	If desired, specify the name of a variable which will contain the headers file. The variable will be of type File and may be used in subsequent tasks that accept File or File List input variables. The variable will be created if it does not exist.

Post Raw Data Method - Request Header

The Post Raw Data Method - Request Header allows you to add headers to your HTTP request.

Field	Definition
Basic Tab	
Name	Specify the name of the header you would like to include in the request. This could be any standard HTTP header or a custom header that is specific to the HTTP server.
Value	Specify the value for this header field.

HTTPS Task

The HTTPS task is very similar to the HTTP task except that it establishes a secure *SSL* connection to the "HTTPS Servers Resource" on page 83. Please refer to the "HTTP Task" on page 502 documentation for more information.

ICAP Task

The *ICAP* task is used to send files to an ICAP-enabled server which can perform Anti-Virus and DLP (Data Loss Prevention) functions. For each file, the ICAP-enabled server will return a status code to Managed File Transfer to indicate if the file contents have "passed" its criteria.

For example, before a file is sent to a trading partner, you could use the ICAP task to send the file to a DLP server to check the file's contents for sensitive data. If the DLP server returns a positive status code, then you could send the file to the trading partner. Otherwise, if the response is a failure, then the Project could be stopped from allowing the file to leave the organization.

ICAP Status Response Codes

The following list contains the status codes that are returned from the ICAP server:

- 100 - Continue after ICAP preview. ICAP requests sent by Managed File Transfer include a preview of the transaction. The ICAP server will respond with code 100 to continue the scan.
- 200 - 201 - The ICAP server modified the content of the request. A modified response indicates the ICAP server found restricted content, and the Managed File Transfer Project will fail.
- 204 - No modifications needed. The ICAP server has scanned the file and did not find restricted content.
- 4xx - Client error codes. The client (Managed File Transfer) cannot reach the ICAP server.
- 5xx - Server error codes. An error exists on the ICAP server, such as out of disk space or the ICAP version is not supported by the server.

Example 1: DLP Scan Example

Follow the steps below to scan a single file using an "ICAP Resource" on page 87:

1. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the ICAP task to the Project Outline.
2. On the Basic tab of the ICAP task, specify the following fields:

   ICAP Server

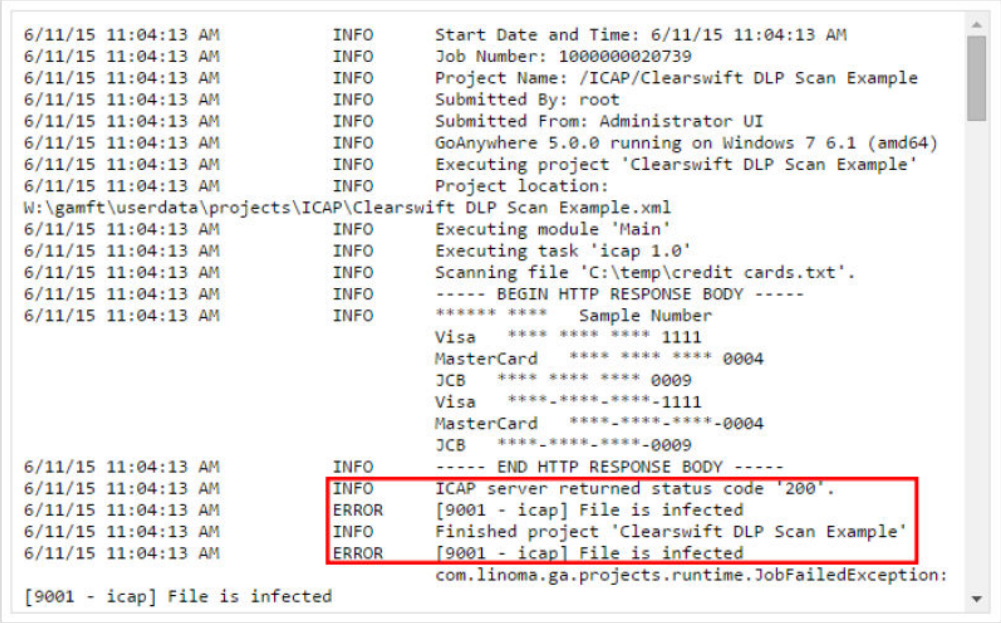
   A pre-configured ICAP server from the drop-down list.

   Source File

   Specify the path and file name of a single file to send. A file name is required, it may not be a directory name only.

3. Click the **Save** button when finished.

   When the Project executes, the Job Log will contain the HTTP Response Body from the DLP server that includes the status code. In this example, the "Credit Cards.txt" file contains sensitive data and the Project failed when the error code was returned . In this example, the DLP server was configured to redact text which removed the sensitive information and replaced them with asterisks. The redacted version was returned in the encapsulated HTTP response body and can be saved to the job log or a file.



```
6/11/15 11:04:13 AM          INFO      Start Date and Time: 6/11/15 11:04:13 AM
6/11/15 11:04:13 AM          INFO      Job Number: 1000000020739
6/11/15 11:04:13 AM          INFO      Project Name: /ICAP/Clearswift DLP Scan Example
6/11/15 11:04:13 AM          INFO      Submitted By: root
6/11/15 11:04:13 AM          INFO      Submitted From: Administrator UI
6/11/15 11:04:13 AM          INFO      GoAnywhere 5.0.0 running on Windows 7 6.1 (amd64)
6/11/15 11:04:13 AM          INFO      Executing project 'Clearswift DLP Scan Example'
6/11/15 11:04:13 AM          INFO      Project location:
W:\gamft\userdata\projects\ICAP\Clearswift DLP Scan Example.xml
6/11/15 11:04:13 AM          INFO      Executing module 'Main'
6/11/15 11:04:13 AM          INFO      Executing task 'icap 1.0'
6/11/15 11:04:13 AM          INFO      Scanning file 'C:\temp\credit cards.txt'.
6/11/15 11:04:13 AM          INFO      ----- BEGIN HTTP RESPONSE BODY -----
6/11/15 11:04:13 AM          INFO      ****** ****   Sample Number
                                       Visa   **** **** **** 1111
                                       MasterCard   **** **** **** 0004
                                       JCB   **** **** **** 0009
                                       Visa   ****-****-****-1111
                                       MasterCard   ****-****-****-0004
                                       JCB   ****-****-****-0009
6/11/15 11:04:13 AM          INFO      ----- END HTTP RESPONSE BODY -----
6/11/15 11:04:13 AM          INFO      ICAP server returned status code '200'.
6/11/15 11:04:13 AM          ERROR     [9001 - icap] File is infected
6/11/15 11:04:13 AM          INFO      Finished project 'Clearswift DLP Scan Example'
6/11/15 11:04:13 AM          ERROR     [9001 - icap] File is infected
                                       com.linoma.ga.projects.runtime.JobFailedException:
[9001 - icap] File is infected
```

Example 2: Scan Multiple Files Using an ICAP Resource

Follow the steps below to scan multiple files using an "ICAP Resource" on page 87:

1. From within the Project Designer page, expand the File System folder in the Component Library, and then drag the Create File List task to the Project Outline.
2. On the Create File List page, specify the File List Variable.
3. Click the **Add** button in the page toolbar and select the File Set menu item.
4. In the File Set page, type the complete directory path to the Base Directory that contains the files or click the icon to browse for the directory.
5. From within the Project Designer page, expand the Loops folder in the Component Library, and then drag the For-Each Loop task to the Project Outline.
6. Specify the Items Variable and the Current Item Variable for the For-Each Loop.
7. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the ICAP task to the Project Outline.
8. On the Basic tab of the ICAP task, specify the following fields:

   ICAP Server

   A pre-configured ICAP server from the drop-down list.

Source File

Specify the current file variable created in step 6.

9. Click the **Save** button when finished.

ICAP Task

The ICAP task sends files to an ICAP server to be scanned for data loss prevention or viruses.

Field	Definition
Basic Tab	
Label	Specify a label for this task.
ICAP Server	Select a pre-configured ICAP server from the drop down list.
Source File	Specify the path and file name of a single file to send. A file name is required, it may not be a directory name only.
Response Body Tab	
Destination	Specify if and where the response body, if any, should be saved. By default, the response body will be saved to the job log.
File	Specify the location of the file to which the response body, if any, should be saved. This is required if the 'Response Body Destination' is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Response Headers Tab	
Destination	Specify if and where the response headers should be saved. By default, the response headers will be discarded.
File	Specify the location of the file to which the response headers should be saved. This is required if the 'Response Headers Destination' attribute is set to 'file'.
When File Exists	Specify the action to take when the response file already exists. The default value is 'rename'.
Output Variables Tab	
ICAP Status Code Variable	If desired, specify the name of a variable which will contain the status code returned by the ICAP server. The variable may be used in subsequent tasks and will be created if it does not exist.
HTTP Status Code Variable	If desired, specify the name of a variable which will contain the status code returned in the encapsulated HTTP response. If an HTTP response is not returned from the ICAP server, this variable will be set to 0. The variable may be used in subsequent tasks and will be created if it does not exist.
ICAP Server Tab	

Refer to the "ICAP Resource" on page 87 page for the ICAP Server field definitions.	
Control Tab	
Version	The version of this task.
Log Level	Specify the level of logging to use while executing this task. Valid options are - silent, normal, verbose and debug. Default Value: Inherited from parent Module
Execute Only If	Specify a condition that must be satisfied before this task can be executed. This task will be skipped if the specified condition is not met.
Disabled	Whether or not this task is disabled. Default Value: false
On Error Tab	
On Error	Specify the action to take when this task errors out. Valid options are - abort, continue, call:[module] and setVariable:[name]=[value]. For call:[module] replace [module] with the name of the module in the project (e.g. call:ErrorModule). For setVariable:[name]=[value] replace [name] with a variable name and [value] with the variable value (e.g. setVariable:error=true). Default Value: Inherited from parent Module

Request Header

The Request Header Element allows you to add a custom header to your ICAP task.

Field	Definition
Basic Tab	
Name	Specify the name of the header you would like to include in the request.
Value	Specify the value for this header field.

CHAPTER 6

Services Overview

Managed File Transfer Services are used for inbound connections from your trading partners, customers and employees. The available services (protocols) are SFTP, FTP, FTPS, HTTPS, MLLP, and AS2.

For example, the SFTP service allows a remote client to connect into Managed File Transfer using their SFTP software to upload or download files. As another example, the HTTPS service could allow a user to connect to Managed File Transfer through their browser to upload, download and share files.

The settings for the Managed File Transfer Services should be reviewed and configured before they are started. For instance, you may want to specify a different port number to listen on for the SFTP server, indicate a certificate for the FTPS server, or specify your corporate logo to use for the HTTPS login screen. These settings can be configured within the "Service Manager" on page 516 screen.

Service Manager

The services (protocols) which are licensed in Managed File Transfer can be configured from within the Service Manager pages. The list of Services is displayed along with the status of each Service.

When Managed File Transfer is running in a cluster configuration, the services for each system in the cluster are displayed in the service manager. When you click the  icon to edit a service, the service configuration page will also display each server in the cluster.

To manage the available Services, log in as an Admin User with the **Product Administrator** role.

From the main menu bar, select **Services** and then click the **Service Manager** link.

HTTPS/AS2 Service

The HTTPS/AS2 Service can be configured with a number of options.

HTTP over SSL/TLS

HTTP connections secured with a SSL/TLS certificate will create an encrypted tunnel between the client system and the server. This will protect any data that flows over the tunnel including commands, user names and passwords. Managed File Transfer uses a HTTPS connection for the File Transfer Portal interface on the default HTTPS port 443.

AS2 and S/MIME over HTTP(S)

Applicability Statement 2 (AS2) is a method used to securely send/receive files over the Internet. The messages are built using the MIME format and sent over HTTP(S). AS2 messages can be compressed, signed, encrypted and then sent over an SSL tunnel, making AS2 a very secure option for transferring files. AS2 also implements MDN (receipts) to ensure the delivery of the message.

Quick Start for HTTPS

HTTPS uses a signed SSL certificate to encrypt an HTTP connection between a server and a client. Follow the steps below to create, sign and setup an SSL certificate for use with the Managed File Transfer HTTPS server.

1. "Create SSL Certificate" on page 734 an SSL certificate in the Default Private Keystore.
2. Generate a "Generate CSR (Certificate Signing Request)" on page 736 (CSR) for the newly created SSL Certificate.
3. "Import CA Reply" on page 737 the CA Reply and any required root (primary) and secondary certificates.
4. Set the key alias name for the signed certificate on the SSL tab of the "HTTPS Configuration" on page 521.
5. Restart the HTTPS/AS2 service on the "Service Manager" on page 516 page.

Configuring the Informatica Managed File Transfer File Transfer Portal

Web Users access the secure HTTPS interface using the format `https://[hostname]:[portnumber]`

[hostname] - the host name or IP address of the HTTPS server

[portnumber] - the port number of the HTTPS server. The default port for HTTPS is 443.

Login Screen Options

The following portions of the File Transfer Portal Login page can be customized as detailed below:

1 - Company Logo

Add a company logo using the Custom File option on the File Transfer Portal tab of the “HTTPS Configuration” on page 521.

2 - Forgot Password Link

Allow Web Users to request a new password through an automated process using a verification page and a reset link sent via email. This option is available when the "Enable Forgot Password Link" on the File Transfer Portal tab of the “HTTPS Configuration” on page 521 is set to Yes. If enabled, verify the SMTP settings are valid on the SMTP Settings tab of the “Global Settings” on page 752.

3 - Create Account Link

New users can create a Web User account using the Create Account link, which will verify the user via email, and then provide the user with options to create a user name and password. This option is available when the "Self-Registration" and "Register Link on Login Page" options are Enabled on the “Web User Self-Registration” on page 645 page.

4 - Disclaimer

Add a custom disclaimer to the login page with the options on the Languages tab of the “HTTPS Configuration” on page 521.

File Transfer Portal Header Options

The following sections in the header (after login) can be configured on either the Basic or Enhanced File Transfer Portal page. The numbered sections are described below. Some options may not be available to all Web Users based on their permissions.

1 - Company Logo

Add a company logo using the Custom File option on the File Transfer Portal tab of the "HTTPS Configuration" on page 521. This is the same logo that is used on the File Transfer Portal Login page.

2 - Shared Drive

When Shared Drive is enabled for a Web User in the "Web Users" on page 589 Features tab, a Web User can open the Shared Drive interface in the HTTPS File Transfer Portal to upload and synchronize files with devices and other users.

3 - Secure Mail

When Secure Mail is enabled for a Web User in the "Secure Mail Settings" on page 569 settings, a Web User can open the Secure Mail interface in the HTTPS File Transfer Portal to send ad-hoc messages with secure file packages.

4 - Secure Folders

If Secure Folders are enabled for a Web User in the "Web Users" on page 589 Features tab, a Web User can open the Secure Folders interface in the HTTPS File Transfer Portal to work with Network folders they are authorized to access.

5 - My Account

After a Web User authenticates, they can manage aspects of their account, like changing their password or updating their profile. Options available to a Web User are displayed in the drop-down list. A Web User can change their own password if the "Allow User to Change Password" option is selected on the Authentication tab of the "Edit Web User" on page 603 account. The update profile option is available on the File Transfer Portal tab of the "HTTPS Configuration" on page 521 page.

6 - Activity Report

When Activity Report is enabled for a Web User in the "Web Users" on page 589 Features Tab, a Web User can view their own audit activity (e.g. lgons, uploads, downloads) from within the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.

7 - Invite Users

When Send Invitations is enabled for a "Edit Web User" on page 603 account and the "Web User Self-Registration" on page 645 option is enabled, an Invite Users link is available to the Web User. This allows an authorized Web User to invite people to self-register on the Managed File Transfer server.

8 - Help

A Help option is available to the Web User when the "Display Help Link" is enabled on the File Transfer Portal tab of the "HTTPS Configuration" on page 521.

Quick Start for AS2

AS2 uses SSL certificates for encrypting and signing messages over a HTTP(S) connection. Each AS2 trading partner must be setup in Managed File Transfer.

1. Obtain and define the following details for each partner:
   AS2 From ID

   Place this in the AS2 ID field on the AS2 tab of the “Add Web User” on page 591.

   Public Certificate

   The trading partner will sign their signatures with their private key. You need to “Import SSL Certificate” on page 737 their public certificate into your Default Trusted Certificate Key Store and refer to its alias in the Signature Certificate Alias field on the AS2 tab of the “Add Web User” on page 591.
   What to provide each trading partner
2. Provide the following details to each partner:
   AS2 From ID

   Place this in the AS2 ID field on the AS2 tab of the HTTP/AS2 Service Preferences (“HTTPS Configuration” on page 521).

   URL

   The trading partner will use this URL to connect to your Managed File Transfer AS2 server. The default URL is [protocol]://[hostname][:port]/as2/receive.
3. Provide the following public certificates to each partner:
   Message Decryption

   Export (“Export SSL Certificates and Private Keys” on page 737) and send the public certificate or Head Certificate portion of the private key that the trading partner will use to encrypt the messages they send to you. Specify the alias of the private key in the Decryption Certificate Alias field on the AS2 tab of the HTTPS/AS2 Service Preferences (“HTTPS Configuration” on page 521).

   Signed MDN Receipts

   Export (“Export SSL Certificates and Private Keys” on page 737) and send the public certificate or Head Certificate portion of the private key you use to sign your MDN receipts. Specify the MDN Signature Certificate Alias of the private key on the AS2 tab of the “HTTPS Configuration” on page 521.

   If you do not have a private key, follow the steps outlined in the "Create an SSL Certificate" (“Create SSL Certificate” on page 734) section to create a private key and its associated public certificate.

Processing Return Receipts

Asynchronous Return Receipts can be handled automatically or manually per Web User. If a message fails however, a return receipt is sent automatically. A signed return receipts ensures the authenticity of the receipts. Signed messages and receipts are considered a Non-Repudiation of Receipt (NRR), which is a “legal event” indicating that both party’s identities and the message’s integrity are valid.

- If MDN Receipts are to be sent via email, configure the SMTP email settings in the “Global Settings” on page 752.
- Specify how receipts will be processed for each Web User on the AS2 tab of the “Add Web User” on page 591 account.

- Specify the global receipt options in the MDN (Receipts) section on the AS2 tab of the "HTTPS Configuration" on page 521.

  Note: Manual MDN receipts are sent by clicking the  icon on the "AS2 Log" on page 684 page.

HTTPS Configuration

The HTTPS/AS2 Server Configuration page provides a logical arrangement of the Preferences and Listeners for the HTTPS/AS2 Service.

Preferences

The following sections describe the Preferences settings.

General Properties

The following General properties can be set:

Automatically Start Service

Specify whether you would like to start the HTTPS/AS2 service automatically when Managed File Transfer starts.

Session Timeout

The length of idle time in seconds before the HTTPS/AS2 session will close. The default is 300 seconds.

File Transfer Portal

The following File Transfer Portal properties can be set.

General Tab

The General Tab contains the following parameters:

Enabled

The Managed File Transfer File Transfer Portal can be enabled or disabled. By default the service is enabled. Changing this setting requires a restart of Managed File Transfer. You must have the appropriate license to use the File Transfer Portal.

Allow Browsers to Save Login Credentials

By default, Managed File Transfer will not allow a browser to save login credentials. If enabled, the first time a Web User logs in to the HTTPS File Transfer Portal, their browser will ask them if they want to save their password.

Allow Session ID in URL

To prevent internet session hijacking vulnerabilities, Managed File Transfer will not allow a Web User's session ID to appear in the URL by default. When this option is enabled, the session ID will appear in the URL while a Web User is using the service (less secure).

Web User's who have their internet browser cookies disabled will not be able to use the service when Allow Session ID in URL is also disabled.

Allow Embedding within an IFrame

To prevent internet clickjacking vulnerabilities, Managed File Transfer will not allow the File Transfer Portal to run within an IFrame by default. When this option is enabled, the File Transfer Portal will be allowed to run in an IFrame, which can include potentially untrusted sources (less secure).

Site URL

The Site URL indicates the address of the File Transfer Portal and is used in emails that are sent from Managed File Transfer. This URL should be accessible from both internal and external network locations.

Secure Folders Tab

Secure Folders allows Web Users to work with authorized folders and files on the Network through the HTTPS File Transfer Portal.

User Interface Tab

The User Interface Tab contains the following parameters:

Logo

By default, the Managed File Transfer logo will be displayed on the login page and header for the Web client. Substitute a corporate logo by selecting the Custom File option and typing a file path and name for a graphic file. Graphic files should be a standard Web format (.jpg, .gif, .png), and sized appropriately (250x75px recommended).

Note: Custom logos must be copied to the <installdirectory>/ghttpsroot/custom folder, where <installdirectory> is the installation directory of Managed File Transfer.

Enable Forgot Password Link

The File Transfer Portal login page displays a Forgot Password link when this option is enabled. If selected by the Web User, the Forgot Password process sends an email to the registered Web User with a link to change their password.

Display Help Link

A User Guide is provided with the File Transfer Portal. A Help link, available at the top of the page, can be turned on or off for the File Transfer Portal.

Help File/URL

The location of the help documentation to display in the File Transfer Portal. The following options can be specified:

Default

The help file included with Managed File Transfer is the default help content.

File

If the Help link will open a document (for example, a PDF, text file, or HTML document), that file must be copied to the <installdirectory>/ghttpsroot/custom folder, where <installdirectory> is the installation directory of Managed File Transfer. Only the file name is placed in the text field (for example, webclienthelp.pdf).

URL

If the Help link will open a Web page, place the full URL in the text field (for example, http://www.example.com/filetransferportalhelp.htm).

Languages

The File Transfer Portal is available to Web Users in the following languages:

- English
- German
- French
- Spanish

- Japanese
- Portuguese
- Indonesian
- Chinese

The Languages tab allows you to configure the custom page heading and disclaimer message that will be displayed for each language. Managed File Transfer uses the Web User's internet browser language settings to choose the File Transfer Portal's default language. If a Web User's internet browser is configured to use multiple languages, and the preferred language is not available or enabled, Managed File Transfer will use the next available language in the order of preference from the Web User's browser. English will be used as the default language if no other language can be found.

Each language can be enabled by expanding the **Enlarge** icon and then select the Enabled option.

The Languages tab contains the following properties:

Page Title

The Page Title is displayed in the title bar of the browser when a Web User accesses Managed File Transfer through the File Transfer Portal.

Display Disclaimer

A disclaimer is information that each Web User will view before accessing Managed File Transfer. If selected, the disclaimer text is displayed below the login box on the File Transfer Portal login page.

Heading

The heading is the title of the disclaimer. The heading is centered under the File Transfer Portal login page.

Short Description/Disclaimer

The disclaimer text cannot exceed 2000 characters and supports HTML. Your description can include linked text that opens a file or web page in a new window. The linked text must be enclosed in `<link> </link>` tags. For example, `Read the full disclaimer <link>here</link>`.

Disclaimer File/URL

Enter the file name or URL for the resource referenced in the `<link>` text from the **Short Description/Disclaimer** field.

- **File** - If the link will open a document (for example, a PDF, text file, or HTML document), that file must be copied to the [installdirectory]/ghttpsroot/custom folder, where `[installdirectory]` is the installation directory of Managed File Transfer. Only the file name is placed in the text field, for example, `disclaimer.pdf`.
- **URL** - If the link opens a web page, place the full URL in the text field, for example, `http://www.example.com/disclaimer.htm`.

SAML Single Sign-On

SAML (Security Assertion Mark-Up Language) is an XML based open standard for authorization and authentication between an Identity Provider and a Service Provider. During authentication, a SAML assertion is transferred from Identity Providers to Service Providers. Assertions contain XML statements that Service Providers use to make access-control decisions.

The settings on the SAML Single Sign-On tab allow you to configure Managed File Transfer as a Service Provider to authenticate Web Users using an Identity Provider, such as ADFS, OpenAM, Shibboleth, Salesforce.com, SimpleSAMLphp, and more. Managed File Transfer supports SAML v2.0 Web Browser SSO

Profile, with HTTP POST and HTTP Redirect bindings. A Web User account must exist within Managed File Transfer before it can be authenticated using SAML. If Managed File Transfer cannot process the SAML assertion, the Web User will be directed to the File Transfer Portal Login page.

Note: Web Users authenticated using SSO will not have access to SMB Network Share resources that are configured with the "Network Shares" on page 52. SAML does not pass the user's password to Managed File Transfer.

The following sections describe the Preferences settings related to SAML.

General Tab

The General Tab contains the following parameters:

Enabled

Enable SAML Single Sign-On (SSO).

Force Identity Provider Login

When enabled, all authentication requests to the File Transfer Portal must go through the Identity Provider. When disabled, Web Users can authenticate to the File Transfer Portal by accessing the login page URL.

Logout Redirect URL

The alternate URL to forward the Web User to when they log out of the File Transfer Portal. By default, Managed File Transfer directs a Web User to the File Transfer Portal Login page when they log out.

Identity Provider Tab

Configure the Identity Provider Managed File Transfer will use to authenticate Web Users to the File Transfer Portal.

Entity ID

The ID given to the Identity Provider as the trusted ID. This ID is also used as the expected certificate alias of the Identity Provider's certificate within the default trusted certificates key store.

Binding

Select the type of protocol method for the Identity Provider.

- HTTP POST - Posts a form that contains the message body.
- HTTP Redirect - Sends the message body as query parameters.

Post URL

When the HTTP POST binding is selected, you must enter the URL used to post authentication requests to.

Redirect URL

When the HTTP Redirect binding is selected, you must enter the URL used to send the message body as query parameters.

Server Time Offset

If the Identity Provider and Managed File Transfer system time are not in sync, you can specify a time offset which will be applied to the assertion's time window (in seconds). This is sometimes necessary when the Identity Provider is not within the same network as Managed File Transfer and you cannot control the servers time.

Import Metadata

Managed File Transfer can import the Identity Provider settings, including the Identity Provider certificate, from a SAML Metadata XML file.

1. Click the Choose File button and browse to the Metadata file.
2. If the Metadata file contains a certificate, it will be added to the Default Trusted Certificates Key Store using the entity ID as the certificate alias. If the certificates already exists, you can choose Replace Certificate If Exists to overwrite the existing certificate.
3. Click the Import Metadata button to parse the Metadata file and populate the Identity Provider settings.

Service Provider Tab

Configure Managed File Transfer (the Service Provider) to authenticate Web Users through the Identity Provider.

The Service Provider tab contains the following settings:

Entity ID

The ID given to Managed File Transfer as the trusted ID. Typically this is the host name defined for Managed File Transfer (similar to the Site URL).

Private Store Certificate Alias

The alias of the certificate located in the Default Private Key Store used to sign requests and decrypt assertions. Click the  icon to browse and select the certificate.

Require Signed Response

Determines if Managed File Transfer requires the response to be signed. Typically the response and/or the assertion is signed to establish trust between the Identity Provider and Managed File Transfer.

Require Signed Assertion

Determines if Managed File Transfer requires the assertion to be signed. Typically the response and/or the assertion is signed to establish trust between the Identity Provider and Managed File Transfer.

Require Encrypted Assertion

Determines if Managed File Transfer requires the assertion to be encrypted when it is received. This is typical when SSL is not used for communication between Managed File Transfer and Identity Provider.

Username Tab

Informatica Managed File Transfer must identify and correlate the subject of an assertion with a Web User in Managed File Transfer. Typically, the user name will be in the NameID field within a SAML assertion. However, Managed File Transfer can also use an attribute within the assertion to identify the user name.

The Username tab contains the following settings:

Username Location

Select the NameID or Attribute where the user name is found.

NameID

The NameID element.

NameID Format

The format of the NameID element within the SAML response. Managed File Transfer will validate the NameID format before authenticating the SAML assertion. Managed File Transfer supports the following SAML Core V2.0 options:

- Unspecified
- X509SubjectName
- Windows Qualified Domain Name
- Email Address
- Persistent
- Transient
- Kerberos
- Entity

Attribute Name Format

The format of the attribute element that identifies a username within the SAML response. Managed File Transfer will validate the attribute format before authenticating the SAML assertion. Managed File Transfer supports the following SAML Core V2.0 options:

- Basic
- Uniform Resource Identifier

Attribute Name

The attribute name within the assertion XML that identifies the username.

Parse Username Value

When enabled, the value retrieved from the assertion can be parsed using a regular expression pattern.

Username Pattern

Specify a regular expression to parse a user a username value from the attribute.

NameID Example: The x509SubjectName NameID element format for user kharris is 'uid=kharris,ou=marketing,o=example,dc=example,dc=com.' To identify kharris using the uid, use uid=(.*),o=.* for the regular expression.

Attribute Example 2: The username 'kharris' will be parsed from the email address attribute from the SAML assertion. To identify the username, you can use the ([^@]+) regular expression to parse 'kharris' from 'kharris@example.com.'6

Test Response

Allows you to submit a sample assertion response to validate the current configuration.

Base64 Encoded

If the assertion is Base64 encoded, enabling this option will decode the assertion before validating.

SAML Response

Copy your sample assertion to this field.

Validate

Click the Validate button to validate the sample assertion against the SSO settings configured on the SAML tab. Managed File Transfer will attempt to find the user and verify they are authorized for the File Transfer Portal.

Note: It is suggested that you set the global log level to debug while configuring SAML Single Sign-On. The SAML request and response messages will be written to the log, and can be validated using the Test Response option.

HTTPS

The settings on the HTTPS tab allow you to define restrictions on the files that can be uploaded to the Managed File Transfer system.

Restrict Uploads to Inbound Directory

When selected, uploads are restricted to the inbound directory and any sub-directories under it. Web Users will not be able to upload files to any directory other than inbound. This option should not be selected if Web Users need to upload files in other locations, or if inbound and outbound folders were not created for Web Users based on the settings of the **Data tab** in global settings.

Note: This option is available only on Managed File Transfer versions earlier than 3.0.0. It is recommended to use virtual folders to control Web User file and folder access.

Maximum Upload File Size

Type a value in this box to limit the size of the files that Web Users can send to your server. Files larger than the specified file size will be rejected.

Allow Files with No Extension

Select this option to upload files that do not have extensions.

Allow Files with an Extension

Select this option when you want to enable the File Extension Filter.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or only permit specific extensions. If you want to specify the file types Web Users can or cannot upload, type each file extension in this box. Type all extensions without periods (.), separate them with commas, and do not add line breaks or spaces. For example, if you want to allow only .txt, .xls, .xlsx, and .csv files, type txt,xls,xlsx,csv. The maximum number of characters for this field is 2000.

ASCII Mode File Name Patterns

Files matching the specified file name patterns will be transferred in ASCII mode. The default transfer method in Managed File Transfer is binary, but some files with specific end-of-line characters (CRLF, etc.) are best transferred between platforms in ASCII mode. Each file name pattern is separated by a comma and can contain text and wildcards (for example, Payroll*.csv,*.txt). The maximum number of characters for this field is 2000.

AS2

The settings on the AS2 tab configures the identity, security and file restrictions for AS2 communications.

Note: Additional AS2 information is located in the "Quick Start for AS2" on page 520.

General Tab

The General tab contains the following settings:

The General Tab contains the following parameters:

Enabled

The AS2 service can be enabled or disabled for use within Managed File Transfer. If selected, AS2 functionality is available to authorized Web Users. The default URL is [protocol]://[hostname][:port]/as2/receive. You must be licensed for the AS2 feature in order to use it.

AS2 ID

List of IDs of the Managed File Transfer AS2 instance. A client uses AS2 ID to reference the Managed File Transfer server. AS2 ID is case sensitive. It can be 1 to 128 ASCII printable characters in length and does not contain spaces. You can add multiple AS2 IDs and the IDs contain a maximum of 4000 characters. Enter each AS2 ID in a separate line.

Decryption Certificate Alias

The Decryption Certificate Alias is the certificate that is used to decrypt incoming messages. The alias references a certificate in the Default Private Key Store. If you do not know the alias name for the certificate, click the icon to select the certificate. The public portion of this certificate should be sent to all Web Users who will be sending AS2 messages to Managed File Transfer.

Default Upload Folder

The default location where AS2 messages are saved when uploaded. The folder location is relative to the Web Users folder and will be created if it does not exist. For example, if the default Web User folder is [installdirectory]/userdata/webdocs/webuser and the specified upload folder is inbound/as2, messages will be uploaded to the [installdirectory]/userdata/webdocs/webuser/inbound/as2 folder. This folder location is overridden at the Web User level.

When File Exists

The action that Managed File Transfer performs when a file with the same name exists in the default upload folder. This action can be overridden at the Web User level. The available options are:

- Rename will automatically rename the uploaded file (appending a unique sequential number) so that both files are maintained.
- Overwrite replaces the existing file with the one being uploaded.
- Skip does not upload the duplicate file. It skips the file and proceeds to the next file in the list.
- Error will stop the upload without processing the remaining files.

MDN (Receipts) Tab

The MDN tab contains the following settings:

Keep Receipts

When enabled, Message Disposition Notifications (also known as Receipts), can be saved for auditing purposes. These receipts are stored in the AS2 audit log database for the number of days indicated in

the Days to Keep Audit Logs field in the Log Settings. The icon on the AS2 Log page allows you to view the saved receipts.

MDN Signature Certificate Alias

This is the alias that refers to the private key used to sign the message receipt. The private key is located in the Default Private Key Store. If you do not know the alias name for the private key, click the icon to select the private key alias.

Asynchronous MDN Approval

If a return receipt is requested by Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed. The icon on the AS2 Log page indicates a manual receipt needs to be sent for a message. A manual receipt can only be sent if a message is received successfully. If an error occurs during transmission, an asynchronous receipt is sent automatically.

Use Proxy for Asynchronous MDN

If enabled, the proxy server is used to send asynchronous MDN. The following proxy configuration details are enabled:

Proxy Type

Managed File Transfer supports SOCKS (version 4 and 5), HTTP tunneling through an HTTP proxy, and Managed File Transfer Gateway. Check with the network administrator for the correct proxy type.

Proxy Host

The host name or IP address of the proxy server.

Proxy Port

The port number to use for connecting to the proxy server.

Proxy Username

The user name to use for connecting to the proxy server.

Proxy Password

The password to use for connecting to the proxy server.

Message Security tab

The Message Security tab contains the following settings:

Require Encryption

This option indicates whether or not files received by Managed File Transfer should be encrypted.

Require Signature

A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any message without a digital signature will be rejected.

Require Authentication

Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the AS2 From ID in the message to find the Web User with a matching AS2 ID. Informatica recommends you select the 'Require Signature' option when authentication is not required.

Upload Restrictions Tab

The Upload Restrictions tab contains the following settings:

Maximum Message Size

Messages that are received with a "Content-Length" header can be validated to ensure that the size of the message is less than the Maximum Message Size specified. Messages that are sent with chunked transfer encoding are not validated against this size restriction.

Allow Files with No Extension

Select this option to allow web users to upload files that don't have extensions.

Allow Files with an Extension

Select this option to allow web users to upload files that have extensions. The web users must enter the file extensions in the **File Extension Filter** field.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or permit specific extensions. To specify the file types Web Users can or cann't upload, enter the file extension in this box. Enter extensions without periods (.), separate them with commas, and don't add line breaks or spaces. For example, to allow .txt, .xls, .xlsx, and .csv files, enter txt,xls,xlsx,csv. The maximum number of characters for this field is 2,000.

Allow Files with No Name

Select this option to allow messages that do not include a file name. Files without a name are saved with the name "as2data_[datetime]" (where [datetime] is the current timestamp including milliseconds).

Listener

The following settings apply to the Listener.

General Tab

The General Tab contains the following parameters:

Name

Providing an identifiable name for the listener helps identify it in the Configuration Outline list.

Port

Listeners monitor specific port numbers. Set the port number that the listener will monitor.

Protocol

Sets the protocol to handle incoming traffic. The default value is HTTP/1.1.

Local Address

This is the IP address of the server hosting the port to which you are listening. If available, you can also select it from the drop-down list.

Enable Lookups

When lookups are enabled, the server will search for and report servers by their DNS name. If lookups are not used only the IP address is returned.

Disable Upload Timeout

Lengthy uploads may decrease server performance or be the result of an error. Select whether uploads are subject to timeouts.

Compression

File compression may increase transfer rates, but lower processing speeds. By default, compression is set to On and will compress only text data. If set to Off, no compression is used on files and if compression is set to Force, compression is used for all files.

No Compression User Agents

This option allows a user with the System Administrator role, in certain instances, to specify the header data of a browser for which files will never be compressed.

Connection Timeout

The number of seconds this connection will remain open before closing if no requests are sent. The default is 60 seconds.

Maximum Threads

The maximum number of threads created by the connection for request processing on this Listener. This determines the maximum number of simultaneous requests that can be handled. The default is 200 threads.

Minimum Spare Threads

This is the number of threads that will be created when this listener is first started. The default is four (4) threads.Note: Changing the Thread values can alter performance. Too few Maximum Threads and transfers may lag, but too many threads may limit performance of other applications. Modify these values to obtain the optimal performance for your configuration requirements.

Server Header

When a User makes a connection to Managed File Transfer via HTTP or HTTPS, the server replies back to the client with the name and version of the server in one of the headers. The Server Header field can be used to customize the server information that is returned. This setting should only be specified when attempting to hide the true identity of the server for security purposes.

Proxy Name

The Proxy Name attribute can be used when Managed File Transfer is run behind a proxy server. This attribute modifies the value returned to web applications that call the request.getServerName() method, which is often used to construct absolute URLs for redirects. Without configuring this attribute, the value returned would reflect the server name on which the connection from the proxy server was received, rather than the server name to whom the client directed the original request.

Proxy Port

The Proxy Port attribute can be used when Managed File Transfer is run behind a proxy server. This attribute modifies the value returned to web applications that call the request.getServerPort() method, which is often used to construct absolute URLs for redirects. Without configuring this attribute, the value returned would reflect the server port on which the connection from the proxy server was received, rather than the server port to whom the client directed the original request.

SSL Tab

SSL Enabled

From the drop-down list, select the appropriate option:

- Yes - A Secure Socket Layer is used to secure transmissions
- No - Transmissions are not secured with SSL

SSL Protocol

From the drop-down list, select the appropriate option:

- SSL - A traditional Secure Socket Layer protocol is used to secure the transmission
- TLS - A new version of SSL, Transport Layer Security will be used to secure the transmission (default)

Enabled SSL Protocols

Specify a comma separated list of SSL/TLS protocol versions to allow. For example, to enable only TLS 1.1, TLS 1.2, and TLS 1.3, specify TLSv1.1, TLSv1.2, TLSv1.3. Likewise, to enable all versions of SSL/TLS, specify SSLv3,TLSv1,TLSv1.1,TLSv1.2, TLSv1.3.

Algorithm

This field displays the certificate encoding algorithm. The field is pre-populated based on your installation. The available options are:

- IbmX509 - Only used for IBM based installations
- SunX509 - Used for Sun and most other installations

Client Authentication

This determines how the client will authenticate with the server.

- None - The SSL connection runs without checking certificates and the User is authenticated with a password. If any of the information being transmitted requires a certificate, the connection will fail.
- Optional - The SSL connection looks for a valid certificate, but continues with password authentication if a certificate is not present.
- Required - The SSL connection will not connect or authenticate a User unless a valid certificate is available.

Enabled Cipher Suites

By default all Cipher Suites are enabled to provide the most options between different clients and servers. Although encrypted, the cipher suite automatically selected by the connection may not be the most secure. This list allows you to limit which ciphers are used. Follow the instructions below to select which Cipher Suites are used:

1. In the left column, click to select (highlight) the Cipher Suites to use. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Cipher Suites are selected, click the arrow between the group boxes to move the Cipher Suites from left to right.

Key Store File

This file contains the private key and associated certificates that a client uses to authenticate to a server. There are default Key Store files provided with Managed File Transfer or you can create your own.

Type the name or click the  icon to browse for the file.

Key Store Password

The password to use for accessing the key store.

Key Store Type

The type of key store. Managed File Transfer supports both the JKS (Java Key Store) and PKCS12 (Public-Key Cryptography Standards) key store types.

Key Store Provider

Based on your installation, not all the providers may be available. The correct Key Store Provider is loaded during the installation. However, if you need specify a provider, from the drop-down list select the appropriate option:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM
- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- SUN - The classic Java cryptographic service
- SUNJSSE - The Java Secure Socket Extension provides an RSA layer to the cryptology
- SUNJCE - The Java Cryptographic Extension is the export compliant variation of the SUN provider
- SUNMSCAPI - The Java implementation of the Microsoft Cryptography API
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509

Key Alias

The key alias identifies a key pair and its associated certificate from all the ones within a Key Store. If no alias is specified, the Key Store opens the first file in the key store. Type the name or click the  icon to browse for an Alias.

Export Head Certificate

Exports the head certificate of the selected Key Alias to your internet browser's default download directory.

Trust Store File

The Trust Store File contains the public keys and certificates used by a server to authenticate a client. There are default Trust Store files provided with Managed File Transfer or you can create your own. Type the name or click the  icon to browse for the file.

Trust Store Password

The password to use for accessing the Trust Store.

Trust Store Type

The type of trust store. Managed File Transfer supports both the JKS (Java Key Store) and PKCS12 (Public-Key Cryptography Standards) trust store types.

Trust Store Provider

Based on your installation, not all the providers may be available. The correct trust store provider is loaded in the installation. However, if you need specify a provider, from the drop-down list select the appropriate option:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM
- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- SUN - The classic Java cryptographic service

- SUNJSSE - The Java Secure Socket Extension provides an RSA layer to the cryptology
- SUNJCE - The Java Cryptographic Extension is the export compliant variation of the SUN provider
- SUNMSCAPI - The Java implementation of the Microsoft Cryptography API
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509
-

Redirection Tab

HTTP/HTTPS traffic can be automatically redirected to the intended protocol, host and/or port. The redirect process substitutes the appropriate portion of the URL (`[protocol]://[host][:port]`). For example, if a user typed the address "secure.example.com" (which translates to http://secure.example.com on port 80), the connection could be redirected to https://secure.example.com:9001 by specifying the HTTPS protocol and providing the port used for SSL traffic.

The Redirection tab contains the following settings:

Enable

When redirection is enabled, traffic is redirected using the values in the following fields.

Redirect Host

The host name or IP address to which HTTP/HTTPS traffic should be redirected. If no redirect host is specified, Managed File Transfer uses the URL or address portion of the original request (for example, if the request is made to secure.example.com, that value will be attached to the specified port or protocol).

Redirect Port

The redirect port is the port to which HTTP/HTTPS traffic should be redirected. If not specified, the default port for HTTP is 80 and HTTPS is 443.

Redirect Protocol

The protocol on which traffic should be redirected. Select the protocol from the drop-down list. The default value is HTTPS.

Signing MDN Receipts

Digital signatures added to an AS2 MDN Receipt allow the receiver of the MDN to verify your authenticity. The Decryption Certificate alias can also be used as the MDN Signature Certificate alias. If the certificate being used is already signed by a trusted authority (for example, Verisign, GoDaddy, Equifax, etc.) the certificate does not need to be imported as the trust is inherited. To add a digital signature to a MDN receipt follow the steps below:

1. On the AS2 tab of the HTTPS/AS2 Service Preferences locate the MDN Signature Certificate Alias field.
2. Type the alias name or click the  icon to browse for the private key. In order for your trading partner to verify your signature, you will need to export and send them the public certificate associated to this private key.

FTP Service

The File Transfer Protocol (FTP) Service can be configured with a number of options on the FTP Server Configuration and FTP Service Preferences pages.

FTP Server Configuration

The FTP Server Configuration page provides configuration options for the FTP Service. From this page, modify or add service parameters such as: Login parameters, Listeners, certificates, etc.

Preferences

The following sections describe the Preferences settings.

General

The following sections describe the general Preferences settings.

Automatically Start Service

Specify whether you would like to start the FTP service automatically when Managed File Transfer starts.

Upload Restrictions

The following sections describe the Preferences settings related to the upload restrictions.

Restrict Uploads to Inbound Directory

When selected, uploads are restricted to the inbound directory and sub-directories. Web Users will not be able to upload files to any directory other than "Inbound." This option should not be selected if Web Users need to upload files in other locations or if Inbound and Outbound folders were not created.

Note: This option is no longer available and will only be visible if it was in use prior to Managed File Transfer version 3.0.0. It is recommended to use "Virtual Folders and Files" on page 586 to control Web User file and folder access.

Allow Files with No Extension

When selected, Web Users can upload files that do not have extensions.

Allow Files with an Extension

This option enables the File Extension Filter.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or only permit specific extensions. If you want to specify the file types Web Users can or cannot upload, type each file extension in this box. Type all extensions without periods (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type txt,xls,xlsx,csv). The maximum number of characters for this field is 2000.

Server

The following sections describe the Server settings:

Maximum Logins

This is the maximum number of sessions allowed to the service at any given time.

Maximum Threads

This is the maximum number of simultaneous threads that the server will use at any one time. If left blank, the default is 100. If more transfer requests (each using a thread) are made than exist, the remaining requests will be held by Managed File Transfer until a thread becomes available.

Login Failure Delay

The amount of time in seconds a Web User must wait before the Web User can retry their login. This delay deflects multiple login attempts in fast succession from an organized online attack.

Maximum Login Failures

The number of failed login attempts before the FTP connection is closed.

Welcome Message

The welcome message is returned to the client after a connection is established to Managed File Transfer. By default, the following welcome message is displayed:

```
Service ready for new user.
```

Logout (Quit) Message

The message to return to the client after the quit command is issued. By default, the logout message is "Goodbye".

Listener

The listener specifies on which port the FTP service will monitor traffic. To add an FTP listener, complete the required fields and click the **Save** button. Click the  Add SSL link in the page toolbar to add an Explicit SSL configuration or click the Explicit SSL link to modify the existing SSL options. Click the Delete link in the page toolbar to delete this FTP Listener.

Name

Providing an identifiable name for the Listener helps identify it in the Configuration Outline list.

Port

Set the port number that the Listener will monitor.

Note: If using the Managed File Transfer Gateway, any changes to the Port number will also need to be updated on the "Configure the Gateway Parameters" on page 559 page for the related Service Mapping.

Idle Timeout

The idle time in seconds before the Listener will timeout.

Local Address

This is the IP address of the server hosting the port to which you are Listening. If available, you can also select it from the drop-down list.

Note: If using Managed File Transfer Gateway, any changes to the Local Address will also need to be updated on the "Configure the Gateway Parameters" on page 559 page as the "To Address" for the FTP Service Mapping.

Force Encrypted Authentication

The Managed File Transfer FTP connection can be configured to require SSL/TLS encryption on the command/control channel before accepting user authentication. The default setting is No, meaning plain FTP is allowed on this listener. When the option is set to Yes, the listener will accept the authentication request only if SSL/TLS encryption has first been established. If the Force Encrypted Authentication option is set to Yes, an Explicit SSL configuration is required.

Explicit SSL

An Explicit SSL connection will start on any available FTP port. The Explicit SSL configuration verifies a connection is made and then requests and verifies an SSL connection before transmitting login or file data.

SSL Protocol

From the drop-down list, select the appropriate option:

- SSL - A traditional Secure Socket Layer protocol is used to secure the transmission
- TLS - A new version of SSL, Transport Layer Security will be used to secure the transmission (default)

Enabled SSL Protocols

Specify a comma separated list of SSL/TLS protocol versions to allow. For example, to enable only TLS 1.1, TLS 1.2, and TLS 1.3, specify TLSv1.1, TLSv1.2, TLSv1.3. Likewise, to enable all versions of SSL/TLS, specify SSLv3,TLSv1,TLSv1.1,TLSv1.2, TLSv1.3.

Client Authentication

The client authentication option indicates if SSL authentication is expected when a client connects to Managed File Transfer. If a "Edit Web User" on page 603 or "Edit Web User Template" on page 632 is configured to authenticate using a certificate, the Optional or Required setting should be selected.

- None - Client certificate authentication is not enabled and client certificates will be ignored. Clients must authenticate with their username and password when connecting to the server.
- Optional - Client certificate authentication is enabled, but a certificate is not required. If a valid certificate is available from the client, it will be used to for authentication. If a valid certificate is not available, the client must authenticate with their username and password when connecting to the server.
- Required - Client certificate authentication is enabled and a valid certificate is required. A client connection without a valid certificate will be rejected.

Enabled Cipher Suites

By default all Cipher Suites are enabled to provide the most options between different clients and servers. Although encrypted, the cipher suite automatically selected by the connection may not be the most secure. This list allows you to limit which ciphers are used. Follow the instructions below to select which Cipher Suites are used:

1. In the left column, click to select (highlight) the Cipher Suites to use. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Cipher Suites are selected, click the → arrow between the group boxes to move the Cipher Suites from left to right.

Key Store File

This file contains the private key and associated certificates that a client uses to authenticate to a server. There are default "Open SSL Key Store" on page 731 files provided with Managed File Transfer or you can create your own. Type the name or click the ... icon to browse for the file.

Key Store Password

The Key Store Password was specified by the person who created the Key Store.

Key Store Type

From the drop-down list, select the appropriate option:

- JKS - Java Key Store
- PKCS12 - Public-Key Cryptography Standards

Key Store Provider

Based on the installation, not all providers may be available. The correct Key Store Provider is loaded during the installation. If you need specify a provider, select the appropriate option from the drop-down list:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM

- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- SUN - The classic Java cryptographic service
- SUNJSSE - The Java Secure Socket Extension provides an RSA layer to the cryptology
- SUNJCE - The Java Cryptographic Extension is the export compliant variation of the SUN provider
- SUNMSCAPI - The Java implementation of the Microsoft Cryptography API
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509

Key Alias

The key alias identifies a key pair and its associated certificate from all the ones within a Key Store. If no alias is specified, the Key Store opens the first file in the key store. Type the name or click the  icon to browse for an Alias.

Export Head Certificate

Exports the head certificate of the selected Key Alias to your internet browser's default download directory.

Trust Store File

The Trust Store File contains the public keys and certificates used by a server to authenticate a client. There are default Trust Store files provided with Managed File Transfer or you can create your own. Type the name or click the  icon to browse for the file.

Trust Store Password

The Trust Store Password was specified by the person who created the Trust Store.

Trust Store Type

See Key Store Type.

Trust Store Provider

See Key Store Provider.

CCC Enabled

Select this option to indicate that Web Users are permitted to send the clear command channel (CCC) command during an encrypted FTP connection. If a Web User sends the CCC command, it terminates the encryption on the command channel and all subsequent FTP communication on the command channel will be transmitted in plain text. Please note that the encryption of the data channel is not affected by this setting. If unselected, the command channel will remain encrypted.

Note: This setting is useful when Managed File Transfer is behind a NAT firewall that requires plain text commands for routing secondary FTPS data connections.

CCC Send Close Notify

Select this option to indicate that Managed File Transfer should perform the CLOSE_NOTIFY operation when the CCC command is received, which will properly terminate the SSL/TLS encryption for the command channel. If unselected, the CLOSE_NOTIFY will not be preformed. Some FTP clients may not support proper termination of SSL/TLS and require this option to be disabled.

Data Connection

The FTP Data Connection is the connection over which data is transferred (sent or received) and is established when a FTP command is issued (for example, GET, PUT, LIST).

Idle Timeout

The idle time in seconds before the Data Connection will close.

Force Encrypted Data Channels

An encrypted data channel protects the data using implicit SSL. If the client connection to Managed File Transfer does not support an encrypted data channel, the connection will fail. The default setting is No.

Active

With an "active" Data Connection, the client computer connects to the server on the control port and specifies to the server which port it is listening on for the data. This can cause issues with a firewall on the client side as it may block the incoming data connection from the server.

Enabled

If set to Yes, the Data Connection for the Listener will attempt a FTP connection to establish the data port.

Validate IP

This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail. If left blank, the default is No.

Local Address

This is the IP address of the server to which Managed File Transfer is listening. If available, you can also select it from the drop-down list.

Local Port

The local port on which the server will make the Active Data Connection. If none specified, any available port is used.

Passive

In a passive Data Connection, the client computer initiates the control port, but then also initiates the data port. This bypasses the firewall issue as the client computer initiates all the connections.

Local Address

This is the IP address of the server to which Managed File Transfer is listening. If available, you can also select it from the drop-down list.

External Address

The address the server will claim to be listening on for the data port. Useful when the server is behind a NAT firewall and the client sees a different address than the server is using.

Validate IP

This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail. If left blank, the default is No.

Ports

The ports on which the server is allowed to accept Passive Data Connections. Multiple port numbers are comma delimited. The text box also accepts ranges separated with hyphens. Ranges and single port numbers can be mixed (i.e. 60000-61000, 61052, 63000-65535). Valid port numbers are from 1 to 65535, however many ports below 1024 are reserved by the operating system and other programs.Note: If you wish to Delete a Listener entry, select the Listener entry in the Configuration Outline, then click the ✖ Delete link in the page toolbar.

FTPS Service (FTP over SSL)

The traditional FTP protocol sends commands and data in “the clear” over the network/internet. This FTP data could be intercepted by an attacker, which could then be viewed and altered before sending it on to the receiver.

If you are sending sensitive data over the internet, then you may want to consider the FTPS (FTP over SSL) protocol for securing data. The following image shows a model of the communications.

When the Project executes, the Job Log will contain the HTTP Response Body from the DLP server that includes the status code. In this example, the "Credit Cards.txt" file contains sensitive data and the Project failed when the error code was returned . In this example, the DLP server was configured to redact text which removed the sensitive information and replaced them with asterisks. The redacted version was returned in the encapsulated HTTP response body and can be saved to the job log or a file.

FTPS creates an encrypted tunnel between two computer systems and will protect against the following attacks:

- IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host
- IP source routing, where a host can pretend that an IP packet comes from another, trusted host
- DNS spoofing, where an attacker forges name server records

- Interception of cleartext passwords and other data by intermediate hosts
- Manipulation of data by attackers in control of intermediate hosts
  FTPS uses a combination of *asymmetric* (public key) cryptology and *symmetric* cryptology to provide strong encryption and optimal performance.

  Both the server and the client can be authenticated (trusted) through the use of X.509 Certificates. In other words, certificates will help ensure that each party is truly who they say they are.

Quick Start for FTP Server

Perform these steps to define and start the FTP Server.

1. Configure the FTPS server.
2. Start the FTPS server.

SSL Certificate Authentication

1. If not already done, configure the SSL Listener for the FTPS Service to either make SSL Client Authentication optional or required for all web users.
   a. From the main menu bar, select **Services** and then click the **Service Manager**link.
   b. Click the  icon next to the FTPS Service.
   c. On the left side of the page, click the Implicit SSL element under the Configuration Outline.
   d. Change the Client Authentication attribute to either Optional or Required:
      1. None (default) – will only accept Password authentication. Certificate authentication is not allowed.
      2. Optional (recommended) – will accept Web Users that use Password only authentication as well as Web Users that use Password and Certificate authentication.
      3. Required – only set this option if all Web Users will be required to authenticate to the FTPS Service using Password and Certificate authentication.
   e. When complete, click the **Save And Finish** button.
   f. On the Service Manager page, click the  icon to restart the FTPS Service.
2. Change the Web User's authentication type:
   a. From the Dashboard, point to Security and then click **Web User**.
   b. On the Web Users page, click the  icon next to the Web User.
   c. In the Edit Web User page, click the Authentication tab and change the FTPS Authentication Type to Password and Certificate.
   d. Click the **Save** button.
3. If Using an SSL Self-Signed Certificate, perform the following steps:
   a. Have your trading partner send you their SSL Public Certificate .
   b. Import the Public Certificate into the Default Trusted Certificates keystore in the SSL Certificate Manager .
   c. Restart the FTPS Service.

FTPS Server Configuration

The FTPS Server Configuration page provides the configuration options for the FTPS Service (Implicit SSL). From this page, modify or add service parameters such as: Login parameters, Listeners, certificates, etc.

Preferences

The following sections describe the Preferences settings.

Automatically Start Service

Specify whether you would like to start the FTPS service automatically when Managed File Transfer starts.

Upload Restrictions

Server

The following Server settings can be modified:

Maximum Logins

This is the maximum number of sessions allowed to the service at any given time.

Maximum Threads

This is the maximum number of simultaneous threads that the server will use at any one time. If left blank, the default is 100. If more transfer requests (each using a thread) are made than exist, the remaining requests will be held by Managed File Transfer until a thread becomes available.

Login Failure Delay

The length of time in seconds a Web User must wait before they can retry their login. This delay will deflect multiple login attempts in fast succession from an organized online attack.

Maximum Login Failures

This value represents the number of failed login attempts before the FTPS connection is closed.

Welcome Message

The welcome message is returned to the client after a connection is established to Managed File Transfer. By default, the welcome message is "Service ready for new user".

Logout (Quit) Message

The message to return to the client after the quit command is issued. By default, the logout message is "Goodbye".

Listener

The listener specifies on which port the FTPS service will monitor traffic. To add an FTPS listener, complete the required fields and click the **Save** button. Click the Implicit SSL link (in the Configuration Outline) to modify existing SSL options. Click the  Delete link in the page toolbar to delete this FTPS Listener.

Name

Providing an identifiable name for the Listener helps identify it in the Configuration Outline list.

Port

Set the port number that the Listener will monitor for connections.Note: If using Managed File Transfer Gateway, any changes to the Port number will also need to be updated on the Gateway for the related Service Mapping.

Idle Timeout

The idle time in seconds before the Listener will timeout. The default is 300 seconds.

Local Address

This is the IP address of the server hosting the port to which Managed File Transfer is listening. If available, you can also select it from the drop-down list.

Note: If using Managed File Transfer Gateway, any changes to the Local Address will also need to be updated on the Gateway page as the "To Address" for the FTPS Service Mapping.

Implicit SSL

An Implicit SSL connection will only start on the specified secure FTP port. The connection automatically starts with an SSL connection.

SSL Protocol

From the drop-down list, select the appropriate option:

- SSL - A traditional Secure Socket Layer protocol is used to secure the transmission
- TLS - A new version of SSL, Transport Layer Security will be used to secure the transmission (default)

Enabled SSL Protocols

Specify a comma separated list of SSL/TLS protocol versions to allow. For example, to enable only TLS 1.1, TLS 1.2, and TLS 1.3, specify TLSv1.1, TLSv1.2, or TLSv1.3. Likewise, to enable all versions of SSL/TLS, specify SSLv3,TLSv1,TLSv1.1,TLSv1.2, TLSv1.3.

Client Authentication

The client authentication option indicates if SSL authentication is expected when a client connects to Managed File Transfer. If a Web User or Web User Template is configured to authenticate using a certificate, the Optional or Required setting should be selected.

- None - Client certificate authentication is not enabled and client certificates will be ignored. Clients must authenticate with their username and password when connecting to the server.
- Optional - Client certificate authentication is enabled, but a certificate is not required. If a valid certificate is available from the client, it will be used for authentication. If a valid certificate is not available, the client must authenticate with their username and password when connecting to the server.
- Required - Client certificate authentication is enabled and a valid certificate is required. A client connection without a valid certificate will be rejected.

Enabled Cipher Suites

By default all Cipher Suites are enabled to provide the most options between different clients and servers. Although encrypted, the cipher suite automatically selected by the connection may not be the most secure. This list allows you to limit which ciphers are used. Follow the instructions below to select which Cipher Suites are used:

1. In the left column, click to select (highlight) the Cipher Suites to use. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.

2. When the desired Cipher Suites are selected, click the arrow between the group boxes to move the Cipher Suites from left to right.

Key Store File

This file contains the private key and associated certificates that a client uses to authenticate to a server. There are default Key Store files provided with Managed File Transfer or you can create your own. Type the name or click the icon to browse for the file.

Key Store Password

The Key Store Password was specified by the person who created the Key Store.

Key Store Type

From the drop-down list, select the appropriate option:

- JKS - Java Key Store
- PKCS12 - Public-Key Cryptography Standards

Key Store Provider

Based on your installation, not all the providers may be available. The correct Key Store Provider is loaded during the installation. If you need specify a provider, select the appropriate option from the drop-down list:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM
- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- SUN - The classic Java cryptographic service
- SUNJSSE - The Java Secure Socket Extension provides an RSA layer to the cryptology
- SUNJCE - The Java Cryptographic Extension is the export compliant variation of the SUN provider
- SUNMSCAPI - The Java implementation of the Microsoft Cryptography API
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509

Key Alias

The key alias identifies a key pair and its associated certificate from all the ones within a Key Store. If no alias is specified, the Key Store opens the first file in the key store. Type the name or click the icon to browse for an Alias.

Export Head Certificate

Exports the head certificate of the selected Key Alias to your internet browser's default download directory.

Key Password

The Key Password was specified by the person who created the Key.

Trust Store File

The Trust Store File contains the public keys and certificates used by a server to authenticate a client. There are default Trust Store files provided with Managed File Transfer or you can create your own. Type the name or click the icon to browse for the file.

Trust Store Password

The Trust Store Password was specified by the person who created the Trust Store.

Trust Store Type

See Key Store Type.

Trust Store Provider

See Key Store Provider.

CCC Enabled

Indicates whether or not Web Users are permitted to use the clear command channel (CCC) command during an encrypted FTPS connection. If a Web User sends the CCC command, it terminates the encryption on the command channel and all subsequent FTPS communication on the command channel will be transmitted in plain text. The encryption of the data channel is not affected by this setting. When selected, the control channel can be switched to plain text. If unselected, the command cManaged File TransferManaged File Transferhannel will remain encrypted.Note: This is useful when Managed File Transfer is behind a NAT firewall that requires plain text commands for routing secondary FTPS data connections.

CCC Send Close Notify

This setting determines whether or not Managed File Transfer will perform the CLOSE_NOTIFY operation as part of the SSL/TLS shutdown when the CCC command is received. Select this option to send the CLOSE_NOTIFY command to properly terminate the SSL/TLS encryption. Some FTPS clients do not support proper termination of SSL/TLS and require this option to be unselected.

Data Connection

The FTP Data Connection is the connection over which data is transferred (sent and received) and is established when a FTP command is issued (for example, GET, PUT, LIST).

The Data Connection has the following settings:

Idle Timeout

The idle time in seconds before the Data Connection will close.

Force Encrypted Data Channels

An encrypted data channel protects the data using implicit SSL. If the client connection to Managed File Transfer does not support an encrypted data channel, the connection will fail. The default setting is No.

Active

The Active connection has the following settings:

Local Address

This is the IP address of the server hosting the port to which Managed File Transfer is listening. If available, you can also select it from the drop-down list.

External Address

The address on which the server will claim to listen for the data port. Useful when the server is behind a NAT firewall and the client sees a different address than the server is using.

Validate IP

This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail. If left blank, the default is No.

Port

The ports on which the server is allowed to accept Passive Data Connections. Multiple port numbers are comma delimited. The text box also accepts ranges separated with hyphens. Ranges and single port numbers can be mixed (i.e. 60000-61000, 61052, 63000-65535). Valid port numbers are from 1 to 65535, however many ports below 1024 are reserved by the operating system and other programs.

Note: If you wish to Delete a Listener entry, select the Listener entry in the left Outline, then click the Delete link in the page toolbar

.

Passive

The Passive connection has the following settings:

Local Address

This is the IP address of the server hosting the port to which Managed File Transfer is listening. If available, you can also select it from the drop-down list.

Enabled

If set to Yes, the Data Connection for the Listener will attempt a traditional FTP connection to establish the data port.

Validate IP

This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail. If left blank, the default is No.

Local Port

The local port on which the server will make the Active Data Connection. If none specified, any available port is used.

MLLP Service

The Minimal Lower Layer Protocol (MLLP) protocol is used to transfer healthcare industry messages, such as HL7 messages. HL7 is a messaging specification for healthcare information systems. The MLLP protocol has a long history of use with HL7 standard messages, although it has never been formally part of the HL7 standard itself. The MLLP protocol is a minimalistic OSI-session layer framing protocol. HL7 is a messaging specification for healthcare information systems.

HL7 Message Handling

When an MLLP client sends a message to the Informatica Managed File Transfer MLLP service, it is required to wait for an HL7 Acknowledgement before sending the next message. The content of the acknowledgement must be examined to determine the specific type of the acknowledgement before the next message can be transmitted.

HL7 Messages are used to transfer electronic data between disparate healthcare systems. Each HL7 message sends information about a particular event such as a patient admission. There are two types of Acknowledgement messages (ACKs) used in healthcare data exchange communications: HL7 ACKs include original mode acknowledgements and enhanced mode acknowledgements, and non-HL7 ACKs, also known as static string acknowledgements.

An HL7 ACK is created with information from the HL7 message, and is in the following HL7 formats.

- Original Mode Acknowledgement: This acknowledgement is a "Receive" ACK. It indicates that a message has been received but not necessarily processed yet.
- Enhanced Mode Acknowledgement: This acknowledgement is an "Application" ACK that is a resultant status return rather than a communication response, such as an order response.

Original Mode Acknowledgements include the following HL7 acknowledgements:

- Application Accept (AA) acknowledgement. The message was accepted without error.
- Application Error (AE) acknowledgement. The message had an error and was rejected.
- Application Reject (AR) acknowledgement. The message was rejected because of an error.

Enhanced Mode Acknowledgement include the following HL7 acknowledgements:

- Application Accept (AA) acknowledgement. The message was accepted without error.
- Application Error (AE) acknowledgement. The message had an error and was rejected.
- Application Reject (AR) acknowledgement. The message was rejected because of an error.
- Commit Accept (CA) acknowledgement. The message was accepted by the backend system.
- Commit Error (CE) acknowledgement. The message had an error and was rejected by the backend system.
- Commit Reject (CR) acknowledgement. The message was rejected in the backend system because of an error.

The MLLP service will send an acknowledgement once it receives the message from client. If the message was accepted without error, it will send AA acknowledgement to the client and save the message in the `userdata/MLLP/ListenerName` folder. The saved message name will be in the format `msg_(Client)IP_(Client)Port_Timestamp`. It will create the service event "`MLLP Message received successfully`".

If the message had validation error and was rejected, it will send an AE acknowledgement to the client and save the message in the `userdata/MLLP/<ListenerName>` folder. The saved message name will be in the format `err_msg_(Client)IP_(Client)Port_Timestamp`. It will create an "`MLLP Message received failed`" service event.

If the message was rejected because of an error such not having write permission to the `userdata/MLLP/ListenerName` directory, it will send AR acknowledgement to the client. It will create an "`MLLP Message received failed`" service event.

MLLP Configuration

The following section describes the Preferences and Server settings.

Preferences Properties - General Properties

Automatically Start Service

Specify whether you would like to start the service automatically when Managed File Transfer starts.

Server Properties - Listener Properties

Name

Providing an identifiable name for the Listener helps identify it in the Configuration Outline list.

Port

Set the port number that the Listener will monitor for connections.

Local Address

This is the IP address of the server hosting the port to which Managed File Transfer listens.

Idle Timeout

The idle time in seconds before the Listener will timeout.

Message Validation

Specify whether to activate message validation.

Acknowledgement Mode

Specify whether to apply Original Mode Acknowledgements or Enhanced Mode Acknowledgements. If you select Enhanced Mode Acknowledgements, define the following settings:

Project

Select a Project that describes the work for Managed File Transfer to perform.

User

The User Name is not case sensitive and can not exceed 20 characters.

Password

Passwords are case sensitive and can contain numbers and characters up to 20 characters.

Is Password Encrypted

Specify if the password is encrypted.

Variables

Define variables to use with the Project. Variables can be used in Projects to supply input values to their attributes.

Note that you can start or stop individual listeners. You must save the edits made to the listener configuration before you start or stop the listener. Also, the MLLP protocol does not require authentication, so no Web User setup is necessary or available for the MLLP protocol.

SFTP Service (FTP over SSH)

The traditional FTP protocol sends cleartext commands and data over the network. The data could be intercepted, viewed, and altered by an attacker before sending it to the receiver.

If you send sensitive data over the network, you might want to consider the SFTP protocol for securing data.

SFTP creates an encrypted tunnel between two computer systems and protects against the following attacks:

- IP spoofing, where a remote host sends out packets that pretend to come from a trusted host
- IP source routing, where a host can pretend that an IP packet comes from another trusted host
- DNS spoofing, where an attacker forges the name server records
- Interception of cleartext passwords and other data by intermediate hosts
- Manipulation of data by attackers in control of intermediate hosts

SFTP uses a combination of asymmetric cryptology and symmetric cryptology to provide a strong encryption and optimal performance.

SFTP is supported by most commercial servers and many open source servers, for example, Linux. SFTP can be used for transmitting large files because SFTP compresses the data stream prior to encryption.

Managed File Transfer implements the most current SSH 2.0 protocol standard.

Quick Start for SFTP

Configuration

1. Configure the SFTP server. For more information, see "SFTP Server Configuration" on page 551.
2. Start the SFTP server.

SSH Key Authentication

Perform the following steps to get authenticated using an SSH key:

1. Have your trading partner send you their SSH Public key.
2. Import the SSH Public key for the Web User.
3. Change the Web User's Authentication Type:
   a. From the Dashboard, point to Security and then click **Web User**.
   b. On the Web Users page, click the icon next to the Web User.

c. In the Edit Web User page, click the Authentication tab and change the SFTP Authentication Type to Public Key.

d. Click the **Save** button.
When the SFTP client connects to the server, it looks up the client's Public Key in the `[installdirectory]/userdata/keys/ssh` directory based on the Web User name. The Web User authenticates if the Public Key matches the Public Key sent by the client.

SFTP Server Configuration

The SFTP Server Configuration page provides the configuration options for the SFTP Service. From this page, modify or add service parameters, for example, login parameters, port numbers, and listeners.

After upgrading to Managed File Transfer 10.5.0 version, a warning message appears with a list of unsupported algorithms if they were selected before the upgrade. Save the configuration to proceed. Saving the configuration deletes the unsupported algorithms.

Preferences

The following sections describe the Preferences settings.

General

Automatically Start Service

Specify whether you would like to start the SFTP service automatically when Managed File Transfer starts.

Upload Restrictions

Restrict Uploads to Inbound Directory

When selected, uploads are restricted to the inbound directory and sub-directories. Web Users will not be able to upload files to any directory other than "Inbound." This option should not be selected if Web Users need to upload files in other locations or if Inbound and Outbound folders were not created.

Note: This option is no longer available and will only be visible if it was in use prior to Managed File Transfer version 3.0.0. It is recommended to use "Virtual Folders and Files" on page 586 to control Web User file and folder access.

Allow Files with No Extension

When selected, Web Users can upload files that do not have extensions.

Allow Files with an Extension

This option enables the File Extension Filter.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or only permit specific extensions. If you want to specify the file types Web Users can or cannot upload, type each file extension in this box. Type all extensions without periods (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type txt,xls,xlsx,csv). The maximum number of characters for this field is 2000.

Server

The following sections describe the Server settings.

Maximum Logins

This is the maximum number of sessions allowed to the service at any given time.

Login Failure Delay

The length of time in seconds a Web User must wait before they can retry their login. This delay not only gives the Web User time to think about their User Name and Password, but it also will deflect multiple login attempts in fast succession from an organized online attack.

Maximum Login Failures

This value represents the number of failed login attempts before the SFTP connection is closed.

Idle Timeout

The idle time in seconds before the connection will timeout.

SCP Enabled

When you enable the **SCP Enabled** option, Managed File Transfer provides Secure Copy (SCP) support for secure file exchange with a client using SCP. SCP is like SFTP, using FTP over SSH.

Enabled Cipher Algorithms

The Cipher Algorithms in the left column are available, the ones in the right column are enabled. By default, all Cipher Suites are enabled to provide the most options between different clients and servers. Although encrypted, the Cipher Suite automatically selected by the connection may not be the most secure.

Perform the following steps to enable Cipher Algorithms:

1. On the left side of the page, click to select the Cipher Algorithm to enable the Cipher Algorithm. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
   The following entries are set as defaults in Managed File Transfer:
   - aes192-ctr
   - aes128-ctr
   - arcfour256

- aes256-cbc
- 3des-cbc
- 3des-ctr
- aes192-cbc
- aes128-cbc
- blowfish-cbc
- arcfour128
- arcfour
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- chacha20-poly1305@openssh.com
- aes256-ctr

2. Click the → arrow between the group boxes to move the algorithms from left to right.
3. Perform the following steps to disable Cipher Algorithms:

   On the right side of the page, click to select the Cipher Algorithm to disable the Cipher Algorithm. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
4. Click the ← arrow between the group boxes to move the algorithms from right to left.

Enabled Mac Algorithms

The SSH transport layer handles algorithm negotiation between the server and client over TCP/IP. Negotiation begins when the SSH client and server send each other textual information that identifies their SSH version. If they both agree that the versions are compatible, the client and server exchange lists that specify the algorithms that they support for key exchange, encryption and data integrity via a message authentication code (MAC). These lists are protected by their own encryption algorithms. The Mac Algorithms in the left column are available, the ones in the right column are enabled.

Perform the following steps to enable Mac Algorithms:

1. On the left side of the page, select the Mac Algorithm that you want to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
   The following entries are set as defaults in Managed File Transfer:
   - hmac-sha2-512-etm@openssh.com
   - hmac-sha2-512-96
   - hmac-sha2-512
   - hmac-sha2-256-etm@openssh.com
   - hmac-sha2-256
   - hmac-sha2-256-96
   - hmac-sha1-etm@openssh.com
   - hmac-sha1
   - hmac-sha1-96
   - hmac-md5
   - hmac-md5-etm@openssh.com

- hmac-md5-96

Note: After upgrading to Managed File Transfer 10.5.0 version, a warning message appears with a list of unsupported algorithms if they were selected before upgrade. You must save the configuration to proceed. Saving the configuration deletes the unsupported algorithms.

The Managed File Transfer 10.5.0 version does not support the following algorithms:

- hmac-sha256@ssh.com
- hmac-sha256
- hmac-sha512
- hmac-sha512@ssh.com
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- hmac-ripemd160-etm@openssh.com

2. Click the → arrow between the group boxes to move the algorithms from left to right.
   Perform the following steps to disable Mac Algorithms:
3. On the right side of the page, select the Mac Algorithm that you want to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
4. Click the ← arrow between the group boxes to move the algorithms from right to left.

Enabled Compression Algorithms

Compression Algorithms help shrink the file size during transport to reduce the transfer time and bandwidth used. The Compression Algorithms in the left column are available, the ones in the right column are enabled.

Perform the following steps to enable Compression Algorithms:

1. On the left side of the page, select the Compression Algorithm that you want to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
   The following entries are set as defaults in Managed File Transfer:
   - none
   - zlib
2. Click the → arrow between the group boxes to move the algorithms from left to right.
   Perform the following steps to disable Compression Algorithms:
3. On the right side of the page, click to select the Compression Algorithm that you want to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
4. Click the ← arrow between the group boxes to move the algorithms from right to left.

Enabled Key Exchange Algorithms

The Key Exchange Algorithms in the left column are available, the ones in the right column are enabled. By default all Key Exchange Suites are enabled to provide the most options between different clients and servers. Although encrypted, the key exchange suite automatically selected by the connection may not be the most secure. This list allows you to limit which key exchanges are used. Follow the instructions below to select which key exchange Algorithms are used:

Perform the following steps to enable key exchange Algorithms:

1. On the left side of the page, click to select (highlight) the key exchange Algorithm(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.

The following entries are set as defaults in Managed File Transfer:

- curve25519-sha256
- rsa2048-sha256
- curve25519-sha256@libssh.org
- rsa1024-sha1
- diffie-hellman-group18-sha512
- diffie-hellman-group17-sha512
- diffie-hellman-group16-sha512
- diffie-hellman-group15-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp521
- ecdh-sha2-nistp384
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- ecdh-sha2-nistp256

2. When the desired key exchange Algorithms are selected, click the → arrow between the group boxes to move the algorithms from left to right.
   Perform the following steps to disable key exchange Algorithms:
3. On the right side of the page, click to select (highlight) the key exchange Algorithm(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
4. When the desired key exchange Algorithms are selected, click the ← arrow between the group boxes to move the algorithms from right to left.

Welcome Message

The welcome message is displayed during the SSH handshake when a client connects using SFTP. Not all SFTP clients display the Welcome Message.

Software Version

The software name or version is exchanged with a client during the initial SFTP connection. The value in this field cannot contain whitespaces. The default value is Managed File Transfer followed by the installed version number.

Comments

The comments field is used for a custom message that is sent along with the software version and connection string to a Web User when they authenticate.

Listener

The following sections describe the Listener settings.

Name

Providing an identifiable name for the Listener helps identify it in the Configuration Outline list.

Port

Set the port number that the Listener will monitor for connections.

Note: If using Managed File Transfer Gateway, any changes to the Port number will also need to be updated on the "Configure the Gateway Parameters" on page 559 page for the related Service Mappings.

Local Address

This is the IP address of the server hosting the port to which Managed File Transfer is Listening. If available, you can also select it from the drop-down list.

Note: If using Managed File Transfer Gateway, any changes to the Local Address will also need to be updated on the "Configure the Gateway Parameters" on page 559 page as the "To Address" for the SFTP Service Mapping.

Host Keys

RSA and DSA keys are used for authenticating a user on a server. RSA keys are typically limited to use within the United States and DSA keys are used world wide.

RSA Key File

The default RSA key files provided with Managed File Transfer. You can use the default RSA key files or create your own RSA key files. Type the file name or click the  icon to browse for the file.

RSA Key Passphrase

The RSA Passphrase was specified by the person who created the passphrase.

DSA Key File

The default DSA key files provided with Managed File Transfer. You can use the default DSA key files or create your own DSA key files. Type the file name or click the  icon to browse for the file.

DSA Key Passphrase

The DSA passphrase was specified by the person who created the passphrase.

Note: If you want to delete a Listener entry, click the Listener entry in the left menu, then click the  Delete link in the page toolbar.

Service Manager Actions

- Edit the Configuration settings for a Service by clicking the  icon.
- Start a Service by clicking the  icon.
- Stop a Service by clicking the  icon. Any active sessions will be terminated for the service.
- Restart a Service by clicking the  icon. Any active sessions will be terminated for the service.
- View the list of Web Users currently active for a service by clicking the "Active Sessions" on page 564 link.

  Note: The last column on the right displays the number of Active Sessions for each Service. Every time a client makes an initial connection, a session is created. If the session count is zero (0), it is safe to Stop or Restart the Service. Click the number in the Active Session column to open the "Active Sessions" on page 564 page to view the active Web Users for that service.

Add a Listener

1. From the main menu bar, select **Services** and then click the **Service Manager**link.
2. In the **Service Manager** page, click the  icon beside the required Service.
3. On the <Protocol> Server page, click the  Server link in the FTP Configuration pane.
4. Click the  Add Listener link in the toolbar to add a new Listener
5. In the Configuration Outline, click an entry to view, modify or delete various settings.
6. Click the **Save** button to save the changes and stay on this page or click the **Save And Finish** button to add or update the Listener and return to the Service Manager page.

Setting Up Managed File Transfer Gateway for Reverse Proxy

You can configure Informatica Managed File Transfer Gateway as a reverse proxy. When you use Informatica Managed File Transfer Gateway as a reverse proxy, the Informatica Managed File Transfer Gateway does not open the inbound ports into the internal network and does not store sensitive data in the DMZ.

Informatica Managed File Transfer Gateway Features

Informatica Managed File Transfer Gateway includes the following features:

- Load balancing when multiple Managed File Transfer systems are running in a clustered configuration.
- Incoming ports are not opened into the private network.
- Files are not stored in the DMZ.
- User credentials and permissions are maintained and stored on the private network.

- Service configurations are maintained and stored on the private network .
- Supports FTP/s, SFTP, HTTPs, and MLLP file transfer protocols.
- Available as a software-only solution.
- Installs on Windows, Linux, AIX, UNIX, and Solaris operating systems.

How it Works

At initial startup, Managed File Transfer opens an outbound connection (control channel) from the private network to Managed File Transfer Gateway (Gateway) in the DMZ. This proprietary control channel is used to pass commands and messages between the products.

Once the proxy IP and port mappings are received from Managed File Transfer, then Gateway will start listening for connections on those IP addresses and ports. When an external client connects to a listener on Gateway, it notifies Managed File Transfer over the control channel. At that point, Managed File Transfer creates a new outbound connection (called a "data channel") to Gateway. This data channel is attached to the desired service (e.g. FTP/s, SFTP, HTTP/s) and all traffic (client authentication requests, data, commands, etc.) are routed over this new data channel. Gateway is monitored and configured on the "Add a New Gateway Configuration" on page 558 page.

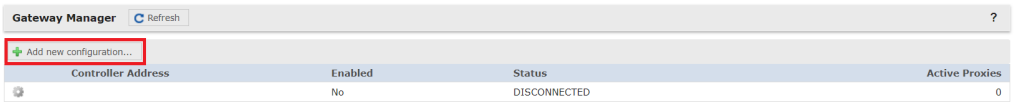
Informatica Managed File Transfer Gateway serves as a transparent interface between external clients (trading partners) and Managed File Transfer without exposing the private network to those clients. This is an essential solution for securing confidential data and complying with state privacy laws, HIPAA, PCI DSS, SOX and GLBA.

Add a New Gateway Configuration

Use the Gateway Manager to control the Managed File Transfer Gateway connection and view the current status of the Managed File Transfer Gateway. When Managed File Transfer is running in a cluster configuration, the service mappings for each system in the cluster are displayed in the Gateway Manager.

Perform the following steps to add a new Gateway configuration:

1. To manage the Managed File Transfer Gateway, log in as an Admin User with the **Product Administrator** role.
2. From the main menu bar, select **Services** and then click **Gateway Manager**.
   The following image shows the **Gateway Manager** page:



3. Add a new Gateway configuration by clicking the **Add new configuration** link.

Page Toolbar

You can perform the following actions from the Page Toolbar:

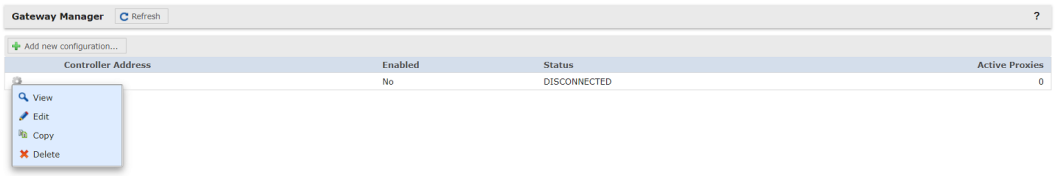
- Add a new Gateway configuration by clicking the **Add new configuration** link. For more information, see "Configure the Gateway Parameters" on page 559.
- Disable a Gateway connection by clicking the Disconnect Gateway icon. Click the Connect Gateway icon to establish a connection again. The status field displays the current connection status. View the **Gateway Details** for more connection information. For more information on **Gateway Details**, see "Gateway Details" on page 564.

Gateway Manager Actions

You can perform the following actions by selecting the Actions icon:

- View Gateway Details by clicking the icon. For more information, see "Gateway Details" on page 564.
- Edit a Gateway by clicking the icon (the Gateway must be disabled to edit the configuration). For more information, see "Configure the Gateway Parameters" on page 559.
- Copy a Gateway by clicking the icon. For more information, see "Configure the Gateway Parameters" on page 559.
- Delete a Gateway by clicking the icon (the Gateway must be disabled to delete the configuration).

The following image shows the gateway manager actions:



Configure the Gateway Parameters

The Gateway Configuration page contains the operating parameters and service mappings for Managed File Transfer Gateway.

Configure the Gateway parameters and service mappings for Managed File Transfer Gateway.

The following table describes the Gateway Configuration parameters:

Gateway Configuration parameter	Description
Enabled	Indicates whether Informatica Managed File Transfer Gateway is enabled. By default, Informatica Managed File Transfer Gateway is disabled.
Automatically Start	Indicates whether Informatica Managed File Transfer Gateway connection is started automatically when Informatica Managed File Transfer starts.
Controller Address	The IP address of the server running the Informatica Managed File Transfer Gateway server component. The IP address must match the controller address defined in the `gateway.xml` file on the Informatica Managed File Transfer Gateway server.
Controller Port	The port on which Informatica Managed File Transfer Gateway listens for incoming control connections. The default port is 9100 and must match the port defined in the `gateway.xml` file on the Informatica Managed File Transfer Gateway Server.
Minimum Number of Threads	The minimum number of threads reserved for connections to Informatica Managed File Transfer Gateway. Default is 10.

Gateway Configuration parameter	Description
Maximum Number of Threads	The maximum number of threads that can be used for connections to Informatica Managed File Transfer Gateway. This determines the maximum number of simultaneous requests that can be handled. Default is 500. **Note:** Changing the thread values can alter the performance. Modify the thread values to obtain the optimal performance for your configuration requirements.
Thread Keep Alive Time	The amount of time that an idle thread waits before it is released. Default is 60 seconds. **Note:** Increasing the value might cause a higher CPU and memory usage on the server. However, the connections start faster because they do not need to create new threads frequently.

Gateway Configuration parameter	Description
Service Mappings	Each service such as IFTP, FTPS, HTTPS, and SFTP is mapped from Informatica Managed File Transfer Gateway to the corresponding service in Informatica Managed File Transfer. When a control connection is established, the mappings are sent to the Informatica Managed File Transfer Gateway server. Informatica Managed File Transfer Gateway listens for incoming connections on the **From Address** and **From Port** for each service mapping. When a connection occurs, Informatica Managed File Transfer Gateway forwards the traffic to Informatica Managed File Transfer based on the **To Address** and **To Port** service mappings. If more service mappings are needed, for example, more than one listener for a particular service, click the **Add Service Mapping** link to add a new service mapping entry row. If a service mapping is no longer needed, click the icon to delete the corresponding service mapping.
Add service mapping	The Add service mapping contains the following parameters: **Label** An identifier for the service mapping. **From Address** The IP address that Managed File Transfer Gateway uses to listen on for incoming traffic. Optionally leave the From Address field blank to use the Controller Address as the bind address for client connections on that particular mapping. **From Port** The port that Managed File Transfer Gateway uses to listen on for incoming connections. The standard ports are 21 for FTP, 990 for FTPS, 22 for SFTP, and 443 for HTTPS/AS2. **To Address** The IP address of the local Managed File Transfer system. **To Port** The port that the service listener uses for a specific service on the Managed File Transfer system. **Load Balancer Rule** The Managed File Transfer Gateway uses the Load Balancer Rule to configure the load balancing for each service mapping. This rule is defined in Managed File Transfer Gateway and should be round-robin for FTP, FTPS, and SFTP protocols. For HTTPS, the Load Balancer Rule should be IP-based round-robin that routes traffic from specific IP addresses for a period of time to a single system. By default, use the `default` rule for FTP, FTPS and SFTP. Use the `https` rule for HTTPs and AS2. Changes made to the Service Mappings take effect the next time the connection to the Managed File Transfer Gateway is reset. To reset the connection, click the **Disconnect** button and then the **Connect** button on the **Gateway Manager** page. For more information, see "Add a New Gateway Configuration" on page 558.

The following image shows the **Gateway Configuration** page:

Enabled

Informatica Managed File Transfer Gateway can be enabled or disabled. By default, Managed File Transfer Gateway is disabled.

Automatically Start

Specify if you would like to start the Managed File Transfer Gateway connection automatically when Managed File Transfer starts.

Controller Address

The Controller Address is the IP address of the server running the Managed File Transfer Gateway server component. This address must match the controller address defined in the `gateway.xml` file on the Managed File Transfer Gateway server.

Controller Port

This is the port on which Managed File Transfer Gateway listens for incoming control connections. The default port is 9100 and must match the port defined in the `gateway.xml` file on the Managed File Transfer Gateway Server.

Minimum Number of Threads

The minimum number of threads reserved for connections to Managed File Transfer Gateway. Default is 10 threads.

Maximum Number of Threads

The maximum number of threads that can be used for connections to Managed File Transfer Gateway. This determines the maximum number of simultaneous requests that can be handled. Default is 500 threads.

Note: Changing the thread values can alter the performance. Modify the thread values to obtain the optimal performance for your configuration requirements.

Thread Keep Alive Time

The amount of time that an idle thread will wait before it is released. Default is 60 seconds.

Note: Increasing the value might cause a higher CPU and memory usage on the server. However, the connections start faster because they do not need to create new threads frequently.

Service Mappings

Each service such as IFTP, FTPS, HTTPS, and SFTP is mapped from Managed File Transfer Gateway to the corresponding service in Managed File Transfer. When a control connection is established, the mappings are sent to the Managed File Transfer Gateway server. Managed File Transfer Gateway listens for incoming connections on the **From Address** and **From Port** for each service mapping. When a connection occurs, Managed File Transfer Gateway forwards the traffic to Managed File Transfer based on the **To Address** and **To Port** service mappings. For more information on establishing a connection and the mapping process, see "Setting Up Managed File Transfer Gateway for Reverse Proxy" on page 557.

If more service mappings are needed, for example, more than one listener for a particular service, click the **Add Service Mapping** link to add a new service mapping entry row. If a service mapping is no longer needed, click the  icon to delete the corresponding service mapping.

Service Mapping Columns

The Service Mapping Columns contain the following parameters:

Label

An identifier for the service mapping.

From Address

The IP address that Managed File Transfer Gateway uses to listen on for incoming traffic. Optionally leave the **From Address** field blank to use the Controller Address as the bind address for client connections on that particular mapping.

From Port

The port that Managed File Transfer Gateway uses to listen on for incoming connections. The standard ports are 21 for FTP, 990 for FTPS, 22 for SFTP, and 443 for HTTPS/AS2.

To Address

The IP address of the local Managed File Transfer system.

To Port

The port that the service listener uses for a specific service on the Managed File Transfer system.

Load Balancer Rule

The Managed File Transfer Gateway uses the Load Balancer Rule to configure the load balancing for each service mapping. This rule is defined in Managed File Transfer Gateway and should be round-robin for FTP, FTPS, and SFTP protocols. For HTTPS, the Load Balancer Rule should be IP-based round-robin that routes traffic from specific IP addresses for a period of time to a single system.

By default, the following rules are defined in the Managed File Transfer Gateway.

default

Use this rule for FTP, FTPS and SFTP.

https

Use this rule for HTTPS and AS2.

Note: AS2 (S/MIME over HTTP(S)) uses the HTTPS Service.

Changes made to the Service Mappings will take effect the next time the connection to the Managed File Transfer Gateway is reset.

To reset the connection, click the **Disconnect** button and then the **Connect** button on the **Gateway Manager** page. For more information, see "Add a New Gateway Configuration" on page 558.

Gateway Details

The view **Gateway Manager** page displays the current details for the selected Gateway connection. Click the **Done** button to return to the **Gateway Manager** page.

For more information, see "Add a New Gateway Configuration" on page 558.

Available Options

Configure the Managed File Transfer Gateway settings by clicking the **Configure Gateway** link in the page toolbar. For more information, see "Configure the Gateway Parameters" on page 559.

Control the connection to the Managed File Transfer Gateway by clicking the Actions button. The button toggles based on the following connection status:

- Disconnect - Stops Managed File Transfer Gateway and releases all proxies.
- Connect - Starts Managed File Transfer Gateway and establishes proxy connections.

Active Sessions

The Active Sessions page displays the Web User sessions that are connected to the Managed File Transfer server.

To access the Active Sessions page, log in as an Admin User with the Product Administrator role.

From the main menu bar, select **Services** and then click the **Active Sessions**link.

The following details are shown for each active session on the page:

- System - The system (within a cluster) to which the connection was made.
- Protocol - The transfer method being used by the Web User (note that FTPES is Explicit FTP and is displayed when the FTP Service is selected).
- Connected Since - The date and time when the Web User connected to Managed File Transfer.
- User - The account name of the authenticated Web User.
- Device - The ID of the device associated to the session.
- Remote Address - The IP address of the Web User's system.
- Gateway - If the box displays a checkmark, this connection is passing through Managed File Transfer Gateway.
- Local Address - The IP address of the Managed File Transfer listener to which the session is connected.
- Local Port - The port on the Managed File Transfer listener that is accepting the connection.
- Bytes Sent - The number of bytes sent or downloaded from Managed File Transfer to the Web User.
- Bytes Received - The number of bytes received or uploaded by Managed File Transfer from the Web User.

Active Sessions Available Options

The Active Sessions page has the following options:

System

From the drop-down list, select the system (within a cluster) to view the Active Sessions for. This option is only available when clustering is enabled.

Services

Select which protocols to display the active sessions for. Changing the service selections automatically refreshes the list.

Auto Refresh

The Active Session list automatically refreshes every 5 seconds. If the Auto Refresh option is disabled, click the **Refresh** button to refresh the Active Session list manually.

Terminate

Click the Terminate icon to terminate a session.

View

Click the View icon to view the "Session Log" on page 565 for the session.

Each Shared Drive device will maintain a constant connection with Managed File Transfer for event notifications and processing. If there are a large number of devices in your organization synchronizing with Shared Drive, it is recommended to set up Managed File Transfer in a "Clustering" on page 772 environment.

Note: Bytes Sent and **Bytes Received** values are not available for sessions for the HTTPS and AS2 service. Additional activity information for these services is available in the Chapter 8, "Logs and Reports" on page 659.

Session Log

The Session Log displays the current audit log details for the selected active session. The session information is displayed at the top of the page and the activity details are listed in the bottom section. Click the **Refresh** button to refresh the session log and click the **Back** button to return to the "Active Sessions" on page 564 page.

Note: The list is shown in descending order by Date/Time.

Shared Drive

The Shared Drive module in Managed File Transfer is a secure on-premise file sharing and synchronization service. All of your Web User's images, documents, videos, and sensitive files are stored on the Managed File Transfer server which your organization controls. Files and folders a Web User adds to Shared Drive will automatically sync through the server and appear on each of their registered devices, as well as the File Transfer Portal, allowing Web User's to access their files from any internet connected computer. With Shared Drive, Web User's can quickly and securely share files and collaborate with team members or trading partners.

Shared Drive Features at a Glance

- Drag and drop files from the desktop directly on to the Shared Drive page
- Restore previous file revisions
- Restore files from the trash bin
- Lock files to prevent shared users from editing or deleting them
- Specify comments on files
- View popular media types in the Media Viewer
- Search for files and folders
- When a file is uploaded to Shared Drive, it is automatically encrypted on the disk with AES 256-bit encryption. When accessed from an authorized Web User, Managed File Transfer automatically decrypts the file while it is being accessed.
- All Web User activity is recorded in the "Shared Drive Log" on page 672. A Web User can also view logs pertaining to Shared Drive transactions via the Shared Drive Activity Stream available on the File Transfer Portal.

Shared Drive Prerequisites

The following Shared Drive settings must be defined:

HTTPS Service

The "Service Manager" on page 516 must be running, since the Shared Drive module is only accessible from the HTTPS File Transfer Portal.

Site URL

The external Web address for Managed File Transfer must be specified in the File Transfer Portal section of the "HTTPS Configuration" on page 521.

Permissions

A Web User must have the Shared Drive Feature enabled on their account or be a member of a Web User Group that has the Shared Drive feature enabled to be able to use the Shared Drive interface.

Shared Drive Settings

The options on the Shared Drive Settings page control the functionality of the "Shared Drive" on page 565 interface, device registration, Media Viewer settings, and thumbnail settings.

To configure Shared Drive settings, log in as an Admin User with the Shared Drive Manager role.

From the main menu bar, select **Services**, and then click the **Shared Drive Settings**link.

General

The General tab has the following options:

Shared Drive Enabled

The Shared Drive function in Managed File Transfer is a secure on-premise file sharing and synchronization service. When selected, a Shared Drive menu option is available to Web Users from the HTTPS File Transfer Portal menu bar.

Note: When running in a clustered environment, Shared Drive cannot be enabled until you configure the Index Directory path and the Shared Drive Directory path to use absolute paths. The Shared Drive and Index directories cannot use SMB shares.

Shared Drive Directory

This is the location where the encrypted Shared Drive file system is stored. By default, the location of the Shared Drive directory is relative to the Managed File Transfer installation directory. If Managed File Transfer is installed in `/informatica/B2B/MFT/server`, then the default location for the documents directory is `/informatica/B2B/MFT/server/userdata/shareddrive`. Click the  icon to browse for a different folder on the server.

When Managed File Transfer is running in a cluster configuration, the Shared Drive Directory must point to a shared or mapped folder location on the network.

Note: All files in Shared Drive are stored in a proprietary folder structure and are encrypted using AES 256-bit encryption. Hence, these files cannot be accessed outside of Managed File Transfer.

Limit Disk Space

Every file that is uploaded to Shared Drive may contain multiple revisions and thumbnails, which are stored in the Shared Drive Directory. It is recommended to set a maximum limit of disk space that is allocated to Shared Drive to prevent the disk from running out of space. You will be unable to upload files when the maximum limit has been reached, but you will still retain the ability to download and view files from Shared Drive.

Maximum Disk Space

The maximum amount of disk space available for Shared Drive.

Days to Keep Files

Specify the number of days to keep files in the trash bin of the Shared Drive before they are permanently deleted.

Max Stored Revisions

Shared Drive saves a file revision every time a file is uploaded, saved on the desktop sync client, or overwritten. Web Users have the ability to restore previous revisions of files. Specify the number of revisions that can be retrieved from the server by the Web User.

Email From Address

Shared Drive email notifications are sent to the recipient of file and folder shares. The From Address can be set to the address of the Web User who shared the item or as the main Managed File Transfer email account set on the **SMTP tab** of the global settings. When using the Sender's Address option, check with your SMTP Administrator to verify the email account defined in Global Settings is able to send emails using different From Addresses.

Email Notifications Allowed

When a Web User shares a file with another Web User, they can request email notifications be sent to them when the other party uploads revisions, downloads, locks, or deletes the file. When an email notification is sent, the From Address specified in the **Email From Address** field is used.

Notification Frequency

Specify the frequency the server will send Shared Drive email notifications to Web Users.

Note: To minimize the impact on server resources, the **Immediately** option sends email notifications on a 30 second interval.

Media Viewer

The following options are available:

Media Viewer Enabled

Enable the Media Viewer on the File Transfer Portal, which allows viewing images and PDFs through the browser, without the need to download them first.

Supported File Types

Choose which media file types will display in the media viewer.

Media Viewer Preferred

Choose the default click action for media files in Shared Drive. When the Media Viewer Preferred option is enabled, clicking on media files in Shared Drive will preview those files in the Media Viewer. When this option is not enabled, clicking a media file in Shared Drive will download the file to the Web User's computer.

Thumbnails

Shared Drive can display thumbnail previews for images. This is useful for helping Web Users to quickly find the images they are looking for. Thumbnail generation adds extra processing overhead to a Managed File Transfer server.

The following options are available:

Thumbnails Enabled

Thumbnails previews will be generated when files are uploaded to Shared Drive.

Supported File Types

Choose which media file will generate a thumbnail preview.

Secure Mail

The Secure Mail option in Managed File Transfer provides authorized Web Users with the ability to send ad-hoc messages. These messages contain a unique link that the recipient can use to securely download files. Package activity and the Secure Mail settings are managed within Managed File Transfer. The Secure Mail interface is available to authorized Web Users in the HTTPS File Transfer Portal.

A Package can be sent to multiple recipients. Each recipient receives a unique link to the Package for downloading its contents. The "Web User Email Templates" on page 812 used to create the message sent to the recipient can be modified as needed.

Several settings are available for Secure Mail packages that can limit the number of times each file can be downloaded per recipient, package expiration, and password protection options. Certified Delivery can be enabled to ensure only registered Web Users can access the package through their Inbox. The Secure Mail Outlook® Plugin can also have default options configured from the Secure Mail Settings. These options include, prompting to send an email containing attachments with Managed File Transfer Secure Mail or when an attachment is automatically sent using Managed File Transfer Secure Mail based on file size.

There are no limits to the number of files that can be sent using the Secure Mail interface. The size per file is limited by the HTTPS upload size setting on the HTTPS tab of the "HTTPS Configuration" on page 521.

Secure Mail At A Glance

Secure Mail has the following key components and features:

Packages

Files that are sent through Secure Mail are stored by Managed File Transfer under a “Packages” folder on your network. The Packages folder location is defined in “Global Settings” on page 752 on the Data tab. Individual packages are organized into subfolders based on their creation date and package id (a 36-character UUID). A typical path to a package folder will be constructed as: [installdirectory]/userdata/packages/[creationdate]/[PackageID]. When a recipient downloads their Secure Mail files through the HTTPS link, those files are retrieved from that package folder on your network.

Encryption

When a Secure Mail Package is created, the message and files in the Package are automatically encrypted on the disk with a unique encryption key and the AES 256-bit cipher to protect the privacy of the data. When accessed from an authorized recipient, Managed File Transfer automatically decrypts the message and files within the Package while it is being accessed. The Package message and files will remain encrypted on your network until they are purged.

Package Mailer

The Package mailer will make three attempts (in 60 second intervals) to deliver a Secure Mail message to each recipient. If the HTTPS service or the Managed File Transfer server is shutdown for any reason, the Package mailer will re-send messages that were in the process of being sent.

Logs

All Web User, Package, file and recipient activity is recorded in the “HTTPS Log” on page 674. Purging events are recorded in the “Server Log Viewer” on page 671. A Web User can also view logs pertaining to the messages they send in the Secure Mail interface via the HTTPS Client.

Purging

A daily process checks for inactive packages and deletes them from the server. If a Web User account is deleted, all packages associated with that account will be set to inactive and deleted as part of the purge process. Purge options are configured on the Secure Mail tab in the “Log Settings” on page 693.

Secure Mail Prerequisites

- HTTPS ServiceThe “Service Manager” on page 516 must be running, since the Secure Mail module is only accessible from the HTTPS File Transfer Portal.
- Site URLThe external Web address for Managed File Transfer must be specified on the File Transfer Portal tab of the “HTTPS Configuration” on page 521.
- Secure MailThe Secure Mail option in “Secure Mail Settings” on page 569 must be enabled.
- PermissionsA Web User must have the Send Secure Mail permission enabled on their account or be a member of a Web User Group that has the Send Secure Mail permission enabled to be able to use the Secure Mail interface. Additionally, a Web User must have "Upload" permission to attach files to a Package from their local computer and have "List" permission to attach a file from a workspace.

Secure Mail Settings

The options on the Secure Mail Settings page control the functionality of the “Secure Mail” on page 568 interface.

To configure Secure Mail settings, log in as an Admin User with the Secure Mail Manager role.

From the main menu bar, select **Services**, and then click the **Secure Mail Settings**link.

General

The options on the General tab apply to Web Users and the Managed File Transfer Secure Mail plugin for Outlook®.

The following options are available:

Secure Mail Enabled

The Secure Mail function in Managed File Transfer sends messages to recipients via email with a link where they can securely download files or view messages. When selected, a Secure Mail menu option is available to Web Users from the HTTPS File Transfer Portal "Quick Start for HTTPS" on page 517.

Email From Address

When emails are sent to recipients of a Package, the From Address can be set to the address of the Web User composing the Package or as the main Managed File Transfer email account set on the SMTP tab of the "Global Settings" on page 752. When using the Sender's Address option, check with your SMTP Administrator to verify the email account defined in Global Settings is able to send emails using different From Addresses.

Default Subject

The default subject that will be populated in the subject line when composing a new message. The default subject cannot exceed 255 characters.

Protection Level

All packages are protected by a unique URL which is sent to the recipient via email. A password can be added to each Package, requiring the recipient to click the link and then type a password before the Package can be opened. When Certified Delivery is enabled, Web Users will be given an option to require recipients to register before they can access the message. Certified Delivery messages can be accessed from the Web User's Inbox in the File Transfer Portal.

Password Generation

If the Package is also protected with a password, the password can be generated automatically by Managed File Transfer or it can be Manually Specified. Passwords generated automatically are 10 lowercase alpha-numeric characters.

Include Password In Email

The password to open the Package can be included in the email, sent in a separate email, or it can be communicated manually. If the password is generated automatically and not sent in the message, it will be displayed on the page when the package is sent. The password is also found by opening the Sent Items page and viewing the details for the message.

Package Expiration

Indicates if the Package will expire after the specified number of days. Recipients will no longer have access to the Package after this point. If selected, a range must be set between 1 and 999 days.

Maximum Downloads

While the Package is active, a recipient can download the file more than once based on the maximum downloads setting. This setting is per file, per recipient. If selected, a range must be set between 1 and 999 downloads. The default, if specified, is displayed when the Web User is composing a message.

Note: If the total number of Maximum Downloads is reached for each file in a Package, the Package is automatically set to inactive.

Reply

Indicates if recipients of URL and Password Protected packages are allowed to reply back to the sender. One or more attachments along with an optional message can be included in the reply. Recipients do not need to be registered users to send replies, but recipient email addresses must be permitted in the Address Rules. Setting the Default option to 'Yes' automatically allows replies to messages.

Address Rules

The Address Rules tab allows you to configure email patterns that will allow or restrict Web Users from sending Secure Mail to certain email addresses.

Add a Rule

Click the Add a Rule link to add a new email pattern to the list.

Note: Email pattern rules will be evaluated from the top to the bottom of the list when determining if the email can be sent.

Actions

The following actions are available for each rule:

- Click the  icon to delete rule.
- Click the  icon to move the rule up in the list.
- Click the  icon to move the rule down in the list.

From and To Email Patterns

The email address or email domain that will be filtered. The email field supports the use of wildcards. For example, use the pattern of *@example.com to include anyone with a domain name of example.com.

Permission

Each email filter can have one of the following permissions:

- Allow: The Web User is allowed to send the Secure Mail message if the To and From email addresses match the pattern.
- Deny: The Web User is not allowed to send the Secure Mail message if the To and From email addresses match the pattern.

Package Manager

The Package Manager page allows you to view the details of all Packages that were created by Secure Mail. In the search results, click the column headings to sort the results based on that column.

To view the Package Manager, log in as an Admin User with the **Secure Mail Manager** role.

From the main menu bar, select **Services**, and then click the **Package Manager**link.

Packages can be filtered by Web User, Package Status, the date it was last modified or when it was sent. The following columns are shown for each Package returned in the results. If a column below is not shown, click the **Show/Hide Columns** button for a complete list.

Package Actions

- Click the  icon to view the "View Package Details" on page 574.
- Click the  icon to delete the files/attachments contained in the Package(s). When a Package is deleted the file attachments are removed immediately. The Inactivated On date is set, the Files Purged flag is set to true and the Package becomes available for purging. Web Users will not see Packages in the Deleted status.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Columns** button to select which Package properties are displayed in the table.

Package Columns

From Web User

The Web User account name that sent the Package.

Note: The From Web User field will be blank when an unregistered user replies to a package.

From Address

The email address of the Web User that sent the Package.

To Address

The recipients of the Package. Only the first 50 characters are shown on the list page. To view all recipients, view the "View Package Details" on page 574.

Status

The current status of the Package. The status will display as one of the following:

- Draft - The Package was saved and can be edited before sending.
- Active - The recipients of the Package are able to view the message and download the file attachments.
- Deleted - The Package was marked as deleted. When a Package is deleted the file attachments are removed immediately. The Inactivated On date is set, the Files Purged flag is set to true and the Package becomes available for purging. Web Users will not see Packages in the Deleted status.

- Inactive - The Package is no longer available for viewing or downloading and will be purged based on the options on the Purging tab of "Secure Mail Settings" on page 569. A Package will become inactive if it is revoked, if it expires or the maximum downloads for the files was reached.

Sent On

The date and time the Package link was sent.

Protection Level

Whether the Package was only URL protected, password protected, or certified delivery.

Subject

The subject of the email sent to the recipient.

Included Password

Whether the password was included in the email along with the link to the Package, or sent in a separate email.

Max Downloads

The maximum number of times each file can be downloaded per recipient. When all files on a Package can no longer be downloaded the Package will become inactive and the inactivated date will be set.

Reply Allowed

Indicates if the recipient of the message is allowed to send a reply.

Notify When Read

Indicates whether the sender requested a read receipt when a recipient clicks the link to read the Package.

Expires On

The date after which the Package will expire. When a Package expires it will be marked as inactive.

Package Size

The total size of the files contained in a Package. When the files on a Package are deleted, the size will be zero (0). The size does not reflect the size of the text the user specified as the message.

Send Status

Indicates the status of the emails sent to the recipients of the Package. The send status will display as one of the following:

- Not Sent - None of the emails for the Package were sent.
- Pending - The emails for the Package are waiting to enter the outbound mail queue.
- Sending - The Package Mailer is currently sending emails.
- All Emails Sent - All emails for the package were successfully sent from the Managed File Transfer server.
- Some Emails Sent - Some of the emails were sent successfully, but at least one recipient did not receive the email.
- Failed - Managed File Transfer attempted to notify the recipients via email but no emails could be sent. The details of the error(s) that occurred while sending are logged in the "Server Log Viewer" on page 671.

Files Purged

Whether the files in a Package have been purged/deleted.

Inactivated On

The date and time the Package status was set to inactive.

Package ID

The unique 36-character UUID code of the Package. The folder containing the Package uses this Package ID as the folder name. The default folder location is **[installdirectory]/userdata/packages**. The default Packages location is defined on the Services tab of the "Global Settings" on page 752.

Created on

The date and time the Package was created.

Modified On

The date and time the Package was last modified.

View Package Details

The View Package Details page displays the logged data for the selected Package.

To view the details of a Package, log in as an Admin User with the **Secure Mail Manager** role.

From the main menu bar, select **Services**, and then click the **Package Manager**link. On the Package Manager page, click the  Action icon next to the package, and then click the  View icon.

General

The General tab displays information related to when a Package was sent, what it contained, who sent it and where it was sent. Click the **Done** button to return to the "Package Manager" on page 571.

Activity

The Activity tab displays the associated entries for the selected Package from the “HTTPS Log” on page 674. Click the **Done** button to return to the “Package Manager” on page 571. The Activity tab has the following settings:

Recipients / File(s)

The Recipients and File(s) sections in the left panel will display either the recipients of the Package or the list of files enclosed in the Package. Clicking a recipient or a file name filters the Log results to display the activity for the selected recipient or file. When a recipient or file is selected, the line below the Activity tab displays what criteria is filtering the results.

Logs

The Logs portion of the page displays details from the HTTPS Audit Log. Click the Event ID number to open the HTTPS Audit Log details for that log entry.

File Downloaded Information

The File Downloaded Information displays the file contents of a Package. For each file, it will show the remaining downloads and how many times each file has been downloaded.

CHAPTER 7

Users

Managed File Transfer implements Roles, "Login Methods" on page 647, "Admin Users" on page 576 and "Admin Groups" on page 581 to control access to administrative functions in the product.

Admin Users

In order to perform administrative functions in Managed File Transfer, an Admin User must login with a valid user name and password. Admin Users can be added and managed only by an Admin User with the Security Officer role.

User passwords can be stored and authenticated within the Managed File Transfer's database, or can be authenticated against Windows Active Directory (AD), Azure Active Directory, LDAP, or Informatica domain authentication.

Each Admin User may belong to one or more "Admin Groups" on page 581. The Admin User will adopt the Admin Roles (authorities) from any Admin Group(s) to which they belong. An Admin User can also be granted individual Admin Roles.

The Admin User's Roles (permissions) will determine which functions the Admin User has access to in Managed File Transfer.

Note: "The Admin User administrator is created by default when installing Managed File Transfer. The "administrative level" users have authorization to all functions in Managed File Transfer. After installing Managed File Transfer, a Security Officer should "Reset Admin User Password" on page 580 for the administrator account in accordance with their corporate data security policy.

Admin User Management

To manage Admin User accounts, log in as an Admin User with the Security Officer role.

From the main menu bar, select **Users**, and then click the Admin Users link.

Admin Users Actions

The following actions are available by selecting the Actions icon:

- "Admin User Details" on page 580 the details for an Admin User by clicking the icon
- "Edit Admin User" on page 578 an Admin User by clicking the icon

- "Reset Admin User Password" on page 580 an Admin User's password by clicking the  icon

- Delete an Admin User by clicking the  icon.

Add Admin User

An Admin User can be created using the Add Admin User page. Follow the instructions below to add a new User:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Admin Users link.
3. In the "Admin User Management" on page 576 page, click the  Add Admin User link in the page toolbar.
4. Type the Admin User information in the appropriate boxes.
5. If needed, select the individual Roles to be assigned to the Admin User. See note below.
6. Assign the Admin User to one or more "Admin Groups" on page 581. The Admin User will adopt the Roles from any Groups to which it belongs.
7. Click the **Save** button to add the Admin User account.

Note: For ease of User management, it is generally not recommended to give individual Roles to an Admin User. Instead, you should assign each Admin User to one or more Groups, from which the Admin User will adopt the roles from those Groups. This allows you to quickly adjust Roles for several Admin Users at once by changing the Roles for the Group(s) to which they belong.

Admin User Tab

The Admin User tab contains the following options:

User Name

The User Name is not case sensitive and cannot exceed 20 characters.

Note: If the login method type used is Azure Active Directory, then use the principal name which is of the format: `username@azuredomainname`.

Use Default Login Method

The default login method that is used for authentication.

Select Login Method

If the Default Login Method is disabled, then you can select one of the Login Methods as a preferred login method for the Admin user.

Description

This describes the Admin User. This optional field cannot exceed 512 characters.

Password

Passwords are case sensitive and can contain numbers and characters up to 20 characters. Specify a password only if the Default Login Method for Users setting on the "Login Methods Management" on page 647 page is set to Native. Otherwise leave blank.

Email Address

The Admin User email address.

Roles

Individual "Admin Roles" on page 583 for the Admin User. The Roles are split into two sections. The Roles to which the User does not belong are shown on the left side of the page. The Roles to which the User does belong are shown on the right side of the page. Select a Role, and then use the arrow buttons to move the Role to the appropriate column. You can also drag and drop a role from one column to another.

Groups

The Groups are split into two sections. The Groups to which the User does not belong are shown on the left side of the page. The Groups to which the User does belong are shown on the right side of the page. Select a Group, and then use the arrow buttons to move the Group to the appropriate column. You can also drag and drop a Group from one column to another. The Admin User will adopt the Roles from any groups to which it belongs.

Home Directory

The home directory that the Admin User will see when launching the "File Manager" on page 750. *DOCROOT/*USER is the Admin User's default home directory located in the global documents directory. *DOCROOT is the global documents directory specified on the Data tab in "Global Settings" on page 752. *OTHER allows the specification of a custom home directory on the file system.

Restrict to Home Directory

Indicates if the Admin User is restricted to the specified home directory or has access to the entire file system when using the "File Manager" on page 750. If checked, the Admin User will only have access to the specified home directory and its sub-directories.

Note: The restriction doesn't apply to the base directory on a Project.

File Permissions

Indicates if the Admin User will have Read Only access to files or Read/Write access to files when using the "File Manager" on page 750. Read Only specifies the Admin User can only browse and download files. Read/Write allows the Admin User to browse, download, upload, copy, move, delete, and rename files.

Note: The **Home Directory**, **Restrict to Home Directory** and **File Permissions** attributes are only applicable if the User has the File Manager role.

Edit Admin User

An Admin User can be edited using the Edit Admin User page. Follow the instructions below to edit an Admin User:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Admin Users link.
3. In the "Admin User Management" on page 576 page, click the  icon next to the Admin User.
4. Modify the field values for the Admin User.

5. Click the **Save** button to save the settings.

Note: For ease of User management, it is generally not recommended to give individual Roles to an Admin User. Instead, you should assign each Admin User to one or more groups, from which the Admin User will adopt the Roles from those groups. This allows you to quickly adjust Roles for several Admin Users at once by changing the Roles for the group(s) to which they belong.

Admin User Tab

The Admin User tab contains the following options:

User Name

The User Name is not case sensitive and cannot exceed 20 characters.

Note: If the login method type used is Azure Active Directory, then use the principal name which is of the format: `username@azuredomainname`.

Use Default Login Method

The default login method that is used for authentication.

Select Login Method

If the Default Login Method is disabled, then you can select one of the Login Methods as a preferred login method for the Admin user.

Description

This describes the Admin User. This optional field cannot exceed 512 characters.

Password

Passwords are case sensitive and can contain numbers and characters up to 20 characters. Specify a password only if the Default Login Method for Users setting on the "Login Methods Management" on page 647 page is set to Native. Otherwise leave blank.

Email Address

The Admin User email address.

Roles

Individual "Admin Roles" on page 583 for the Admin User. The Roles are split into two sections. The Roles to which the User does not belong are shown on the left side of the page. The Roles to which the User does belong are shown on the right side of the page. Select a Role, and then use the arrow buttons to move the Role to the appropriate column. You can also drag and drop a role from one column to another.

Groups

The Groups are split into two sections. The Groups to which the User does not belong are shown on the left side of the page. The Groups to which the User does belong are shown on the right side of the page. Select a Group, and then use the arrow buttons to move the Group to the appropriate column. You can also drag and drop a Group from one column to another. The Admin User will adopt the Roles from any groups to which it belongs.

Home Directory

The home directory that the Admin User will see when launching the "File Manager" on page 750. *DOCROOT/*USER is the Admin User's default home directory located in the global documents directory. *DOCROOT is the global documents directory specified on the Data tab in "Global Settings" on page 752. *OTHER allows the specification of a custom home directory on the file system.

Restrict to Home Directory

Indicates if the Admin User is restricted to the specified home directory or has access to the entire file system when using the "File Manager" on page 750. If checked, the Admin User will only have access to the specified home directory and its sub-directories.

Note: The restriction doesn't apply to the base directory on a Project.

File Permissions

Indicates if the Admin User will have Read Only access to files or Read/Write access to files when using the "File Manager" on page 750. Read Only specifies the Admin User can only browse and download files. Read/Write allows the Admin User to browse, download, upload, copy, move, delete, and rename files.

Note: The **Home Directory**, **Restrict to Home Directory** and **File Permissions** attributes are only applicable if the User has the File Manager role.

Admin User Details

The Admin User Details page shows the properties for the Admin User, when the Admin User was created and when it was last modified. It also shows the Roles assigned to the Admin User and the groups to which it belongs. The Admin User Details page is only available to Users with the Security Officer role. Follow the instructions below to view User Details:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Admin Users link.
3. In the "Admin User Management" on page 576 page, click the  icon next to the User.

Reset Admin User Password

The reset password function can be used if the password is authenticated against the Managed File Transfer database. Follow the instructions below to reset an Admin User password:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Admin Users link.
3. In the "Admin User Management" on page 576 page, click the  icon next to the Admin User.
4. Select the  **Reset Password** option.
5. Provide a new password.
6. When complete, click the **Reset** button.

Note: The passwords for the administrator and root accounts are encrypted and can only be stored in the Managed File Transfer database.

Change User Password

To change your own password, click the Change Password link in the upper right corner of the Managed File Transfer page.

1. In the Change Password page, type your current password in the Current Password box.
2. Type a new password in the New Password box and re-type it in the Confirm New Password box.
3. When complete, click the **Save** button.

Admin Groups

An Admin Group is an association of one or more "Admin Users" on page 576. Each Group can be assigned specific Roles for controlling access to various Managed File Transfer functions. Any Admin Users belonging to a group will adopt the Roles from that Group.

For instance, you may want to create a Group for Auditors that would only have authority to view Logs. Another Group could be created for IT Security or Managers that have the authority to create or disable Users.

Admin Groups Management

To administer Groups, log in as an Admin User with the **Security Officer** role.

From the main menu bar, select **Users**, and then click the Admin Groups link.

Page Toolbar

The following actions are available from the page toolbar:

- "Add Admin Group" on page 582 a Group by clicking the **Add Group** button.

Admin Groups Actions

The following actions are available by selecting the Actions icon:

- "Edit Admin Group" on page 582 a Group by clicking the icon.
- "View Group" on page 582 a Group by clicking the icon.

  - Delete a Group by clicking the icon.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Admin Groups.

Add Admin Group

Follow the instructions below to add a new Admin Group:

1. From the main menu bar, select **Users**, and then click the Admin Groups link.
2. In the **Admin Groups** page, click the **Add Admin Group** link in the page toolbar.
3. Type the Group information in the appropriate boxes.
4. Select a Group "Admin Roles" on page 583, and then use the arrow buttons to move the Group Role to the appropriate column. You can also drag and drop a Group Role from one column to another.
5. Select a Group Member, and then use the arrow buttons to move the member to the appropriate column. You can also drag and drop a Group Member from one column to another.
6. Click the **Save** button to add the Group.

Edit Admin Group

Follow the instructions below to edit the properties for an Admin Group:

1. From the main menu bar, select **Users**, and then click the Admin Groups link.
2. In the "Admin Groups Management" on page 581 page, click the Action icon beside the Admin Group you wish to edit, and then click the **Edit** button.
3. Modify the field values for the Admin Group.
4. Select a Group "Admin Roles" on page 583, and then use the arrow buttons to move the Group Role to the appropriate column. You can also drag and drop a Group Role from one column to another.
5. Select a Group Member, and then use the arrow buttons to move the member to the appropriate column. You can also drag and drop a Group Member from one column to another.
6. Click the **Save** button to apply the changes.

View Group

The Group Details page shows the properties for the Group, when the Group was created and when it was last modified. It also shows the Roles assigned to the Group and the members that belong to it. Follow the instructions below to view Group Details:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Admin Groups link.
3. In the "Admin Groups Management" on page 581 page, click the icon next to the Group.
4. Click the **View** button.

Admin Roles

Roles are assigned to "Admin Users" on page 576 and "Admin Groups" on page 581. A role specifies which Managed File Transfer functions (authorities) are available to the Admin User or Admin Group.

Listed below are the roles available in Managed File Transfer:

Role Name	Authorized Functions
Auditor	- View Audit Logs for Shared Drive, FTP, FTPS, SFTP, HTTPS, MLLP, and AS2 services - View statistics of total uploads, downloads and errors - View the Server Log - View Trigger Logs View Completed Job Logs for Projects
Dashboard Manager	- Manage Shared Dashboards
File Manager	- Manage files (for example, download, copy, delete, upload) on the server where Managed File Transfer is installed
Job Manager	- Add, change and delete Scheduled Jobs and Monitors - Disable Monitors or Scheduled Jobs - View any jobs in the job queue - Cancel any jobs from the job queue - View, hold, release and cancel any active jobs - View any completed job logs for Projects
Key Manager	- Manage OpenPGP keys - Manage SSH Keys - Manage SSL Certificates
Key Manager (Read-Only)	- View OpenPGP keys - View SSH Keys - View SSL Certificates
Product Administrator	- View and change global preferences - Download product updates - View, install and uninstall the product license - View the Server Log - Manage Services Configuration and Preferences - Manage Managed File Transfer Gateway - Configure, tune and migrate the Managed File Transfer database - View and change settings for the Log Settings and Audit Log Rules
Project Designer	- Create new Project folders - Rename and delete Project folders * - Create, change, copy and delete Projects * - Import Project definitions from external sources * - Promote Projects into other installations of Managed File Transfer *
Project Executor	- Run Projects * - Monitor jobs on the job queue (which the Project Executor submitted) - Monitor active jobs (which the Project Executor submitted) - View completed jobs and job logs (which the Project Executor submitted)
Resource Manager	- Create and manage Managed File Transfer resources that are used by Triggers - Create and manage Network Shares resources

Role Name	Authorized Functions
Resource Manager (Read-Only)	- View Managed File Transfer resources that are used by Triggers - View Network Shares resources
Secure Mail Manager	- View and edit Secure Mail settings - Manage Packages
Security Officer	- Configure how User and Web User passwords are authenticated - Manage Users and their assigned Roles - Manage Groups and their assigned Roles - Manage IP Filters - Manage Web User Password Policy - Manage Web User Self-Registration Settings - Reset User passwords
Shared Drive Manager	- Manage Web User devices - Manage Shared Drive Settings
Trigger Manager	- Manage Triggers - View Trigger Logs
Web User Manager	- Manage Web Users and their assigned permissions - Manage Web User Groups and their assigned permissions - Assign Web Users to Web User Groups - Manage Web User Templates
Web User Manager (Read-Only)	- View Web Users and their assigned permissions - View Web User Groups and their assigned permissions - View Web User Templates

* The Admin User must also have appropriate permissions to the Project folder.

Note: Roles assigned to a Group will be adopted by the Admin Users belonging to that Group.

Admin Roles Management

To work with roles, log in as an Admin User with the **Security Officer** role.

From the main menu bar, select **Users**, and then click the Admin Roles link.

Admin Roles Actions

The following actions are available by selecting the  Actions icon:

- "Role Details" on page 584 the Admin Users and Groups assigned to the role by clicking the  icon.
- "Edit Admin Role" on page 585 the Admin Users and Groups assigned to the Role by clicking the  icon.

Role Details

The Role Details page displays the Admin Users and Groups assigned to a Role.

Note: The **Role Details** page is only available to Admin Users with the Security Officer role.

Edit Admin Role

A Role can be assigned to Admin Users and Groups through the **Edit Role** page. The **Edit Role** page is split in two columns. The Admin Users and Groups not assigned to the role are displayed in the left column. The Admin Users and Groups assigned to the role are displayed in the right column.

Follow the instructions below to edit the Roles for an Admin User or Group:

1. From the main menu bar, select **Users**, and then click the Admin Roles link.
2. In the "Admin Roles Management" on page 584 page, click the Action icon beside the Role you wish to edit, and then click the Edit icon.
3. Assign or remove Admin Users to the appropriate roles.
   Assign Admin Users or Groups to a Role:
   a. In the left column, click to select the Admin Users or Groups to assign to the Role. Multiple entries can be selected by pressing the Ctrl or Shift key while selecting Admin Users or Groups.
   b. When the desired Admin Users or Groups are selected, click the icon to move the Admin Users or Groups from left to right.
   Remove Admin Users or Groups from a Role:
   c. In the right column, click to select the Admin Users or Groups to remove from the role. Multiple entries can be selected by pressing the Ctrl or Shift key while selecting Admin Users or Groups.
   d. When the desired Admin Users or Groups are selected, click the icon to move the Users or Groups from right to left.
4. Click the **Save** button to apply the changes.

Security Settings

The Security Settings option is only available to Admin Users with the Security Officer role. The security settings on this page apply only to Administrative Users.

From the main menu bar, select **Users**, and then click **Admin Security Settings**.

Session Timeout

The length of idle time (in seconds), before an Admin User is automatically logged out of Managed File Transfer. The session timeout default is 3600 seconds (60 minutes). A value of 0 indicates the session will never timeout.

Allow Browsers to Save Login Credentials

By default, Managed File Transfer will not allow a browser to save login credentials. If enabled, the first time an Admin User logs in to Managed File Transfer, their browser will ask them if they want to save their password.

Allow Viewing of Resource Passwords

If enabled, Admin Users with the Resource Manager role can view Resource passwords. If the password for a Resource was encrypted when it was entered, then only the encrypted password value will be shown (not the clear text value).

This option should remain disabled (the default setting), if the Resource Manager should not be able to view the password for Resources.

Allow Session ID in URL

To prevent internet session hijacking vulnerabilities, Managed File Transfer will not allow an Admin User's session ID to appear in the URL by default. When this option is enabled, the session ID can appear in the URL while an Admin User is using the service (less secure).

Note: Admin User's who have their internet browser cookies disabled will not be able to use the service when Allow Session ID in URL is also disabled.

Allow Embedding within an IFrame

To prevent internet clickjacking vulnerabilities, Managed File Transfer will not allow the Administrator portal to run within an IFrame by default. When this option is enabled, the Administrator portal will be allowed to run in an IFrame, which can include potentially untrusted sources (less secure).

Default Resource Permissions for All Admin Users

When a Chapter 3, “Resources” on page 42 is added, this setting will determine if the All Admin Users “Admin Groups” on page 581 is added to the Resource using the selected “Resource Permissions” on page 45. If no permissions are selected, the All Admin Users group is not added to a Resource's permissions when the Resource is added.

Virtual Folders and Files

Managed File Transfer allows you to define the individual folders and files that can be accessed by Web Users. The paths for these folders and files can be on the local server or other file systems in the network. Virtual folders and files are created and managed from the Folders tab of “Add Web User Template” on page 623, “Web User Groups Management” on page 615 and “Web User Management” on page 589.

Virtual Folder Highlights

- Multiple folders and files can be authorized to the Web User, each having their own individual permissions.
- Home directories and sub-folders can be shared or private.
- Aliases can be defined to hide the physical names/locations of folders and files.
- Folder and file paths can point to various file systems (local, IFS, NFS or SMB/CIFS).
- Disk Quotas can limit the amount of disk space used by each Web User.

- Files and Folders can be shared between Web Users.

Virtual Folder Interface

The left column displays the folder structure that the Web User will see. The right side of the page shows the alias, path and permissions for the selected folder or file.

Folders

The left column starts with the Web User's home directory. By default, a home directory is created for every Web User based on the WebDocs Directory setting in "Global Settings" on page 752. Additional folders and files can be created under this home directory.

The following actions are available based on the selected folder or file.

 - Adds a new folder or file below the selected folder.

 - Deletes the selected folder or file.

Name and Location

Each folder or file must have an alias name and location.

Alias - The alias is the name of the folder or file that the Web User will see when they login.

Path - The location of the folder or file, which can be a physical or relative path. Click the  icon to browse the file system or a network share. Click the  icon to select a variable to use within the path. The ${homeDirectory} variable refers to the Web User's home directory under the WebDocs Directory as defined in the "Global Settings" on page 752. The alias name must match the relative folder name when using the home directory variable. For example, if using the folder location of ${homeDirectory}/Inbound/Accounts, then the alias name must be Accounts.

Type - Select if the path points to a folder or file.

Disk Quotas

The disk quota settings are used to control the maximum storage space allowed for a Web User. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

When determining the disk space used by a Web User, Managed File Transfer will only consider those folders which the Web User has upload, overwrite or append permissions. To view the disk space currently used by a Web User, you can access the "View Web User File System" on page 612 page.

Disk quotas can be specified on the Web User's home directory and subfolders. If a quota is specified on a subfolder, this quota will override a value that may be specified on the parent folder.

Disk quotas can be defined at the "Web User Template Management" on page 623, "Web User Groups Management" on page 615, and "Web User Management" on page 589 level. When disk quotas are specified for the same folder on both the Web User and Web User Group level, the highest value will be used. For example, if a Web User has a disk quota of 10 MB and belongs to a Web User Group that has 25 MB, then this Web User would have 25 MB of available space.

Folder Level Permissions

The following permissions can be defined at the folder level. All permissions can be enabled using the select all link.

General

List

Contents of a folder can be listed or viewed.

Download (Read)

Files can be downloaded (read) from the folder.

Upload (Write)

Files can be uploaded (written) to the folder.

Overwrite

Existing files are allowed to be overwritten when uploading files with the same name.

Append

Existing files are allowed to have data appended to them on uploads. This allows failed transfers to resume uploading.

Rename Files

Existing files can be renamed.

Delete Files

Existing files can be deleted.

Checksum

A checksum is calculated to verify the file is complete and not compromised during transmission. This is a common setting for AS2 transfers. The checksum option can be used by HTTPS, FTP and FTPS transfers. Please note that an error may occur if a "Trigger Manager" on page 206 moves the file before the checksum process completes.

Share

Folders can be shared with registered Web Users. When sharing is enabled, the  icon appears on the File Manager toolbar and context menus within the File Transfer Portal.

If the **Apply To Subfolders** option is enabled, all folders under the selected folder will inherit these permissions.

Subfolders

If enabled, these permissions apply to all sub-folders under the selected folder.

Create

Subfolders can be created under the selected folder.

Rename

Sub-folders can be renamed.

Delete

Sub-folders and their contents can be deleted.

Share

Sub-folders can be shared with registered Web Users.

File Level Permissions

The following permissions can be defined at the file level.

Download (Read)

The file can be downloaded (read).

Overwrite

A file with the same name can overwrite the existing file on an upload.

Append

The file can be appended to on an upload. This allows a failed transfer to resume uploading a partial file.

Checksum

A checksum is calculated to verify the file is complete and not compromised during transmission. This is a common setting for AS2 transfers.

Share

The file can be shared with registered Web Users. When sharing is enabled, context menus will display the share option within the File Transfer Portal.

Note: A consolidated view of the folders and files for a Web User is available on the "View Web User File System" on page 612 page.

Web Users

Web Users are the accounts that can access Managed File Transfer for exchanging files using standard protocols. Web Users can be external (for example, Trading Partners) or internal to your company (for example, employees or custom applications).

Web Users are managed by an Admin User that has a Web User Manager role. Web Users can be added individually, from an "Add LDAP Server" on page 651, or through an "Import Web Users From CSV" on page 600 process that provides the ability to add multiple Web Users based on "Web User Template Management" on page 623. A Web User account can also be created through a "Web User Self-Registration" on page 645 process available on the HTTPS File Transfer Portal. APIs are also available to create Web Users from your in-house applications.

Each Web User may belong to one or more "Web User Groups Management" on page 615. The Web User will adopt the Permissions (authorities) from any Web User Group to which they belong. A Web User can also be granted individual Permissions for various services, "Virtual Folders and Files" on page 586. IP Filters can also be configured to ensure that Web Users are only accessing Managed File Transfer from an expected location.

Web User Management

Web User accounts are created to provide users with the ability to connect to the services they need for secure file transfers. Web User accounts can be created individually, mass imported or self-registered via the File Transfer Portal. The anonymous Web User account can be enabled on the Anonymous tab of the "Web User Settings" on page 641 page.

To manage Web User accounts, log in as an Admin User with the **Web User Manager** role.

From the main menu bar, select **Users**, and then click the **Web Users** link.

Web User accounts can be filtered on this page by typing all or part of a User Name, by selecting an Account Status or a Web User Group from the drop-down lists. Show more or fewer columns on the page by clicking the **Columns** button. From the displayed columns, click a column heading to sort the Web Users by the selected column.

Note: If a Web User is "grayed out," it means that the account is expired, disabled or pending approval from a self-registration. If you wish to re-enable the account, then edit the "Edit Web User" on page 603 account and enable the account on the General tab. If the Web User is pending approval, you can approve the account by clicking the  icon and then clicking  Approve.

Page Toolbar

The following actions are available from the page toolbar:

- "Add Web User" on page 591 a Web User by clicking  **Add Web User**.
- "Pending Invitations" on page 603 Pending Invitations by clicking  Pending Invitations.
  - Import Web Users from "Import Web Users From CSV" on page 600 by selecting  Import From CSV.
  - Import Web Users by from "Import Web Users From XML" on page 602 by selecting the  Import From CSV.

Web User Actions

The following actions are available by selecting the  Actions icon:

- "Web User Details" on page 612 Web User details by clicking the  icon.
- "View Web User File System" on page 612 the Web User File System by clicking the  icon.
- "Edit Web User" on page 603 a Web User by clicking the  icon.
  - Approve a self-registered Web User by clicking the  icon.
- "Reset Web User Password" on page 612 a Web User's password by clicking the  icon.
  - Delete a Web User by clicking the  icon. Delete one or more Web Users by selecting the appropriate check boxes and clicking the **Delete** button.
- "Web User SSH Keys" on page 613 the public SSH keys for a Web User by clicking the  icon.
- "Promote Web Users" on page 614 a Web User's account to another Managed File Transfer server by clicking the icon.
  - Export a Web User's account information to an XML file by clicking the  icon. The selected Web User(s) are saved in a file named "export-web-users.xml" on your local computer.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Web Users.
- "Promote Web Users" on page 614 one or more selected Web Users to another Managed File Transfer server.

- Export the selected Web User's account information to an XML file. The selected Web User(s) are saved in a file named "export-web-users.xml" on your local computer. This file can be used as a backup or for importing the Web User(s) to another Managed File Transfer instance.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Export the account information for all Web Users that meet the filter criteria to an XML file. The account information is saved in a file named "export-web-users.xml" on your local computer. This file can be used as a backup or for importing the Web User(s) to another Managed File Transfer instance.
  - Click the **Columns** button to select which Web User properties are displayed in the table.

Add Web User

A Web User can be added using the Add Web User page. Follow the instructions below to add a Web User:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the **Web Users** link.
3. In the "Admin User Management" on page 576 page, click the Add Web User link in the page toolbar.
4. Choose the "Web User Templates" on page 622 that will apply default security settings for the Web User, and then click the **Continue** button.
5. Type the Web User information in the appropriate boxes.
6. Click the **Save** button to add the Web User account.

General

The General tab has the following fields:

User Name

The user name for a Web User. The account name must conform to the "Web User Settings" on page 641.

Note: If the login method type used is Azure Active Directory, then the user name if of the format: username@AzureDomainName.

First Name

The Web User's first name.

Last Name

The Web User's last name.

Description

The description is optional information pertaining to the Web User. This field is limited to 512 characters.

Organization

The company or organization which the Web User belongs to.

Email Address

The primary email address of the Web User. An email address should be specified if the Web User receives email communication for account creation, password reset, forgot password or they have access to Secure Mail.

Phone

The primary phone number for the Web User.

Authentication

The Authentication tab has the following fields:

Login Method

Specify which login method should be used to authenticate the Web User.

When the default option is selected, the Web User will use the default Login Method for Web Users specified in the Login Methods page. To authenticate against another Login Method, clear the checkbox and select it from the drop-down list. The password options are only shown when authentication is performed against the Managed File Transfer database.

Password Generation

Passwords for Web User accounts can be generated automatically based on the Web User Password Policy. Otherwise the Web User Manager creating the account can manually specify a password. If specifying the password, Managed File Transfer will alert you if the password does not meet the Web User Password Policy. The maximum password length is 20 characters.

Password Options

If authenticating the Web User account against the Managed File Transfer database, the following options can be specified for the Web User password:

- Display password to the page - The new Web User password is displayed on the page.
- Email password - The password is emailed to the Web User using a Web User Email Template.
- Allow User to Change Password - This option makes a Change Password link available at the top of the page in the HTTPS File Transfer Portal.
- Force Password Change at Next Login - This option is only available to Web Users using the HTTPS service. If selected, this option will force a Web User to type a new password after a successful initial login.

Password Expiration Interval

If authenticating the Web User account against the Managed File Transfer database, the password expiration interval determines how long before a password expires.

- Default - The Password Expiration Interval is defined in the Web User Password Policy
- Password Never Expires
- Password Expires After - The Web User password will expire after the specified number of days.

Authentication Types

The Authentication Type can be specified per service. This provides the Web User Manager with complete control over the Web User's access. For example, a Web User can be forced to use a Password and Certificate when authenticating to FTPS but only require a Password for HTTPS. If a certificate is used for authentication, the Client Authentication setting on the SSL tab of the specific service must be set to Optional or Required.

If certificate authentication is specified and the certificate being used is either self-signed or signed by an untrusted Certificate Authority (CA), then the certificate will need to be imported into the Default Trusted Certificates Key Store. Importing the certificate instructs Managed File Transfer to trust this source. If the certificate being used is already signed by a trusted authority (for example, Verisign, GoDaddy, Equifax, etc.) the certificate does not need to be imported since the trust is inherited.

HTTPS

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box. Each Web User must have a unique SHA1 Fingerprint.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the unique SHA1 Fingerprint for the Web User's certificate in the box.

AS2

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type a SHA1 Fingerprint for the Web User's certificate in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with a shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPES (Explicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a password any time they use Managed File Transfer.On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPS (Implicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

SFTP

- Password - Web Users login using their standard Web User name and password.
- Public Key - Web Users use a public key on the server to encrypt a session key that produces a secure login.

- Either - If a matching public key is found during the connection, the Web User will automatically pass authentication. However if a key match is not found, the Web User can still login to the Managed File Transfer server with a user name and password.
- Password and Public Key - Web Users must login using their Web User name and password along with a public key.

Note: Associate an SSH Public Key with a Web User by using the SSH Keys option on the Web Users page.

Groups

Web Users can belong to one or more Web User Groups. A Web User will adopt the permissions from any Web User Groups they belong to. They will also have access to any folders which the Web User Groups are authorized to access.

The Groups tab is split into two columns. The column on the left displays the available Groups to which the Web User does not belong. The column on the right displays the Groups in which the Web User is a member. Click to highlight groups and then use the direction buttons between the columns to move Groups to the appropriate side.

Assigning Web Users to a Web User Group

Perform the following steps to assign Web Users to a Web User Group:

1. On the left side of the page, click to select the Web User(s) to assign to the Web User Group.
2. When the desired Web Users are selected, click the >> arrow between the group boxes to move the Web Users from left to right.
3. Click the **Save** button to apply the changes.

Removing Users from a Web User Group

Perform the following steps to remove Web User Groups from a Web User:

1. On the right side of the page, click to select (highlight) the Web User Group(s) to remove from the Web User. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Web User Groups are selected, click the ← button between the group boxes to move the Web User Groups from right to left.
3. Click the **Save** button to apply the changes.

   Note: For ease of Web User management, it is generally not recommended to give individual permissions to a Web User. Instead, assign each Web User to one or more Web User Groups, from which the Web User will adopt the permissions assigned to those Web User groups. This allows you to quickly adjust permissions for several Web Users at once by changing the permissions for the Web User Group(s) in which they belong.

Features

The Features tab contains the following options:

Protocols

Select the services the Web User can use for performing file transfers. If the Web User is a member of a group, these services are in addition to the services inherited from the group.

Share Drive

This option provides Web Users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents. This option can also be enabled at the "Web User Groups Management" on page 615 level.

Shared Drive Access

When Shared Drive is enabled for the Web User, you can select the Web User's access level to this feature:

- Full Licensed User: This is a fully licensed user that can read, write, modify, delete, upload, download, synchronize files, and share files in Shared Drive.
- View Only: This is a limited user that can only read and download files that are shared with them by other Web Users.

Shared Drive Disk Space Limited

Disk quotas can be used to control the maximum Shared Drive storage space allowed for a Web User. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

Shared Drive uses the following rules to determine what is counted towards a Web User's maximum disk quota:

- All files and folders located in the user's Shared Drive workspace
- Files that are shared to a user when the user has accepted the shared file
- Files that have been deleted to the Trash Bin
- When multiple revisions of a file are available, only the current revision of the file is counted towards a user's disk quota.
  There are three options available on the Disk Space Limited field:
  - Blank (not specified): The Web User will have unlimited disk space, unless disk space is limited at the Web User Group level. This option is preferred when you want to control disk quotas from the Web User Group this user belongs to.
  - Yes: The disk space is limited for the Web User. When Shared Drive disk quotas are specified on both the Web User and Web User Group level, the highest value will be used. If the Web User Group this user belongs to does not have a disk limit (by selecting "No" on the Disk Space Limited field for the Web User Group), this user will be unlimited. If the Shared Drive Disk Space Limited field is unspecified on the Web User Group level, this user will be limited.
  - No: This user does not have a disk quota. This setting will take precedence over any limit specified on the Web User Group level.

Shared Drive Disk Space Limited

The maximum amount of disk space available for this Web User in Shared Drive.

Secure Folders

The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Secure Mail

This option provides a Web User with the ability to send Secure Mail through the File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Invitations

Web Users logged in to the File Transfer Portal can invite other individuals to "Web User Self-Registration" on page 645 when this option is active.

View Activity Report

This option allows Web Users to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.

Max Concurrent Sessions

The total number of active sessions a Web User can have open at any one time across all available services. If this field is left blank, the Web User is permitted to have unlimited concurrent sessions.

Folders

A Web User can be authorized to one or more folders or files, which may be located on the local file system or other file systems on the network. A disk quota can also be established for each Web User. The disk quotas, folders and files can be assigned at the "Web User Management" on page 589, "Web User Template Management" on page 623 or "Web User Groups Management" on page 615 level.

Learn more about virtual folders and how they are configured in "Virtual Folders and Files" on page 586.

Note: When the Web User account is saved, Managed File Transfer attempts to create the Home Directory and all relative sub-folders if those folders do not already exist.

IP Filter

The IP filter can be used to indicate which IP addresses are allowed or restricted when the Web User connects to Managed File Transfer. Both IPv4 and IPv6 address formats are supported.

Enable IP Filter

The IP Filter can be enabled or disabled at the individual Web User level.

Filter Type

Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others. In most cases a "IP Filter" on page 780 is set to Blacklist addresses that are known threats. At the Web User level, it is common to specify a white list of allowable addresses.

Filter Entries

The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above. Click a row to enter an IP address in either single, range, or CIDR notation format. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255). Click **Add Filter Entry** to add multiple rows. A red flag on an entry simply indicates that it is a new entry.

Note: Note: A single IPv4 address is comprised of four sets of three numbers from 0 to 255, separated by periods. A single IPv6 address is comprised of eight sets of four hexidecimal numbers, separated by colons. An IP range includes all the addresses between two specified addresses. The addresses are separated by a hyphen. An IP address in CIDR notation is an IP address followed by a "prefix." The prefix notates a range of IP addresses without the need to type all the sets.

Time Limits

The Time Limits tab allows specifying options for expiring the Web User account on a certain date or when no activity occurs for a period of time. You can also use this page to limit the times of day and weekdays that a Web User can login.

The Time Limits tab has the following settings:

Account Expires On

If you would like the Web User account to expire on a certain date, enter or select the date. If specified, the Web User will not be able to login on or after that date.

Limit Time of Day

To limit the time period in which the Web User can login, choose the "Only allow between..." option and then specify the range.

Limit Days of Week

To limit which days of the week the Web User can login, choose the "Only allow on..." option and then select the days.

Disable Account When No Activity

The Web User account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.

- Default - The Disable Inactive Account value is defined on the General tab of "Web User Settings" on page 641.
- Never - The account will not disable based on inactivity.
- Disable account after - The Web User account will become disabled after the specified number of inactive days.

AS2

The AS2 tab allows specifying properties for receiving AS2 messages from the Web User. Additional AS2 information is located in the "Quick Start for AS2" on page 520.

The AS2 tab has the following settings:

AS2 ID

The AS2 ID of the sender (Web User). The AS2 ID is case sensitive and can be 1 to 128 ASCII printable characters in length.

Signature Certificate Alias

This is the alias of the public certificate used by this Web User to sign their messages. If the certificate is signed by a certificate authority (for example, Verisign), this field can be left blank since the certificate chain already exists in the Default Trusted Certificates Key Store. If a specific certificate is to be used by the Web User for signing messages or they use a self-signed certificate, then that certificate should be imported into the Default Trusted Certificates Key Store. If you do not know the alias name for the certificate, click the  icon to select the certificate alias.

Default Upload Folder

The location where AS2 messages are saved when received (uploaded). The default location is the default home directory for the Web User, which is the [installdirectory]/userdata/webdocs/[webuser] folder, where [installdirectory] is the installation directory of Managed File Transfer and [webuser] is the

account name of the Web User. If files for this Web User should be saved in a different location, use the Other... option to manually type a folder location (for example, inbound/as2).

When File Exists

The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.

Require Encryption

This option indicates whether or not messages sent by this Web User must be encrypted.

Require Signature

A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this Web User will be rejected.

Require Authentication

Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the AS2 ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.

Asynchronous MDN Approval

If a return receipt is requested by the Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed. The  icon on the AS2 Log page indicates a manual receipt needs to be sent for a message. A manual receipt can only be sent if a message is received successfully. If an error occurs during transmission, an asynchronous receipt is sent automatically.

Upload Restrictions

You can restrict the web users on the files to upload to the Managed File Transfer system. Upload restrictions don't apply to MLLP protocol.

The Upload Restrictions tab contains the following options:

Allow Files with No Extension

Select this option to allow web users to upload files that don't have extensions.

Allow Files with an Extension

Select this option to allow web users to upload files that have extensions. The web users must enter the file extensions in the **File Extension Filter** field.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or permit specific extensions. To specify the file types web users can or can't upload, enter the file extensions in this box. Enter extensions without periods (.), separate them with commas, and don't add line breaks or spaces. For example, to allow .txt, .xls, .xlsx, and .csv files, enter txt,xls,xlsx,csv. The maximum number of characters for this field is 2,000.

Case Sensitive

Select this option to specify that file extensions are case sensitive.

Import Web Users From CSV

The import Web Users process can automatically create Web Users from a CSV file based on a template. The information contained in this CSV file specifies a Web User account name and other pieces of information that can be used in the Web User account creation process. Follow the steps below to import Web Users:

1. Establish the "Login Methods Management" on page 647 the new Web users will use to authenticate with Managed File Transfer.
2. Define the "Web User Templates" on page 622 that will specify the password settings, file access permissions, email communications, etc. for each created Web User.
3. "Create the CSV File" on page 600 a CSV file for importing Web Users.
4. "Validate and Import CSV File" on page 602 the CSV file to create new Web User accounts.
5. "Review Import Web User Results" on page 602 the import results including any values that were created during the import process (for example, passwords).

Create the CSV File

The CSV file contains the information used to create one or more Web User accounts. The first row of the CSV file is the header row and only contains column names. The column names are not case sensitive and can be arranged in any order. The following column names are valid for the CSV file:

WebUserTemplate

Specifying a template in the CSV file is optional and will override the template selected on the Import Web Users page for the given record. This can be used to import multiple Web Users with different templates in a single import.

UserName

The Web User name for the Web User account is a required field. The Web User Name must also conform to the "Web User Settings" on page 641.

Password

If the Web User Template requires a user specified password, a password meeting the "Web User Settings" on page 641 must be included in this column.

PasswordAlgorithm

If the password specified is in encrypted format (hashed and base64 encoded) the PasswordAlgorithm column should be included. Supported hash algorithms are MD2, MD5, SHA-1, SHA-256, SHA-384 and SHA-512. The algorithms must be specified in upper case.

FirstName

The Web User's first name. This field is required if the Home Directory refers to the variable ${user.firstName}.

LastName

The last name of the Web User. This field is required if the Home Directory refers to the variable ${user.lastName}.

Description

The description field is limited to 512 characters and used for notes regarding the Web User.

Organization

The Web User's company. This field is required if the Home Directory refers to the variable ${user.organization}.

Email

The email address of the Web User becomes a required field if the template uses the Web User's email (for example, sending an account password). This field is also required if the Home Directory refers to the variable ${user.email}.

Phone

The Web User's phone number.

HTTPSFingerprint

If the specified Web User Template has the Authentication Type for HTTPS set to Certificate or Either, the HTTPSFingerprint column is required.

AS2Fingerprint

If the specified Web User Template has the Authentication Type for AS2 set to Certificate, Either, or Certificate and Password, the AS2Fingerprint column is required.

FTPESFingerprint

If the specified Web User Template has the Authentication Type for FTPES set to Certificate, Either or Certificate and Password, the FTPESFingerprint column is required.

FTPSFingerprint

If the specified Web User Template has the Authentication Type for FTPS set to Certificate, Either or Certificate and Password, the FTPSFingerprint column is required.

HomeDirectory

The Home Directory is optional. It can use the value defined in the template or can be defined in the CSV file. In either case, variables can be used to define the HomeDirectory (for example, C:\webdocs\${user.organization}\${user.name}).

Variable	Description
${user.name}	User name from the CSV file
${user.firstName}	First name from the CSV file
${user.lastName}	Last name from the CSV file
${user.organization}	Organization from the CSV file
${user.email}	Email from the CSV

CSV File Example

In the following example, three Web Users will be imported using the Customers template, which would need to be predefined before the import.

Note: If the Web User Import CSV file is created using a spreadsheet, save the file as file type CSV.

Validate and Import CSV File

1. On the Import Web Users page, specify the following:
   Import From

   The CSV file can be imported from either a file on the end user's PC or a file on the Managed File Transfer server.

   Input File

   The path or location of the CSV file containing the import information.

   Web User Template

   The Web User Template to use for authentication, permissions and groups, IP filters and account status settings. The selected Web User Template is used if no template is specified in the CSV file.
2. When complete, click the **Validate and Import** button.
3. The Import Web Users dialog box opens, providing the results of the validation. The Input Row number corresponds with the row that contains the information in the CSV file. If the validation process detects an error or inconsistencies, the dialog box provides a message with what caused the error.
   - If no errors were found, click the **Import** button to create the Web User accounts.
   - If errors were found, click the **Cancel** button and then correct the specified errors in the CSV file.

Review Import Web User Results

After the Web User Import completes, a dialog box displays the results. Any errors encountered will also display in this dialog box. The Input Row number corresponds to the row in the CSV file that triggered the message.

- Click the **Download Import Results** button to download a file of the Import messages to a location on your computer.
- Click the **Done** button to close the Import Web Users dialog box.

Import Web Users From XML

Web Users can be exchanged between Managed File Transfer servers using XML format. To generate the XML file, export the "Web User Management" on page 589 from the source Managed File Transfer server. After the XML file is generated, follow the instructions below to import these Web Users from the XML file:

1. Log in as an Admin User with the Web User Manager role.
2. Verify the "Web User Groups Management" on page 615 and "Web User Template Management" on page 623 settings on the target server match the settings of the source server.
3. From the main menu bar, select **Users**, and then click the **Web Users** link.
4. In the "Admin User Management" on page 576page, click the Import Web Users link in the toolbar.
5. From the drop-down menu select, click **Import from XML**.
6. On the Import Web Users From XML page, specify the following:
   Import From

   The XML file can be imported from either a file on the end user's PC or a file on the source Managed File Transfer server.

   Input File

   The path or location of the XML file containing the import information.

7. When complete, click the Import button. A message on the page displays the import results.

Note: It is not recommended to import Web Users from an XML file created outside of Managed File Transfer. Instead, you should use the Import Web Users from CSV option.

Pending Invitations

Invitations that have been sent, but not yet accepted by the recipient, will be displayed on the Pending Invitations page. Follow the instructions below to view pending invitations:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the **Web Users** link.
3. In the "Web User Management" on page 589 page, click the  Pending Invitations link in the toolbar. The information displayed on the Pending Invitations page shows who was invited, which Web User invited them and when. Pending invitations expire based on the value set for the Email Verification Grace Period on the "Web User Self-Registration" on page 645 page. The email sent to the recipient is based on an "Web User Email Templates" on page 812 that contains a unique 36-character UUID code, which the recipient clicks to finish the self-registration process on the Managed File Transfer server.

   Pending invitations can be individually deleted by clicking the  icon beside the entry. Delete multiple pending invitations by selecting the corresponding checkboxes and clicking the **Delete** button.

Edit Web User

Use this feature to edit the properties for an existing Web User.

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the **Web Users** link.
3. In the "Web User Management" on page 589 page, click the icon next to the Web User.
4. Modify the field values for the Web User.
5. Click the **Save** button to save the settings.

General

The General tab has the following fields:

Enabled

Indicates if the Web User account is enabled or not. If disabled, the Web User will not be able to login.

First Name

The Web User's first name.

Last Name

The Web User's last name.

Description

The description is optional information pertaining to the Web User. This field is limited to 512 characters.

Organization

The primary email address of the Web User. An email address should be specified if the Web User receives email communication for account creation, password reset, forgot password or they have access to Secure Mail.

Email Address

The primary email address of the Web User. An email address should be specified if the Web User receives email communication for account creation, password reset, forgot password or they have access to Secure Mail.

Phone

The primary phone number for the Web User.

Authentication

The Authentication tab has the following fields:

Login Method

Specify which technique should be used to authenticate the Web User. Valid methods are Azure Active Directory, Windows Active Directory (AD), LDAP, IBM i user profiles, LDAP Managed server(s), and the Managed File Transfer database. The valid methods are defined on the "Login Methods Management" on page 647 page.

When the default option is selected, the Web User will use the default Login Method for Web Users specified in the "Login Methods Management" on page 647 page. To authenticate against another Login Method, clear the checkbox and select it from the drop-down list. The password options are only shown when authentication is performed against the Managed File Transfer database.

Password Generation

Passwords for Web User accounts can be generated automatically based on the "Web User Settings" on page 641. Otherwise the Web User Manager creating the account can manually specify a password. If specifying the password, Managed File Transfer will alert you if the password does not meet the "Web User Settings" on page 641. The maximum password length is 20 characters.

Password Options

If authenticating the Web User account against the Managed File Transfer database, the following options can be specified for the Web User password:

- Display password to the page - The new Web User password is displayed on the page.
- Email password - The password is emailed to the Web User using a "Web User Email Templates" on page 812.
- Allow User to Change Password - This option makes a Change Password link available at the top of the page in the HTTPS File Transfer Portal.
- Force Password Change at Next Login - This option is only available to Web Users using the HTTPS service. If selected, this option will force a Web User to type a new password after a successful initial login.

Password Expiration Interval

>If authenticating the Web User account against the Managed File Transfer database, the password expiration interval determines how long before a password expires.

- Default - The Password Expiration Interval is defined in the "Web User Settings" on page 641
- Password Never Expires

- Password Expires After - The Web User password will expire after the specified number of days.

Authentication Types

The Authentication Type can be specified per service. This provides the Web User Manager with complete control over the Web User's access. For example, a Web User can be forced to use a Password and Certificate when authenticating to FTPS but only require a Password for HTTPS. If a certificate is used for authentication, the Client Authentication setting on the SSL tab of the specific "Service Manager" on page 516 must be set to Optional or Required.

If certificate authentication is specified and the certificate being used is either self-signed or signed by an untrusted Certificate Authority (CA), then the certificate will need to be "Import SSL Certificate" on page 737 into the Default Trusted Certificates Key Store. Importing the certificate instructs Managed File Transfer to trust this source. If the certificate being used is already signed by a trusted authority (for example, Verisign, GoDaddy, Equifax, etc.) the certificate does not need to be imported since the trust is inherited.

HTTPS

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box. Each Web User must have a unique SHA1 Fingerprint.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the unique SHA1 Fingerprint for the Web User's certificate in the box.

AS2

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384

- SHA512

- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type a SHA1 Fingerprint for the Web User's certificate in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with a shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPES (Explicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPS (Implicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File

Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.

- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

SFTP

- Password - Web Users login using their standard Web User name and password.
- Public Key - Web Users use a public key on the server to encrypt a session key that produces a secure login.
- Either - If a matching public key is found during the connection, the Web User will automatically pass authentication. However if a key match is not found, the Web User can still login to the Managed File Transfer server with a user name and password.
- Password and Public Key - Web Users must login using their Web User name and password along with a public key.

Note: Associate an SSH Public Key with a Web User by using the "Web User SSH Keys" on page 613 option on the "Web User Management" on page 589 page.

Groups

Web Users can belong to one or more Web User Groups. A Web User will adopt the permissions from any Web User Groups they belong to. They will also have access to any folders which the Web User Groups are authorized to access.

The Groups tab is split into two columns. The column on the left displays the available Groups to which the Web User does not belong. The column on the right displays the Groups in which the Web User is a member. Click to highlight groups and then use the direction buttons between the columns to move Groups to the appropriate side.

Assigning Web User Groups to a Web User

Perform the following steps to assign Web User Groups to a Web User:

1. On the left side of the page, click to select (highlight) the Web User Group(s) to assign to the Web User. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Web User Groups are selected, click the → button between the Group boxes to move the Web User Groups from left to right.
3. Click the **Save** button to apply the changes.
   Removing Users from a Web User Group

   Perform the following steps to remove Web User Groups from a Web User:
4. On the right side of the page, click to select (highlight) the Web User Group(s) to remove from the Web User. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
5. When the desired Web User Groups are selected, click the ← button between the group boxes to move the Web User Groups from right to left.
6. Click the **Save** button to apply the changes.

   Note: For ease of Web User management, it is generally not recommended to give individual permissions to a Web User. Instead, assign each Web User to one or more Web User Groups, from which the Web User will adopt the permissions assigned to those Web User groups. This allows you to quickly adjust permissions for several Web Users at once by changing the permissions for the Web User Group(s) in which they belong.

Features

The Features tab contains the following options:

Protocols

Select the services the Web User can use for performing file transfers. If the Web User is a member of a group, these services are in addition to the services inherited from the group.

Share Drive

This option provides Web Users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents. This option can also be enabled at the "Web User Groups Management" on page 615 level.

Shared Drive Access

When Shared Drive is enabled for the Web User, you can select the Web User's access level to this feature:

- Full Licensed User: This is a fully licensed user that can read, write, modify, delete, upload, download, synchronize files, and share files in Shared Drive.
- View Only: This is a limited user that can only read and download files that are shared with them by other Web Users.

Shared Drive Disk Space Limited

Disk quotas can be used to control the maximum Shared Drive storage space allowed for a Web User. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

Shared Drive uses the following rules to determine what is counted towards a Web User's maximum disk quota:

- All files and folders located in the user's Shared Drive workspace
- Files that are shared to a user when the user has accepted the shared file
- Files that have been deleted to the Trash Bin
- When multiple revisions of a file are available, only the current revision of the file is counted towards a user's disk quota.
  There are three options available on the Disk Space Limited field:
  - Blank (not specified): The Web User will have unlimited disk space, unless disk space is limited at the Web User Group level. This option is preferred when you want to control disk quotas from the Web User Group this user belongs to.
  - Yes: The disk space is limited for the Web User. When Shared Drive disk quotas are specified on both the Web User and Web User Group level, the highest value will be used. If the Web User Group this user belongs to does not have a disk limit (by selecting "No" on the Disk Space Limited field for the Web User Group), this user will be unlimited. If the Shared Drive Disk Space Limited field is unspecified on the Web User Group level, this user will be limited.
  - No: This user does not have a disk quota. This setting will take precedence over any limit specified on the Web User Group level.

Shared Drive Disk Space Limited

The maximum amount of disk space available for this Web User in Shared Drive.

Secure Folders

The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Secure Mail

This option provides a Web User with the ability to send Secure Mail through the File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Invitations

Web Users logged in to the File Transfer Portal can invite other individuals to "Web User Self-Registration" on page 645 when this option is active.

View Activity Report

This option allows Web Users to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.

Max Concurrent Sessions

The total number of active sessions a Web User can have open at any one time across all available services. If this field is left blank, the Web User is permitted to have unlimited concurrent sessions.

Folders

A Web User can be authorized to one or more folders or files, which may be located on the local file system or other file systems on the network. A disk quota can also be established for each Web User. The disk quotas, folders and files can be assigned at the "Web User Management" on page 589, "Web User Template Management" on page 623 or "Web User Groups Management" on page 615 level.

Learn more about virtual folders and how they are configured in "Virtual Folders and Files" on page 586.

Note: When the Web User account is saved, Managed File Transfer attempts to create the Home Directory and all relative sub-folders if those folders do not already exist.

IP Filter

The IP filter can be used to indicate which IP addresses are allowed or restricted when the Web User connects to Managed File Transfer. Both IPv4 and IPv6 address formats are supported.

Enable IP Filter

The IP Filter can be enabled or disabled at the individual Web User level.

Filter Type

Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others. In most cases a "IP Filter" on page 780 is set to Blacklist addresses that are known threats. At the Web User level, it is common to specify a white list of allowable addresses.

Filter Entries

The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above. Click a row to type an IP address in either single, range, or CIDR notation format. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255). A red flag on an entry simply indicates that it is a new entry.

Note: Note: A single IPv4 address is comprised of four sets of three numbers from 0 to 255, separated by periods. A single IPv6 address is comprised of eight sets of four hexidecimal numbers, separated by colons. An IP range includes all the addresses between two specified addresses. The addresses are separated by a hyphen. An IP address in CIDR notation is an IP address followed by a "prefix." The prefix notates a range of IP addresses without the need to type all the sets.

Time Limits

The Time Limits tab allows specifying options for expiring the Web User account on a certain date or when no activity occurs for a period of time. You can also use this page to limit the times of day and weekdays that a Web User can login.

The Time Limits tab contains the following settings:

Account Expires On

If you would like the Web User account to expire on a certain date, enter or select the date. If specified, the Web User will not be able to login on or after that date.

Limit Time of Day

To limit the time period in which the Web User can login, choose the "Only allow between..." option and then specify the range.

Limit Days of Week

To limit which days of the week the Web User can login, choose the "Only allow on..." option and then select the days.

Disable Account When No Activity

The Web User account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.

- Default - The Disable Inactive Account value is defined on the General tab of "Web User Settings" on page 641
- Never - The account will not disable based on inactivity.
- Disable account after - The Web User account will become disabled after the specified number of inactive days.

AS2

The AS2 tab allows specifying properties for receiving AS2 messages from the Web User. Additional AS2 information is located in the "Quick Start for AS2" on page 520.

The AS2 tab contains the following settings:

AS2 ID

The AS2 ID of the sender (Web User). The AS2 ID is case sensitive and can be 1 to 128 ASCII printable characters in length.

Signature Certificate Alias

This is the alias of the public certificate used by this Web User to sign their messages. If the certificate is signed by a certificate authority (for example, Verisign), this field can be left blank since the certificate chain already exists in the Default Trusted Certificates Key Store. If a specific certificate is to be used by the Web User for signing messages or they use a self-signed certificate, then that certificate should be

imported into the Default Trusted Certificates Key Store. If you do not know the alias name for the certificate, click the  icon to select the certificate alias.

Default Upload Folder

The location where AS2 messages are saved when received (uploaded). The default location is the default home directory for the Web User, which is the [installdirectory]/userdata/webdocs/[webuser] folder, where [installdirectory] is the installation directory of Managed File Transfer and [webuser] is the account name of the Web User. If files for this Web User should be saved in a different location, use the Other... option to manually type a folder location (for example, inbound/as2).

When File Exists

The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.

Require Encryption

This option indicates whether or not messages sent by this Web User must be encrypted.

Require Signature

A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this Web User will be rejected.

Require Authentication

Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the AS2 ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.

Asynchronous MDN Approval

If a return receipt is requested by the Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed. The  icon on the AS2 Log page indicates a manual receipt needs to be sent for a message. A manual receipt can only be sent if a message is received successfully. If an error occurs during transmission, an asynchronous receipt is sent automatically.

Upload Restrictions

You can restrict the web users on the files to upload to the Managed File Transfer system. Upload restrictions don't apply to MLLP protocol.

The Upload Restrictions tab contains the following options:

Allow Files with No Extension

Select this option to allow web users to upload files that don't have extensions.

Allow Files with an Extension

Select this option to allow web users to upload files that have extensions. The web users must enter the file extensions in the **File Extension Filter** field.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or permit specific extensions. To specify the file types web users can or can't upload, enter the file extensions in this box. Enter extensions without periods (.), separate them with commas, and don't add line breaks or spaces. For example, to allow .txt, .xls, .xlsx, and .csv files, enter txt,xls,xlsx,csv. The maximum number of characters for this field is 2,000.

Case Sensitive

Select this option to specify that file extensions are case sensitive.

Web User Details

The Web User Details page shows the properties, such as the creation date and last modified date for a Web User.

View Web User File System

The View Web User File System page displays the Network folders and files to which the Web User has access. Each file and folder is displayed in the right column and its details are summarized in the left. Click the  icon beside each file or folder to view its details. No changes to the file or folder permissions can be made on this page.

The files and folders displayed reflect the selected options on the Folder tabs of the "Edit Web User" on page 603 account and "Edit Web User Group" on page 619 to which it belongs. The home directory is a consolidation of all folder permissions granted to the Web User and their Web User Group memberships. The permissions for files and subfolders are consolidated based on the Consolidate Subfolders option on the Folders tab of the "Web User Settings" on page 641.

This page also shows the relative/virtual path displayed to the Web User and the actual physical path where the file resides. The physical path can be on a shared network location and referenced using variables. When disk quotas are configured, the page displays the quota size and amount used. Learn more about disk quotas and virtual folders in Managed File Transfer in the "Virtual Folders and Files" on page 586 section.

To view the Web User File System, log in as an Admin User with the Web User Manager role.

From the Web Users page, click the  Action icon beside a Web User and then click  **View File System**.

Folder and File Icons

The following icons indicate where the file or folder is defined:

 - A virtual folder defined at the Web User level.

 - A virtual file defined at the Web User level.

 - A virtual folder defined at the Web User Group level.

 - A virtual file defined at the Web User Group level.

 - A folder not defined in Managed File Transfer. The folder permissions on are inherited from the parent.

 - A file not defined in Managed File Transfer. The file permissions are inherited from the parent folder.

Reset Web User Password

This feature allows you to reset the password for a Web User if their password is authenticated against the Managed File Transfer database.

1. Log in as an Admin User with the Web User Manager role.

2. From the main menu bar, select **Users**, and then click the **Web Users** link.
3. In the "Web User Management" on page 589 page, click the  Action icon next to the Web User.
4. From the drop-down list click the  icon.

Password Generation

Passwords for Web User accounts can be generated based on the "Web User Settings" on page 641. Otherwise, the Web User Manager can type in the password manually. If specifying the password, Managed File Transfer will alert you if the password does not meet the "Web User Settings" on page 641. The maximum password length is 20 characters.

Password Options

The password options allow you to choose how the new Web User password is handled. The following options can be specified when resetting the Web Users password:

Display password to the page

The new Web User password is displayed on the page.

Email password

The password is emailed to the Web User using a "Web User Email Templates" on page 812. If an email address is not defined for a Web User, this option is not available.

Force Password Change at Next Login

This option is only available to Web Users using the HTTPS service. If selected, this option will force a Web User to type a new password after a successful initial login.

Web User SSH Keys

The Web User SSH Keys page provides options to associate SSH keys to a Web User account by either importing keys or selecting existing keys. This allows the Web User to authenticate to the SFTP service using a public key as long as their account's authentication type is setup to allow public key authentication. A Web User can be associated with multiple SSH keys. A single SSH key can be shared across multiple Web Users.

To manage SSH keys for a Web User:

1. Log in as an Admin User with the **Web User Manager** role.
2. From the main menu bar, select **Users**, and then click the **Web Users** link.
3. In the Web Users page, click the  Action icon next to the Web User, and then click the  **SSH Keys** option.

Available Options

- Remove an associated SSH Key from a Web User by clicking the  icon. This will not delete the SSH key from the key store, but will just disassociate the SSH key from the Web User.
- "Import Public SSH Key" on page 743 an SSH Public Key for a Web User by clicking the **Import Public Key** button. Once the key is imported, it will become associated to the Web User account.
  - Select an existing SSH public key from the SSH Key Manager by clicking the **Select Existing Key** button. This action will launch a pop-up showing all public SSH keys that can be associated with the Web User. Click the name of a key in the list to select the key for the Web User.

Promote Web Users

One or more Web Users can be promoted to another Managed File Transfer server using the Promote Web User process.

To promote Web User Groups, follow the instructions below:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu, select **Users**, and then click the Web User Groups link.
3. In the "Web User Groups Management" on page 615 page, select the check boxes for the Web User Groups to promote and then click the **Promote** button.
4. On the Promote Web Groups page, specify the following:
   - **Replace Target Web User**- Select this option to migrate an updated Web User to the target. That is, you can replace a Web User in the target with the same name.
   - **Target Server**- The host name or IP address of the Managed File Transfer installation where the Web User Groups are being promoted. The value specified must be a URL of the form http://[host]:[port]/goanyhwere, where [host] is the host name or IP address of the target Managed File Transfer installation, and [port] is the port number on which Managed File Transfer is running, which by default is 8000. An example value would be http://10.1.4.1:8000/informaticamft.
   - **User Name**- A User account with the Web User Manager role on the target server.
   - **Password**- The password for the User account.
5. When complete, click the **Promote** button to promote the Web User Groups.
6. test

   test

Web User Groups

A Web User Group is an association of one or more "Admin Users" on page 576. Each Web User Group can be assigned specific permissions for controlling access to various Managed File Transfer functions. All Web Users belonging to a Web User Group will adopt the permissions from that Group.

For instance, you may want to create a Web User Group for employees that have both upload and download permissions and another Web User Group could be created for trading partners who can only download files.

Web User Groups Management

To manage Web User Groups, log in as an Admin User with the **Web User Manager** role.

From the main menu bar, select **Users**, and then click the Web User Groups link.

Page Toolbar

The following actions are available from the page toolbar:

- "Select Web User Group Type" on page 615 a Web User Group by clicking the **Add Web User Group** button.
- "Import Web User Groups From XML" on page 619 Web User Groups by clicking the **Import from XML** button.

Web User Groups Actions

The following actions are available by selecting the Actions icon:

- "Edit Web User Group" on page 619 a Web User Group by clicking the icon.
- "Web User Group Details" on page 621 Web User Group details by clicking the icon.
  - Delete a Web User Group by clicking the icon.
  - Click the **Promote** button to "Promote Web User Groups" on page 622 the selected Web User Groups to another Managed File Transfer server.
  - Click the **Export** button to export the selected Web User Group information to an XML file. The selected Web User Groups are saved in a file named "export-web-groups.xml" on your local computer.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Web User Groups.
- "Promote Web User Groups" on page 622 one or more selected Web User Groups to another Managed File Transfer server.
- Export the selected Web User Groups to an XML file. The selected Web User Groups are saved in a file named "export-web-groups.xml" on your local computer. This file can be used as a backup or for importing the Web User Groups to another Managed File Transfer instance.

Select Web User Group Type

When an LDAP Managed Login Method exists, you will be prompted to select the type of Web User Group to create. By default, the membership for the Web User Group is managed by Managed File Transfer. Select the LDAP Managed Group option if the group membership is maintained on the LDAP server.

Informatica Managed File Transfer Group

The Web Users associated in the group are defined by the Managed File Transfer administrator pages.

LDAP Managed Group

The Web Users associated in the group are defined by the LDAP Managed server.

Login Method – When LDAP Managed Group is selected, you must select an LDAP Login Method available from the "Login Methods Management" on page 647 page.

LDAP Group – Displays the available groups in the selected LDAP server.

Add Web User Group

Follow the instructions below to add a new Web User Group:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the Web User Groups link.
3. In the **Web User Groups** page, click the **Add Web User Group** link in the toolbar.
4. "Select Web User Group Type" on page 615 and then click Continue.
5. Type the Web User Group information in the appropriate boxes on the General tab.
6. Assign members (Web Users) to the Web User Group.
7. Click to select the folders and file permissions that will be assigned to the Web User Group on the Folders tab.
8. Click the **Save** button to add the Web User Group.

General

The General tab contains the following options:

Group Name

A unique name for the Web User Group.

Description

The optional description for the Group.

Protocols

The protocols to which the members of the Web User Group have access.

Share Drive

This option allows members of the Web User Group to use the Shared Drive file system for collaboration, sharing and synchronization of documents.

Shared Drive Access

When Shared Drive is enabled, you can select the access level for the Web User Group members:

- Full Licensed User: Members of this Web User Group can read, write, modify, delete, upload, download, synchronize files, and share files in Shared Drive.
- View Only: Members of this Web User Group can only read and download files that are shared with them by other Web Users.

Shared Drive Disk Space Limited

Disk quotas can be used to control the maximum Shared Drive storage space allowed for a Web User Group. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

Shared Drive uses the following rules to determine what is counted towards a Web User's maximum disk quota:

- All files and folders located in the user's Shared Drive workspace
- Files that are shared to a user when the user has accepted the shared file
- Files that have been deleted to the Trash Bin
- When multiple revisions of a file are available, only the current revision of the file is counted towards a user's disk quota.
  There are three options available on the Disk Space Limited field:
  - Blank (not specified): The Web User will have unlimited disk space, unless disk space is limited at the Web User Group level. This option is preferred when you want to control disk quotas from the Web User Group this user belongs to.
  - Yes: The disk space is limited for the Web User. When Shared Drive disk quotas are specified on both the Web User and Web User Group level, the highest value will be used. If the Web User Group this user belongs to does not have a disk limit (by selecting "No" on the Disk Space Limited field for the Web User Group), this user will be unlimited. If the Shared Drive Disk Space Limited field is unspecified on the Web User Group level, this user will be limited.
  - No: This user does not have a disk quota. This setting will take precedence over any limit specified on the Web User Group level.

Shared Drive Disk Space Limited

The maximum amount of disk space available for the Web User Group in Shared Drive.

Secure Folders

The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Secure Mail

This option allows Web User Group members to send Secure Mail through the File Transfer Portal.

Send Invitations

Web User Group members logged in to the File Transfer Portal can invite other individuals to "Web User Self-Registration" on page 645 when this option is active.

View Activity Report

This option allows Web User Group members to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view login activity, along with file upload and download information.

Max Concurrent Sessions

The total number of active sessions a Web User Group members can have open at any one time across all available services. If this field is left blank, the Web User is permitted to have unlimited concurrent sessions.

Allow Users to Change Password

This option makes a Change Password link available at the top of the page in the File Transfer Portal for members of the Web User Group.

Members

The Web User Group members can be managed from Managed File Transfer or an LDAP Managed server. The following options are based on the group membership type:

Folders

Multiple folders and files can be authorized to a Web User Group from the Folders tab. These folders and files can have individual permissions assigned, which are inherited by all Web Users belonging to the Web User Group. Folder and file paths can point to locations on the local file system or other file systems on the network. If defining virtual folders that are relative to the Web User's home directory (using the ${homeDirectory} variable in the path name), a prompt will allow you to automatically create these folders for all Web Users belonging to the group.

The disk quota settings control the total storage space for each Web User. Files uploaded that exceed the disk quota are not saved. The amount of space used per Web User and a summary of the files and folders to which they have access is available on the "View Web User File System" on page 612 page.

Learn more about virtual folders and how they are configured in "Virtual Folders and Files" on page 586.

Note: If the Web User has a virtual folder or file defined with the same alias as the Group to which they belong, the Web User's defined virtual folder or file will take precedence.

Informatica Managed File Transfer Group

The Web Users are split in two columns. The column on the left displays the available members who do not belong to this Group. The column on the right displays the members who are assigned to this Group. Click to select members individually or all Web Users by clicking the checkbox in the heading and then use the direction buttons between the columns to move members to the appropriate side.

Assigning Web Users to a Web User Group

Perform the following steps to assign Web Users to a Web User Group:

1. On the left side of the page, click to select the Web User(s) to assign to the Web User Group.
2. When the desired Web Users are selected, click the >> arrow between the group boxes to move the Web Users from left to right.
3. Click the **Save** button to apply the changes.

Removing Web Users from a Web User Group

Perform the following steps to remove Web Users from a Web User Group:

1. On the right side of the page, click to select the Web User(s) to remove from the group.
2. When the desired Web Users are selected, click the << arrow between the group boxes to move the Web Users from right to left.
3. Click the **Save** button to apply the changes.

LDAP Managed Group

Membership for LDAP Managed Web User Groups is maintained by the LDAP server. The Members tab displays read-only attributes for which LDAP group it is associated with.

Managed by Login Method

Displays the LDAP Managed Login Method name.

Group Distinguished Name

Displays the group DN from the "Add LDAP Server" on page 651.

Import Web User Groups From XML

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the **Web User Groups** link.
3. In the Web Users Groups page, click the  Import Web Users link in the toolbar.
4. On the Import Web Users From XML page, specify the following:
   Import From

   The XML file can be imported from either a file on the end user's PC or a file on the source Managed File Transfer server.

   Input File

   The path or location of the XML file containing the import information.

   Ignore User Membership

   When a Web User Group is exported, the XML file contains a list of Web Users that are associated with the Web User Group. When importing, this option can be specified to ignore all Web Users associated with the Web User Group. If this option is not specified and Web Users are listed in the XML file, those Web Users must already exist in Managed File Transfer. When importing Web User Groups and Web Users from another system, it is recommended to first import the Web User Groups using the Ignore User Membership option and then import the Web Users. The Web Users will be associated to the Web User Groups when they are imported.
5. When complete, click the Import button. A message on the page displays the import results.

   Note: It is not recommended to import Web User Groups from an XML file created outside of Managed File Transfer.

Edit Web User Group

Follow the instructions below to edit a Web User Group:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the Web User Groups link.
3. In the **Web User Groups** page, click the  icon beside the Web User Group you wish to edit.
4. Change the desired Web User Group information on the General tab.
5. Click to select the folders and file permissions for the Web User Group on the Folders tab.
6. Click the **Save** button to finish editing the Web User Group.

General

The General tab contains the following options:

Group Name

A unique name for the Web User Group.

Description

The optional description for the Group.

Protocols

The protocols to which the members of the Web User Group have access.

Share Drive

This option allows members of the Web User Group to use the Shared Drive file system for collaboration, sharing and synchronization of documents.

Shared Drive Access

When Shared Drive is enabled, you can select the access level for the Web User Group members:

- Full Licensed User: Members of this Web User Group can read, write, modify, delete, upload, download, synchronize files, and share files in Shared Drive.
- View Only: Members of this Web User Group can only read and download files that are shared with them by other Web Users.

Shared Drive Disk Space Limited

Disk quotas can be used to control the maximum Shared Drive storage space allowed for a Web User Group. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

Shared Drive uses the following rules to determine what is counted towards a Web User's maximum disk quota:

- All files and folders located in the user's Shared Drive workspace
- Files that are shared to a user when the user has accepted the shared file
- Files that have been deleted to the Trash Bin
- When multiple revisions of a file are available, only the current revision of the file is counted towards a user's disk quota.
  There are three options available on the Disk Space Limited field:
  - Blank (not specified): The Web User will have unlimited disk space, unless disk space is limited at the Web User Group level. This option is preferred when you want to control disk quotas from the Web User Group this user belongs to.
  - Yes: The disk space is limited for the Web User. When Shared Drive disk quotas are specified on both the Web User and Web User Group level, the highest value will be used. If the Web User Group this user belongs to does not have a disk limit (by selecting "No" on the Disk Space Limited field for the Web User Group), this user will be unlimited. If the Shared Drive Disk Space Limited field is unspecified on the Web User Group level, this user will be limited.
  - No: This user does not have a disk quota. This setting will take precedence over any limit specified on the Web User Group level.

Shared Drive Disk Space Limited

The maximum amount of disk space available for the Web User Group in Shared Drive.

Secure Folders

The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Secure Mail

This option allows Web User Group members to send Secure Mail through the File Transfer Portal.

Send Invitations

Web User Group members logged in to the File Transfer Portal can invite other individuals to "Web User Self-Registration" on page 645 when this option is active.

View Activity Report

This option allows Web User Group members to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view login activity, along with file upload and download information.

Max Concurrent Sessions

The total number of active sessions a Web User Group members can have open at any one time across all available services. If this field is left blank, the Web User is permitted to have unlimited concurrent sessions.

Allow Users to Change Password

This option makes a Change Password link available at the top of the page in the File Transfer Portal for members of the Web User Group.

Members

The Web Users associated to a Web User Group can be managed from Managed File Transfer or an LDAP Managed server. The following options are based on the group membership type:

Folders

Multiple folders and files can be authorized to a Web User Group from the Folders tab. These folders and files can have individual permissions assigned, which are inherited by all Web Users belonging to the Web User Group. Folder and file paths can point to locations on the local file system or other file systems on the network. If defining virtual folders that are relative to the Web User's home directory (using the ${homeDirectory} variable in the path name), a prompt will allow you to automatically create these folders for all Web Users belonging to the group.

The disk quota settings control the total storage space for each Web User. Files uploaded that exceed the disk quota are not saved. The amount of space used per Web User and a summary of the files and folders to which they have access is available on the "View Web User File System" on page 612 page.

Learn more about virtual folders and how they are configured in "Virtual Folders and Files" on page 586.

Note: If the Web User has a virtual folder/file defined with the same alias as the Group to which they belong, the Web User's defined virtual folder/file will take precedence.

Web User Group Details

The Web User Group Details page shows the properties for the Web User Group, as well as the Web User Templates and Web User Members assigned to that Group. Follow the instructions below to view the Web User Group Details:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu, select **Users**, and then click the Web User Groups link.
3. In the "Web User Groups Management" on page 615 page, click the  icon next to the Web User Group.

Promote Web User Groups

One or more Web User Groups can be promoted to another Managed File Transfer server using the Promote Web User Groups process.

One or more Web User Groups can be promoted to another Managed File Transfer server using the Promote Web User Groups process.

To promote Web User Groups, follow the instructions below:

1. Log in as an Admin User with the Web User Manager role.
2. Verify the Web User Groups and Web User Templates settings on the target server match the settings of the source server.
3. In the Web User Groups page, select the check boxes for the Web User Groups to promote and then click the Promote button.
4. On the Promote Web Groups page, specify the following:
   - **Target Server** - The host name or IP address of the Managed File Transfer installation where the Web User Groups are being promoted. The value specified must be a URL of the form http://[host]:[port]/informaticamft, where [host] is the host name or IP address of the target Managed File Transfer installation, and [port] is the port number on which Managed File Transfer is running, which by default is 8000. An example value would be http://10.1.4.1:8000/informaticamft.
   - User Name - A User account with the Web User Manager role on the target server.
   - Password - The password for the User account.
   - Ignore User Membership - A Web User Group is typically linked to a number of Web Users. When promoting a Web User Group, this option can be specified to ignore all Web Users associated with the Web User Group. If this option is not specified, the Web Users associated with that group must already exist in Managed File Transfer on the target system. When promoting Web User Groups and Web Users from one system to another, it is recommended to first promote the Web User Groups using the Ignore User Membership option and then promote the Web Users. The Web Users will be associated to the Web User Groups when they are promoted.
5. When complete, click the Promote button to promote the Web User Groups.

Web User Templates

Web User Templates provide a method to configure the default account settings when new Web Users are created. By defining templates that share common settings (authentication, permissions, account expirations, etc.), this can dramatically reduce the time needed to create new Web User accounts.

For example, a template could be defined for internal employees with all service and command permissions, Active Directory authentication and no account expiration. Another template could be defined for trading partners to authenticate against Managed File Transfer with limited account permissions and the account automatically expires after 30 days. With these templates defined, Web User creation can be as simple as specifying the Web User name and other general information like a first and last name, phone number and email address.

Web User Template Management

To manage Web User Templates, log in as an Admin User with the **Web User Manager** role.

From the main menu bar, select **Users**, and then click the Web User Templates link.

Page Toolbar

The following actions are available from the page toolbar:

- "Add Web User Template" on page 623 a Web User Template by clicking the **Add Web User Template** link in the toolbar.
  - Click the **Edit** button to change the Default template for adding Web Users. Click the **Save** button to apply the change.

Web User Template Actions

The following actions are available by selecting the Actions icon:

- "Web User Template Details" on page 640 Web User Template details by clicking the icon.
- "Edit Web User Template" on page 632 a Web User Template by clicking the icon.
  - Delete a Web User Template by clicking the icon. The default Web User Template cannot be deleted.
- "Add Web User" on page 591 a new Web User based on the corresponding template by clicking the icon.

Add Web User Template

A Web User template can be created using the Add Web User Template page. Follow the instructions below to add a Web User Template:

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the Web User Templates link.
3. In the "Web User Template Management" on page 623 page, click the Add Web User Template link in the page toolbar.
4. Type the Web User template information in the appropriate boxes.
5. Click the **Save** button to create the Web User template.

General

The General tab has the following fields:

Name

A unique name for the Web User Template.

Description

This is optional space to further describe the Web User Template. This field is limited to 512 characters.

Authentication

The Authentication tab has the following fields:

Login Method

Specify which technique should be used to authenticate the Web User. Valid methods are Azure Active Directory, Microsoft Active Directory (AD), Generic LDAP, Informatica Domain Authentication, Okta Multi Factor Authentication, IBM i user profiles, LDAP Managed server(s), and the Managed File Transfer database. The valid methods are defined on the "Login Methods Management" on page 647 page.

When the default option is selected, the Web User will use the default Login Method for Web Users specified in the "Login Methods Management" on page 647 page. To authenticate against another Login Method, clear the checkbox and select it from the drop-down list. The password options are only shown when authentication is performed against the Managed File Transfer database.

Password Generation

Passwords for Web User accounts can be generated automatically based on the "Web User Settings" on page 641. Otherwise the Web User Manager creating the account can manually specify a password. If specifying the password, Managed File Transfer will alert you if the password does not meet the "Web User Settings" on page 641. The maximum password length is 20 characters.

Password Options

If authenticating the Web User account against the Managed File Transfer database, the following options can be specified for the Web User password:

- Display password to the page - The new Web User password is displayed on the page.
- Email password - The password is emailed to the Web User using a "Web User Email Templates" on page 812.
- Allow User to Change Password - This option makes a Change Password link available at the top of the page in the HTTPS File Transfer Portal.
- Force Password Change at Next Login - This option is only available to Web Users using the HTTPS service. If selected, this option will force a Web User to type a new password after a successful initial login.

Password Expiration Interval

>If authenticating the Web User account against the Managed File Transfer database, the password expiration interval determines how long before a password expires.

- Default - The Password Expiration Interval is defined in the "Web User Settings" on page 641
- Password Never Expires
- Password Expires After - The Web User password will expire after the specified number of days.

Authentication Types

The Authentication Type can be specified per service. This provides the Web User Manager with complete control over the Web User's access. For example, a Web User can be forced to use a Password and Certificate when authenticating to FTPS but only require a Password for HTTPS. If a certificate is used for authentication, the Client Authentication setting on the SSL tab of the specific "Service Manager" on page 516 must be set to Optional or Required.

If certificate authentication is specified and the certificate being used is either self-signed or signed by an untrusted Certificate Authority (CA), then the certificate will need to be "Import SSL Certificate" on page 737 into the Default Trusted Certificates Key Store. Importing the certificate instructs Managed File Transfer to trust this source. If the certificate being used is already signed by a trusted authority (for

example, Verisign, GoDaddy, Equifax, etc.) the certificate does not need to be imported since the trust is inherited.

HTTPS

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box. Each Web User must have a unique SHA1 Fingerprint.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the unique SHA1 Fingerprint for the Web User's certificate in the box.

AS2

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type a SHA1 Fingerprint for the Web User's certificate in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with a shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPES (Explicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not

require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
You can select one of the following digest algorithm:

- SHA1
- SHA224
- SHA256
- SHA384
- SHA512

- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPS (Implicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

SFTP

- Password - Web Users login using their standard Web User name and password.
- Public Key - Web Users use a public key on the server to encrypt a session key that produces a secure login.
- Either - If a matching public key is found during the connection, the Web User will automatically pass authentication. However if a key match is not found, the Web User can still login to the Managed File Transfer server with a user name and password.
- Password and Public Key - Web Users must login using their Web User name and password along with a public key.

Groups

Web Users can belong to one or more Web User Groups. A Web User will adopt the permissions from any Web User Groups they belong to. They will also have access to any folders which the Web User Groups are authorized to access.

The Web User Groups are split in two columns. The column on the left displays the available Groups to which the Web User Template is not a member. The column on the right displays the Groups in which the Web User Template is a member. Click to highlight groups and then use the direction buttons between the columns to move Groups to the appropriate side.

Assigning Web User Groups to a Web User Template

Perform the following steps to assign Web User Groups to a Web User Template:

1. On the left side of the page, click to select (highlight) the Web User Group(s) to assign to the Web User Template. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Web User Groups are selected, click the → button between the Group boxes to move the Web User Groups from left to right.
3. Click the **Save** button to apply the changes.
   Removing Web Users Groups from a Web User Template

   Perform the following steps to remove Web User Groups from a Web User Template:
4. On the right side of the page, click to select (highlight) the Web User Group(s) to remove from the Web User Template. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
5. When the desired Web User Groups are selected, click the ← button between the group boxes to move the Web User Groups from right to left.
6. Click the **Save** button to apply the changes.

   Note: For ease of Web User management, it is generally not recommended to give individual permissions to a Web User. Instead, assign each Web User to one or more Web User Groups, from which the Web User will adopt the permissions assigned to those Web User groups. This allows you to quickly adjust permissions for several Web Users at once by changing the permissions for the Web User Group(s) in which they belong.

Features

The Features tab contains the following options:

Protocols

Select the services the Web User can use for performing file transfers. If the Web User is a member of a group, these services are in addition to the services inherited from the group.

Share Drive

This option provides Web Users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents. This option can also be enabled at the "Web User Groups Management" on page 615 level.

Shared Drive Access

When Shared Drive is enabled for the Web User, you can select the Web User's access level to this feature:

- Full Licensed User: This is a fully licensed user that can read, write, modify, delete, upload, download, synchronize files, and share files in Shared Drive.

- View Only: This is a limited user that can only read and download files that are shared with them by other Web Users.

Shared Drive Disk Space Limited

Disk quotas can be used to control the maximum Shared Drive storage space allowed for a Web User. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

Shared Drive uses the following rules to determine what is counted towards a Web User's maximum disk quota:

- All files and folders located in the user's Shared Drive workspace
- Files that are shared to a user when the user has accepted the shared file
- Files that have been deleted to the Trash Bin
- When multiple revisions of a file are available, only the current revision of the file is counted towards a user's disk quota.
  There are three options available on the Disk Space Limited field:
  - Blank (not specified): The Web User will have unlimited disk space, unless disk space is limited at the Web User Group level. This option is preferred when you want to control disk quotas from the Web User Group this user belongs to.
  - Yes: The disk space is limited for the Web User. When Shared Drive disk quotas are specified on both the Web User and Web User Group level, the highest value will be used. If the Web User Group this user belongs to does not have a disk limit (by selecting "No" on the Disk Space Limited field for the Web User Group), this user will be unlimited. If the Shared Drive Disk Space Limited field is unspecified on the Web User Group level, this user will be limited.
  - No: This user does not have a disk quota. This setting will take precedence over any limit specified on the Web User Group level.

Shared Drive Disk Space Limited

The maximum amount of disk space available for this Web User in Shared Drive.

Secure Folders

The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Secure Mail

This option provides a Web User with the ability to send Secure Mail through the File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Invitations

Web Users logged in to the File Transfer Portal can invite other individuals to "Web User Self-Registration" on page 645 when this option is active.

View Activity Report

This option allows Web Users to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.

Max Concurrent Sessions

The total number of active sessions a Web User can have open at any one time across all available services. If this field is left blank, the Web User is permitted to have unlimited concurrent sessions.

Folders

A Web User can be authorized to one or more folders or files, which may be located on the local file system or other file systems on the network. When creating a Web User, the virtual folders and files defined in the template will be assigned to the Web User. These folders and files can be later modified at the Web User level. More information about virtual folders and disk quotas is available on the "Virtual Folders and Files" on page 586 page.

For example, if each Web User should have an Inbound and Outbound directory, then there should be two sub-folders defined on the Web User Template with paths of ${homeDirectory}/Inbound and ${homeDirectory}/Outbound respectively.

Home Directory Variables

When defining the home directory for a template, variables can be specified within the directory path by clicking the `${var}` icon. To combine text with one or more variables, hold the Ctrl key while selecting the variable from the drop-down list. The following variables are supported:

Variable	Description
${user.name}	The Web User account name.
${user.firstName}	The first name of the Web User.
${user.lastName}	The last name of the Web User.
${user.organization}	The Web User's organization.
${user.email}	The email address of the Web User.

Multiple variables can be used within the path name, for example: C:\webdocs\${user.organization}\${user.name}.

IP Filter

The IP filter can be used to indicate which IP addresses are allowed or restricted when the Web User connects to Managed File Transfer. Both IPv4 and IPv6 address formats are supported.

Enable IP Filter

The IP Filter can be enabled or disabled at the individual Web User level.

Filter Type

Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others. In most cases a "IP Filter" on page 780 is set to Blacklist addresses that are known threats. At the Web User level, it is common to specify a white list of allowable addresses.

Filter Entries

The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above. Click a row to type an IP address in either single, range, or CIDR notation format. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255). A red flag on an entry simply indicates that it is a new entry.

Note: Note: A single IPv4 address is comprised of four sets of three numbers from 0 to 255, separated by periods. A single IPv6 address is comprised of eight sets of four hexidecimal numbers, separated by colons. An IP range includes all the addresses between two specified addresses. The addresses are separated by a hyphen. An IP address in CIDR notation is an IP address followed by a "prefix." The prefix notates a range of IP addresses without the need to type all the sets.

Time Limits

The Time Limits tab allows specifying options for expiring Web User accounts after a certain number of days. Options are also provided to limit times of day and weekdays on which a Web User can login.

The Time Limits tab contains the following settings:

Account Expires On

This option can automatically expire Web User accounts based on the number of days after the account was created.

Limit Time of Day

To limit the time period in which the Web User can login, choose the "Only allow between..." option and then specify the range.

Limit Days of Week

To limit which days of the week the Web User can login, choose the "Only allow on..." option and then select the days.

Disable Account When No Activity

The Web User account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.

- Default - The Disable Inactive Account value is defined on the General tab of "Web User Settings" on page 641
- Never - The account will not disable based on inactivity.
- Disable account after - The Web User account will become disabled after the specified number of inactive days.

Expire Account After Creation

AS2

The AS2 tab allows specifying properties for receiving AS2 messages from the Web User. Additional AS2 information is located in the "Quick Start for AS2" on page 520.

The AS2 tab contains the following settings:

AS2 ID

The AS2 ID of the sender (Web User). The AS2 ID is case sensitive and can be 1 to 128 ASCII printable characters in length.

Signature Certificate Alias

This is the alias of the public certificate used by this Web User to sign their messages. If the certificate is signed by a certificate authority (for example, Verisign), this field can be left blank since the certificate chain already exists in the Default Trusted Certificates Key Store. If a specific certificate is to be used by the Web User for signing messages or they use a self-signed certificate, then that certificate should be

imported into the Default Trusted Certificates Key Store. If you do not know the alias name for the certificate, click the  icon to select the certificate alias.

Default Upload Folder

The location where AS2 messages are saved when received (uploaded). The default location is the default home directory for the Web User, which is the [installdirectory]/userdata/webdocs/[webuser] folder, where [installdirectory] is the installation directory of Managed File Transfer and [webuser] is the account name of the Web User. If files for this Web User should be saved in a different location, use the Other... option to manually type a folder location (for example, inbound/as2).

When File Exists

The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.

Require Encryption

This option indicates whether or not messages sent by this Web User must be encrypted.

Require Signature

A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this Web User will be rejected.

Require Authentication

Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the AS2 ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.

Asynchronous MDN Approval

If a return receipt is requested by the Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed. The  icon on the AS2 Log page indicates a manual receipt needs to be sent for a message. A manual receipt can only be sent if a message is received successfully. If an error occurs during transmission, an asynchronous receipt is sent automatically.

Upload Restrictions

You can restrict the web users on the files to upload to the Managed File Transfer system. You can configure these restrictions using the web user template. Upload restrictions don't apply to MLLP protocol.

The Upload Restrictions tab contains the following options:

Allow Files with No Extension

Select this option to allow web users to upload files that don't have extensions.

Allow Files with an Extension

Select this option to allow web users to upload files that have extensions. The web users must enter the file extensions in the **File Extension Filter** field.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or permit specific extensions. To specify the file types web users can or can't upload, enter the file extensions in this box. Enter extensions without periods (.), separate them with commas, and don't add line breaks or spaces. For example, to allow .txt, .xls, .xlsx and .csv files, enter txt,xls,xlsx,csv. The maximum number of characters for this field is 2,000.

Case Sensitive

Select this option to specify that file extensions are case sensitive.

Edit Web User Template

Use this feature to edit the properties for an existing Web User Template.

1. Log in as an Admin User with the Web User Manager role.
2. From the main menu bar, select **Users**, and then click the Web User Templates link.
3. In the "Web User Template Management" on page 623 page, click the  icon next to the Web User template.
4. Modify the field values for the Web User template.
5. Click the **Save** button to save the settings.

General

The General tab has the following fields:

Name

A unique name for the Web User Template.

Description

This is optional space to further describe the Web User Template. This field is limited to 512 characters.

Authentication

The Authentication tab has the following fields:

Login Method

Specify which technique should be used to authenticate the Web User. Valid methods are Azure Active Directory, Microsoft Active Directory (AD), Generic LDAP, Informatica Domain Authentication, Okta Multi Factor Authentication, IBM user profiles, LDAP Managed server(s), and the Managed File Transfer database. The valid methods are defined on the "Login Methods Management" on page 647 page.

When the default option is selected, the Web User will use the default Login Method for Web Users specified in the "Login Methods Management" on page 647 page. To authenticate against another Login Method, clear the checkbox and select it from the drop-down list. The password options are only shown when authentication is performed against the Managed File Transfer database.

Password Generation

Passwords for Web User accounts can be generated automatically based on the "Web User Settings" on page 641. Otherwise the Web User Manager creating the account can manually specify a password. If specifying the password, Managed File Transfer will alert you if the password does not meet the "Web User Settings" on page 641. The maximum password length is 20 characters.

Password Options

If authenticating the Web User account against the Managed File Transfer database, the following options can be specified for the Web User password:

- Display password to the page - The new Web User password is displayed on the page.

- Email password - The password is emailed to the Web User using a "Web User Email Templates" on page 812.
- Allow User to Change Password - This option makes a Change Password link available at the top of the page in the HTTPS File Transfer Portal.
- Force Password Change at Next Login - This option is only available to Web Users using the HTTPS service. If selected, this option will force a Web User to type a new password after a successful initial login.

Password Expiration Interval

>If authenticating the Web User account against the Managed File Transfer database, the password expiration interval determines how long before a password expires.

- Default - The Password Expiration Interval is defined in the "Web User Settings" on page 641
- Password Never Expires
- Password Expires After - The Web User password will expire after the specified number of days.

Authentication Types

The Authentication Type can be specified per service. This provides the Web User Manager with complete control over the Web User's access. For example, a Web User can be forced to use a Password and Certificate when authenticating to FTPS but only require a Password for HTTPS. If a certificate is used for authentication, the Client Authentication setting on the SSL tab of the specific "Service Manager" on page 516 must be set to Optional or Required.

If certificate authentication is specified and the certificate being used is either self-signed or signed by an untrusted Certificate Authority (CA), then the certificate will need to be "Import SSL Certificate" on page 737 into the Default Trusted Certificates Key Store. Importing the certificate instructs Managed File Transfer to trust this source. If the certificate being used is already signed by a trusted authority (for example, Verisign, GoDaddy, Equifax, etc.) the certificate does not need to be imported since the trust is inherited.

HTTPS

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box. Each Web User must have a unique SHA1 Fingerprint.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the unique SHA1 Fingerprint for the Web User's certificate in the box.

AS2

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a user name or password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type a SHA1 Fingerprint for the Web User's certificate in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with a shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPES (Explicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
  You can select one of the following digest algorithm:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

FTPS (Implicit SSL)

- Password - Web Users login using their standard Web User name and password.
- Certificate - Web Users are authenticated by a certificate which must be in the Managed File Transfer Default Trusted Key Store and on the Web User's local computer. This method does not

require the Web User to specify a password any time they use Managed File Transfer. On enabling the Certificate authentication type, select the **Digest Algorithm** from the menu, and enter the corresponding fingerprint for the Web User's certificate in the box.
You can select one of the following digest algorithm:

- SHA1
- SHA224
- SHA256
- SHA384
- SHA512

- Either - If a matching certificate is found during the connection, the Web User will automatically authenticate. However if a match is not found, the Web User can still login to the Managed File Transfer server with a user name and password. If Either is selected, type the certificate's SHA1 Fingerprint in the box.
- Password and Certificate - Web Users are authenticated by their standard Web User name and password along with shared certificate that is both on the Managed File Transfer server and the Web Users' local computer. Type the certificate's SHA1 Fingerprint in the box.

SFTP

- Password - Web Users login using their standard Web User name and password.
- Public Key - Web Users use a public key on the server to encrypt a session key that produces a secure login.
- Either - If a matching public key is found during the connection, the Web User will automatically pass authentication. However if a key match is not found, the Web User can still login to the Managed File Transfer server with a user name and password.
- Password and Public Key - Web Users must login using their Web User name and password along with a public key.

Groups

Web Users can belong to one or more Web User Groups. A Web User will adopt the permissions from any Web User Groups they belong to. They will also have access to any folders which the Web User Groups are authorized to access.

The Web User Groups are split in two columns. The column on the left displays the available Groups to which the Web User Template is not a member. The column on the right displays the Groups in which the Web User Template is a member. Click to highlight groups and then use the direction buttons between the columns to move Groups to the appropriate side.

Assigning Web User Groups to a Web User Template

Perform the following steps to assign Web User Groups to a Web User Template:

1. On the left side of the page, click to select (highlight) the Web User Group(s) to assign to the Web User Template. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Web User Groups are selected, click the → button between the Group boxes to move the Web User Groups from left to right.
3. Click the **Save** button to apply the changes.
   Removing Web Users Groups from a Web User Template

   Perform the following steps to remove Web User Groups from a Web User Template:
4. On the right side of the page, click to select (highlight) the Web User Group(s) to remove from the Web User Template. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
5. When the desired Web User Groups are selected, click the ← button between the group boxes to move the Web User Groups from right to left.
6. Click the **Save** button to apply the changes.

   Note: For ease of Web User management, it is generally not recommended to give individual permissions to a Web User. Instead, assign each Web User to one or more Web User Groups, from which the Web User will adopt the permissions assigned to those Web User groups. This allows you to quickly adjust permissions for several Web Users at once by changing the permissions for the Web User Group(s) in which they belong.

Features

The Features tab contains the following options:

Protocols

Select the services the Web User can use for performing file transfers. If the Web User is a member of a group, these services are in addition to the services inherited from the group.

Share Drive

This option provides Web Users the ability to use the Shared Drive file system for collaboration, sharing and synchronization of documents. This option can also be enabled at the "Web User Groups Management" on page 615 level.

Shared Drive Access

When Shared Drive is enabled for the Web User, you can select the Web User's access level to this feature:

- Full Licensed User: This is a fully licensed user that can read, write, modify, delete, upload, download, synchronize files, and share files in Shared Drive.

- View Only: This is a limited user that can only read and download files that are shared with them by other Web Users.

Shared Drive Disk Space Limited

Disk quotas can be used to control the maximum Shared Drive storage space allowed for a Web User. If a Web User attempts to upload a file which would exceed their disk quota, Managed File Transfer will cancel the transfer and return an error to the Web User.

Shared Drive uses the following rules to determine what is counted towards a Web User's maximum disk quota:

- All files and folders located in the user's Shared Drive workspace
- Files that are shared to a user when the user has accepted the shared file
- Files that have been deleted to the Trash Bin
- When multiple revisions of a file are available, only the current revision of the file is counted towards a user's disk quota.
  There are three options available on the Disk Space Limited field:
  - Blank (not specified): The Web User will have unlimited disk space, unless disk space is limited at the Web User Group level. This option is preferred when you want to control disk quotas from the Web User Group this user belongs to.
  - Yes: The disk space is limited for the Web User. When Shared Drive disk quotas are specified on both the Web User and Web User Group level, the highest value will be used. If the Web User Group this user belongs to does not have a disk limit (by selecting "No" on the Disk Space Limited field for the Web User Group), this user will be unlimited. If the Shared Drive Disk Space Limited field is unspecified on the Web User Group level, this user will be limited.
  - No: This user does not have a disk quota. This setting will take precedence over any limit specified on the Web User Group level.

Shared Drive Disk Space Limited

The maximum amount of disk space available for this Web User in Shared Drive.

Secure Folders

The Secure Folders option provides Web Users the ability to work with authorized network folders and files from within the browser-based File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Secure Mail

This option provides a Web User with the ability to send Secure Mail through the File Transfer Portal. This feature can also be enabled at the "Web User Groups Management" on page 615 level.

Send Invitations

Web Users logged in to the File Transfer Portal can invite other individuals to "Web User Self-Registration" on page 645 when this option is active.

View Activity Report

This option allows Web Users to view their own activity report from the Managed File Transfer File Transfer Portal. Web Users will be able to view their login activity, as well as audit logs on their file uploads and downloads.

Max Concurrent Sessions

The total number of active sessions a Web User can have open at any one time across all available services. If this field is left blank, the Web User is permitted to have unlimited concurrent sessions.

Folders

A Web User can be authorized to one or more folders or files, which may be located on the local file system or other file systems on the network. When creating a Web User, the virtual folders and files defined in the template will be assigned to the Web User. These folders and files can be later modified at the Web User level. More information about virtual folders and disk quotas is available on the "Virtual Folders and Files" on page 586 page.

For example, if each Web User should have an Inbound and Outbound directory, then there should be two sub-folders defined on the Web User Template with paths of ${homeDirectory}/Inbound and ${homeDirectory}/Outbound respectively.

Home Directory Variables

When defining the home directory for a template, variables can be specified within the directory path by clicking the ${var} icon. To combine text with one or more variables, hold the Ctrl key while selecting the variable from the drop-down list. The following variables are supported:

Variable	Description
${user.name}	The Web User account name.
${user.firstName}	The first name of the Web User.
${user.lastName}	The last name of the Web User.
${user.organization}	The Web User's organization.
${user.email}	The email address of the Web User.

Multiple variables can be used within the path name, for example: C:\webdocs\${user.organization}\${user.name}.

IP Filter

The IP filter can be used to indicate which IP addresses are allowed or restricted when the Web User connects to Managed File Transfer. Both IPv4 and IPv6 address formats are supported.

Enable IP Filter

The IP Filter can be enabled or disabled at the individual Web User level.

Filter Type

Blacklist will deny any specified addresses and permit all others, whereas a Whitelist will only permit the specified addresses and deny all others. In most cases a "IP Filter" on page 780 is set to Blacklist addresses that are known threats. At the Web User level, it is common to specify a white list of allowable addresses.

Filter Entries

The Filter Entries is a list of IP addresses that will either be denied or permitted based on the Filter Type selected above. Click a row to type an IP address in either single, range, or CIDR notation format. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255). A red flag on an entry simply indicates that it is a new entry.

Note: Note: A single IPv4 address is comprised of four sets of three numbers from 0 to 255, separated by periods. A single IPv6 address is comprised of eight sets of four hexidecimal numbers, separated by colons. An IP range includes all the addresses between two specified addresses. The addresses are separated by a hyphen. An IP address in CIDR notation is an IP address followed by a "prefix." The prefix notates a range of IP addresses without the need to type all the sets.

Time Limits

The Time Limits tab allows specifying options for expiring Web User accounts after a certain number of days. Options are also provided to limit times of day and weekdays on which a Web User can login.

The Time Limits tab contains the following settings:

Account Expires On

If you would like the Web User account to expire on a certain date, enter or select the date. If specified, the Web User will not be able to login on or after that date.

Limit Time of Day

To limit the time period in which the Web User can login, choose the "Only allow between..." option and then specify the range.

Limit Days of Week

To limit which days of the week the Web User can login, choose the "Only allow on..." option and then select the days.

Disable Account When No Activity

The Web User account can be disabled after a number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified.

- Default - The Disable Inactive Account value is defined on the General tab of "Web User Settings" on page 641
- Never - The account will not disable based on inactivity.
- Disable account after - The Web User account will become disabled after the specified number of inactive days.

AS2

The AS2 tab allows specifying properties for receiving AS2 messages from the Web User. Additional AS2 information is located in the "Quick Start for AS2" on page 520.

The AS2 tab contains the following settings:

Default Upload Folder

The location where AS2 messages are saved when received (uploaded). The default location is the default home directory for the Web User, which is the [installdirectory]/userdata/webdocs/[webuser] folder, where [installdirectory] is the installation directory of Managed File Transfer and [webuser] is the account name of the Web User. If files for this Web User should be saved in a different location, use the Other... option to manually type a folder location (for example, inbound/as2).

When File Exists

The action that Managed File Transfer performs when a file with the same name already exists in the default upload folder.

Require Encryption

This option indicates whether or not messages sent by this Web User must be encrypted.

Require Signature

A signed message contains a digital signature from the sender to further authenticate the message. If signatures are required, any unsigned message sent by this Web User will be rejected.

Require Authentication

Require username/password or certificate authentication for messages uploads. If authentication is not required, Managed File Transfer will use the AS2 ID to identify the Web User. Informatica recommends you set the 'Require Signature' option to 'true' when authentication is not required.

Asynchronous MDN Approval

If a return receipt is requested by the Web User, select if the MDN will be sent automatically during the Web User's session or manually after the message is processed. The  icon on the AS2 Log page indicates a manual receipt needs to be sent for a message. A manual receipt can only be sent if a message is received successfully. If an error occurs during transmission, an asynchronous receipt is sent automatically.

Upload Restrictions

You can restrict the web users on the files to upload to the Managed File Transfer system. You can configure these restrictions using the web user template. Upload restrictions don't apply to MLLP protocol.

The Upload Restrictions tab contains the following options:

Allow Files with No Extension

Select this option to allow web users to upload files that don't have extensions.

Allow Files with an Extension

Select this option to allow web users to upload files that have extensions. The web users must enter the file extensions in the **File Extension Filter** field.

File Extension Filter

The file extension filter can permit all files, restrict specific extensions or permit specific extensions. To specify the file types web users can or can't upload, enter the file extensions in this box. Enter extensions without periods (.), separate them with commas, and don't add line breaks or spaces. For example, to allow .txt, .xls, .xlsx and .csv files, enter txt,xls,xlsx,csv. The maximum number of characters for this field is 2,000.

Case Sensitive

Select this option to specify that file extensions are case sensitive.

Web User Template Details

The Web User Template Details page shows the properties for the template.

Web User Settings

The Web User Settings page allows you to define the global security settings and password policies for Web Users.

To manage the Web User Settings, log in as an Admin User with the **Security Officer** role.

From the main menu bar, select **Users**, and then click the Web User Settings link.

The settings are broken out over six tabs named General, Password Policy, User Name Policy, Profile, Anonymous, and Folders.

General

Disable Web User Accounts After

This value specifies the maximum number of invalid login attempts before a Web User account is disabled. The number of invalid attempts is reset after a successful login or when the Web User account is re-enabled. A value of 0 indicates this setting is disabled and a Web User will have unlimited login attempts. This setting does not apply to the anonymous Web User account.

Disable Inactive Web User Accounts After

A Web User account is disabled after the specified number of inactive days. Inactive days are calculated from the last login date or the last date the account was modified. A value of 0 indicates the Web User should not be disabled based on inactivity. This setting can be overridden at the Web User level.

Password Policy

The Password Policy is used for Web Users that authenticate against the Managed File Transfer database. This page allows you to specify the password strength, minimum and maximum password ages, and the ability to reuse older passwords.

Password Strength

Enforce Settings

Select the checkbox if the Web User passwords must adhere to the Password Strength settings.

Minimum Password Length

The minimum number of characters required for a password.

Minimum Number of Upper Case Letters

The minimum number of upper case (capital) letters that each password must contain.

Minimum Number of Lower Case Letters

The minimum number of lower case letters that each password must contain. If you do not want Web Users to use all upper case letters, change this value to a number greater than zero (0).

Minimum Number of Digits

The minimum number of numerical characters that each password must contain.

Minimum Number of Special Characters

The minimum number of special characters that each password must contain.

Allowable Special Characters

The Managed File Transfer default special characters are all the non-alphanumeric characters on a standard US-101 keyboard. You can add more special characters if you are in a location using more characters (for example, Japanese or Arabic characters).

Password Age

If a Web User's password expires and they attempt to login using the HTTPS File Transfer Portal, they will be immediately prompted to change it.

Minimum Password Age

The number of days a password must be used before it can be changed. A value of zero (0) indicates there is no password age and it can be changed at any time.

Maximum Password Age

The number of days before the password expires and must be changed. A value of zero (0) indicates the password never expires.

Password Expiration Email Notification

The number of days before a password expires that a Web User is sent a password expiration notice using an "Web User Email Templates" on page 812. A value of zero (0) indicates an email is not sent. Click the Add Another Notification link to add additional expiration reminders. For example, a Web User could be sent a reminder 10 days before, 5 days before and 3 days before.

Password History

Enforce Password History

Select this checkbox to indicate that passwords cannot be reused for a specified number of times.

Disallow Reuse of the Last

When specified, a Web User must use this number of different passwords before they can reuse an old password. The reuse value is any number between 1 and 25.

User Name Policy

Enforce Settings

Select the checkbox if the user name for a Web User must adhere to the User Name Policy.

Minimum User Name Length

The minimum number of characters required for a user name. By default, the minimum length is one (1).

Maximum User Name Length

The maximum number of characters that a user name can contain. The Managed File Transfer default and maximum length is sixty-four (64) characters.

Prohibited Special Characters

The characters that cannot be used in a user name. This is especially important if you create folders based on User names.

Profile

The Profile tab allows you to indicate which Web User fields are required when creating or editing a Web User. You can also indicate which fields can be changed by Web Users when they perform a Self-Registration or when they update their profile from within the File Transfer Portal.

Required

Indicates if the field should be required from all places that allow this field to be configured. Required fields are always allowed during Self-Registration and on the Update Profile page in the File Transfer Portal. By default, all profile fields are optional.

Allow on Update Profile

Allows the Web User to edit this field on the Update Profile page in the File Transfer Portal. If this field is not enabled, the option will not appear.

Allow on Self-Registration

When enabled, this field will be presented to a Web User during self-registration.

Unique Email Address

If enabled, Web User email addresses must be unique.

Anonymous

Like a Web User, anonymous logins allow access to the set of folders, permissions and services configured for the anonymous Web User. If enabled, an anonymous Web User can login with the Web User name "anonymous" and the password is validated based on the Password Validation setting. The home directory for anonymous users is [installdirectory]/userdata/webdocs/anonymous (the location of the WebDocs directory is defined on the Services tab in "Global Settings" on page 752). The default setting is disabled.

Allow Anonymous Web User

If enabled, an anonymous Web User account will be shown on the Web User management page. Users with the Web User Manager role can configure this special account with many of the same options as a regular Web User. The anonymous Web User account is typically used for FTP and FTPS protocols, but it can be configured to allow access to HTTPS, SFTP and AS2. The anonymous account is not allowed to be promoted, exported or deleted.

Password Validation

The password for the anonymous Web User account can be configured to validate in one of the following ways:

No Validation

Regardless of what is entered for the password, it is not validated.

Valid Email Address

The password is validated to ensure that it follows a [name]@[domain].[extension] syntax (for example, jsmith@example.com).

Regular Expression

The Regular Expression option allows you to customize how the password is validated. Selecting this option requires that you specify a Password Regular Expression. For example, a value of .+@example.com would require a user to specify a password that ends with @example.com.

Show Password in Audit Log Remarks

The password value used by the anonymous Web User will be saved in the audit log when this option is enabled.

Folders

Consolidate Subfolders

Permissions for folders and files can be specified on a Web User account and on the Web User Groups to which they belong. Conflicts can occur when an Alias specified for a folder or file matches another Alias at the same level. For example, when a subfolder called 'inbound' is defined on the Web User and on the Web

User Group of which it is a member. When the Consolidate Subfolders option is enabled, the permissions for a folder or file are consolidated between all duplicate aliases found. When disabled, the permissions are taken from the first reference found, starting with the Web User account first followed by Web User Groups in sequential order.

Disk quotas are also governed by the Consolidate Subfolders option. In much the same way, when subfolders are consolidated, the highest disk quota is used. If subfolders are not consolidated, the quota is taken from the first reference found, starting with the Web User account and followed by Web User Groups in sequential order.

It is generally recommended to enable this setting unless overriding permissions is required. Regardless of whether this setting is enabled, the permissions specified on the Home Directory between Web Users and Web User Groups are always consolidated.

Web User Self-Registration

Web User Self-Registration allows your employees and trading partners to create an account in Managed File Transfer through the File Transfer Portal interface. When allowed, a "Create Account" link is displayed on the File Transfer Portal "Quick Start for HTTPS" on page 517. The self-registration process is based on "Web User Template Management" on page 623 and is based on the requester's email address or email domain.

When a user initiates self-registration, they complete a three step process to verify and register an account. The first step requires the user to enter their email and a Captcha code. If their email passes the Email Patterns filter, they are sent a unique 36-character UUID verification code, which can be pasted in the Verification Code box. The third step gathers login credentials and contact information for the new Web User account. If the Email pattern for a new user requires approval, users with the Web User Manager role are notified of the pending registration request.

Quick Start for Web-User Self-Registration

1. Specify the User Name Policy on the "Web User Settings" on page 641 page. Any new Web User names must meet this criteria. The Prohibited Special Characters are important as the Web User name is used to create a folder on the server for that account. Some special characters are not permitted in the folder names on most platforms.
2. Configure the "Login Methods Management" on page 647 that each email filter group will use. The Login Methods are subsequently used when configuring the Web User Template. If Web Users will authenticate with the Managed File Transfer Login Method, their password must conform to the "Web User Settings" on page 641. If LDAP, Azure Active Directory, Windows Active Directory, or IBM i options are used, Web Users will be prompted for their existing credentials.
3. Create a "Web User Template Management" on page 623 for each type of Web User who might self-register. The Web User Template will define the access and services permitted for each new Web User.
4. Define the Web User Self-Registration filters below. To access the Web User Self-Registration page, log in as an Admin User with the Security Officer role. From the main menu bar, select **Users**, and then click the Web User Self-Registration link.

Self-Registration Allowed

Indicates if self-registration and the ability to invite other people to use Managed File Transfer is enabled. If disabled, Web Users will not be able to send invitations from the "Quick Start for HTTPS" on page 517.

Show Register Link on Login Page

When self-registration is enabled, this setting indicates if a link to register a new account should be shown on the File Transfer Portal login page. Otherwise if the link is disabled, users will be able to access the registration link with the URL `https://[hostname]:[port]/portal/Register.xhtml`.

Email Verification Grace Period

The length of time the unique verification code for self-registrations and invitations is valid. The grace period time is displayed in hours.

Reverify Email on Invitations

When enabled, invited users will be presented with an additional email verification step to confirm they have access to the email address used in the invitation. This additional verification prevents users from forwarding invitations to others.

Email Patterns

The list of email domains either allowed or denied for self-registration. Additional email domains can be added by clicking the Add Email Pattern link. When clicked, a new pattern is added to the table.

Actions

The following actions are available for each Email pattern:

- Click the  icon to delete the Email pattern.
- Click the  icon to move the Email pattern up in the list.
- Click the  icon to move the Email pattern down in the list

  Note: Items higher in the list will be matched first even if a filter lower in the list explicitly allows or denies an email address. For example, if email patterns were set for '*support.informatica.com' and '*informatica.com', the email account 'user@informatica.com' would fail the first filter, but match the second.

Email Pattern

The email address or email domain that will be filtered. The email field supports the use of wildcards. For example, use the pattern of *@example.com to include anyone with a domain name of example.com.

Permission

Each email filter can have one of the following permissions:

- **Allowed**

  The Web User registration is allowed if their email address matches the pattern.

- **Denied**

  The Web User registration is denied if their email address matches the pattern.

- **Invite Only**

  The Web User registration is allowed only if they were specifically invited by another Web User and their email address matches the pattern.

Web User Template

The Web User Template to use when creating the Web User account. All permissions and settings defined in the selected Web User Template will be applied to the new Web User.

Requires Approval

If required, the new Web User will be placed into a Pending Approval status. An Admin User with the Web User Manager role can approve accounts by clicking the Approve icon in the More Actions drop-down list on the "Web User Management" on page 589 page.

Notify Web User Manager

Admin Users with the Web User Manager role (that are enabled and contain a valid email address), can be notified by email each time a self-registered account is created. Select the checkbox if notification should be sent.

Login Methods

The default Native login method allows Admin User and Web User passwords to be authenticated against the passwords stored in the Managed File Transfer database. Optionally, you can configure Managed File Transfer Login Methods for basic authentication of Admin User and Web User passwords against a **Azure Active Directory**, **Windows Active Directory**, or a **Generic LDAP** located within your organization. Web User accounts can also be synchronized with users stored in an LDAP server.

The Login Method page provides options to create Login Methods, select default Login Methods for User or Web User accounts and edit available Login Methods.

Login Methods Management

To manage Login Methods, log in as an Admin User with the **Security Officer** role.

From the main menu bar, select **Users**, and then click the Login Methods link.

Page Toolbar

The following actions are available from the page toolbar:

- "Select Login Method Type" on page 649 a Login Method by clicking the **Add Login Method** link in the toolbar.
  - Click the **Edit** button to select the Default Login Method for Managed File Transfer Admin Users or Web Users. The available options in the drop-down lists are based on the created Login Methods. The default Login Method is Managed File Transfer. When finished making a selection, click the **Save** button.

Login Methods Actions

The following actions are available by selecting the Actions icon:

- Configure a "Edit Login Method" on page 655 or "Add LDAP Server" on page 651 login method by clicking the icon.
- View "Login Method Details" on page 657 or "LDAP Login Method Details" on page 657 details by clicking the icon.
- Delete a Login Method by clicking the icon. Login methods referenced by Admin Users, Web Users, Web User Groups, Web User Templates or specified as a default setting cannot be deleted.
- "Test Login Method" on page 657 a Login Method by clicking the Test link.
  - Synchronize a LDAP Managed server by clicking the Synchronize Now icon. Synchronizing will add, update, or disable Web users based on the configuration of the login method. Managed File Transfer will display a list of status messages when the synchronize process is completed:
  - Web Users added - Displays the number of Web Users imported into Managed File Transfer .
  - Web Users updated - Displays the number of Web Users with LDAP profile or group changes.
  - Web User disabled - Displays the number of Web Users that were disabled due to the removal of their account from an enforced Web User Group.
  - Web Users bypassed - Displays the number of user accounts in the LDAP server that do not belong to an enforced Web User Group.
  - Web User conflicts - Displays the number of Web Users in Managed File Transfer that are not managed by this Login Method. For example, a Web User with the user name of 'Kharris' would be in conflict if it is managed by Managed File Transfer and exists in the LDAP server.
  - Web Users synched - Displays the total number of Web Users who were synchronized.

    Note: In a disaster recovery scenario, verify the Login Methods are updated to point to the disaster recovery server or instance. User authentication will fail if the Login Method is not referencing the proper location.
  - Admin users that are authenticated by using the Informatica domain authentication can synchronise to the ISP server by clicking the **Synchronize Now** icon. Synchronizing will add, update, or disable Admin users based on the configuration of the login method. Managed File Transfer will display a list of status messages when the synchronize process is completed:
  - Amin Users added - Displays the number of Admin Users imported into Managed File Transfer .
  - Admin Users updated - Displays the number of Admin Users with ISP profile or group changes.
  - Admin Users bypassed - Displays the number of user accounts in the ISP server that do not belong to an enforced Web User Group.

- Admin User conflicts - Displays the number of Admin Users in Managed File Transfer that are not managed by this Login Method. For example, a Admin User with the user name of 'Kharris' would be in conflict if it is managed by Managed File Transfer and exists in the ISP server.
- Admin Users synched - Displays the total number of Admin Users who were synchronized.

  Note: In a disaster recovery scenario, verify the Login Methods are updated to point to the disaster recovery server or instance. User authentication will fail if the Login Method is not referencing the proper location.

Select Login Method Type

When adding a Login Method, you will be prompted to select the type of authentication to use.

Basic Authentication

Select the Basic Authentication option to "Add Login Method" on page 649 that can be used to authenticate Managed File Transfer users against an Azure Active Directory, Microsoft Active Directory (AD), Generic LDAP, Informatica Domain Authentication or Okta Multi Factor Authentication at the time of login.

LDAP Managed

LDAP Managed Login Methods allow you to perform basic authentication for Admin Users and Web Users. Web Users can also be created automatically during login and synchronized based on the configuration.

This login method type supports Active Directory®, Active Directory Lightweight Directory Services (AD LDS), IBM Tivoli®, Oracle® Directory Service (ODS), Apache™ DS, Azure Active Directory, and Generic LDAP servers.

Select the LDAP Managed option to "Add LDAP Server" on page 651 login method. You will be prompted to select an LDAP server type.

LDAP Server Type

Managed File Transfer will populate the Add LDAP Server page using the recommended settings for the selected server type.

Add Login Method

Follow the instructions below to add a new Login Method:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Login Methods link.
3. In the "Login Methods Management" on page 647 page, click the ✚ Add Login Method link in the page toolbar.
4. Select **Basic Authentication** from the "Select Login Method Type" on page 649 page and then click **Continue**.
5. Complete the required information.
6. Click the **Save** button to save the settings.

Name

A unique name for the Login Method.

Description

The description field is optional text to describe the login method. Limited to 512 characters.

Type

The authentication type used by the Login Method. Based on the selection, additional Login Method information is requested in the Options section based on the Login Method Type selection.

Microsoft Active Directory

Active Directory (LDAP) UR

The URL should be in the format [protocol]://[hostname]:[port]. For example, ldap://mydomainhostname:389 or ldaps://10.1.4.1:636. The default port for the Active Directory Server is 389. The default port for a secure LDAPS connection is 636.

Domain Name

The Domain Name where the accounts authenticate. For example, MYDOMAIN.

Generic LDAP

LDAP URL

The URL should be in the format [protocol]://[hostname]:[port]. For example, ldap://mydomainhostname:389 or ldaps://10.1.4.1:636. The default port for a LDAP Server is 389. The default port for a secure LDAPS connection using SSL is 636.

DN Pattern

The DN Pattern used to identify a user in the Generic LDAP database. The variable ${user} must be included in the DN pattern and will be replaced with the username during login. For example, cn=${user},ou=users,dc=example,dc=com

Azure Active Directory

Azure Active Directory URL

The URL should be in the format [protocol]://[hostname]:[port].

Okta Multi Factor Authentication

Okta Domain URL

The URL assigned to the organization. The URL should be in <http or https>:// <url> format.

Edit Default Login Method

You can change the default login method for Web and Admin users.

1. Select **Users** > **Login Methods**.

   The Login Methods page displays.

2. Click Edit.

   Default Login Methods for Admin Users and **Default Login Methods for Web Users** fields are enabled.

3. Login Methods are listed in the drop-down list of Login methods for Web and Admin Users. Change the login method for Web and Admin Users in the corresponding drop-down list.
   - Change the login method for Web users in the **Default Login Methods for Admin Users** drop-down list.
   - Change the login method for Admin users in the **Default Login Methods for Admin Users** drop-down list.

4. Click **Save**.

Add LDAP Server

Follow the instructions below to add a new LDAP Server Login Method:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Login Methods link.
3. In the "Login Methods Management" on page 647 page, click the Add Login Method link in the page toolbar.
4. In the "Select Login Method Type" on page 649 page, select **LDAP Managed.** Choose your server type and then click **Continue**.
5. Complete the required information.
6. Click the **Save** button to save the settings.

Server

The Server tab contains the fields used to establish a connection to the LDAP server.

Name

A unique name for the LDAP Login Method.

Description

The description field is optional text to describe the Login Method. Limited to 512 characters.

Primary Host

The host name or IP address of the LDAP server.

Alternate Host

The host name or IP address of the LDAP server to use when the primary host is unavailable.

Port

The port number for the LDAP server.

Use SSL

Enable this option to use SSL for secure transmission with the LDAP server.

Implicit SSL

When enabled, Managed File Transfer will trust any certificate from the LDAP server. When not enabled, the certificate will be validated using the Default Trusted Certificates "Open SSL Key Store" on page 731.

User

An LDAP trusted user ID for performing searches within the LDAP server.

Password

The password for the trusted user ID.

Base DN

The Base DN within the LDAP server restricts where Managed File Transfer will find users and groups.

Object Class Attribute

The name of the attribute that holds the class value for a LDAP entry.

Distinguished Name Attribute

The name of the attribute that stores the unique identifier for a LDAP entry.

Web Users

The Web Users tab controls how users in the LDAP server are integrated with the Web Users in Managed File Transfer.

Synchronization

- Synchronization EnabledWhen enabled, Managed File Transfer will scan the LDAP server during timed intervals looking for new or modified users and create or update Web Users in Managed File Transfer. When Web User group membership is enforced, only users that have a matching LDAP and Managed File Transfer Web User Group will by synchronized.

Web User Authentication

- Create Web User Automatically During LoginIf the Web User account does not exist in Managed File Transfer when the user first logs in, an account will be created in Managed File Transfer as long as their LDAP user ID and password is valid.
- Update Web User InfoWhen the Web User logs in, Managed File Transfer can update their account information with the latest attributes from the LDAP server.

Web User Groups

- Enforce Web User Group MembershipWhen enabled, Web Users can login only if they belong to a "Select Web User Group Type" on page 615 that is associated with this LDAP Login Method.

Web User Template

- Use Default Web User TemplateWhen enabled, any Web User that is created during login or synchronization will use the default template. When unchecked, you can select which Web User Template to use when creating the Web User.

Advanced

The Advanced tab allows you to set log levels and server timeout settings.

Log Level

The "Server Log Viewer" on page 671 will record information and error messages that pertain to LDAP activity during synchronization or login. The default setting, Summary, writes synchronization status information to the log. If Detail is selected, synchronization results will be recorded for every user that was processed. Detail logging should only be used for troubleshooting an issue since it can impact performance and increase the size of the log file.

Connection Timeout

The maximum number of seconds to wait when establishing a connection with the LDAP server. The default is 60 seconds.

Read Timeout

The maximum amount of time, in seconds, to wait for a read response from the LDAP server.

Search Timeout

The maximum amount of time, in seconds, to wait for a response from a search request to the LDAP server. A timeout value of 0 (zero) indicates an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

User

The User tab allows you to configure the LDAP schema settings for finding users. Managed File Transfer populates these fields using default attributes based on the type of LDAP server selected.

Object Class

The object class name for a user.

Object Filter

The filter that is used when searching for users.

Example: The following object filter will ignore disabled accounts in Active Directory:

(&(objectClass=User)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

User Name Attribute

The attribute for a user name.

First Name Attribute

The attribute for a user's first name.

Last Name Attribute

The attribute for a user's last name.

Email Attribute

The attribute for the user's email address.

Phone Attribute

The attribute for the user's telephone number.

Membership Attribute

The attribute that determines membership on the user object.

Group

The Group tab allows you to configure LDAP settings for finding groups. Managed File Transfer populates these fields using default attributes based on the type of LDAP server selected.

Object Class

The object class name for a group.

Object Filter

The filter used when searching for groups.

Name Attribute

The attribute for the group name.

Membership Attribute

The attribute name that determines membership of the group object.

Membership

The Membership tab allows you to configure LDAP schema settings for determining membership of groups.

Membership Source

Determines if the Membership Attribute on the User or Group tab will define membership.

Include Nested Groups

When a Group's members includes users and groups (nested Groups), Managed File Transfer will include the users who belong to the nested group. When this setting is not enabled, users that belong to the nested groups will not be included.

For example:

The Software Development group membership contains individual users (software developers) as well as the QA group. When Include Nested Groups is enabled, the users that belong to the QA group will also be included. If Include Nested Groups is not enabled, users that belong to the QA group will not be included.

Edit Login Method

Follow the instructions below to edit a Login Method:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Login Methods link.

3. In the "Login Methods Management" on page 647 page, click the  Action icon next to the Login Method, and then click  **Edit** icon.
4. Modify the field values for the Login Method.
5. Click the **Save** button to save the settings.

Name

A unique name for the Login Method.

Description

Use this text-box for any extra information pertaining to the Login Method. This field is limited to 512 characters.

Type

The authentication type used by the Login Method. Based on the selection, additional Login Method information is requested in the Options section based on the Login Method Type selection.

Microsoft Active Directory

Active Directory (LDAP) URL

The URL should be in the format [protocol]://[hostname]:[port]. For example, ldap://mydomainhostname:389 or ldaps://10.1.4.1:636. The default port for the Active Directory Server is 389. The default port for a secure LDAPS connection is 636.

Domain Name

The Domain Name where the accounts authenticate. For example, MYDOMAIN.

Generic LDAP

LDAP URL

The URL should be in the format [protocol]://[hostname]:[port]. For example, ldap://mydomainhostname:389 or ldaps://10.1.4.1:636. The default port for a LDAP Server is 389. The default port for a secure LDAPS connection using SSL is 636.

DN Pattern

The DN Pattern used to identify a user in the Generic LDAP database. The variable ${user} must be included in the DN pattern and will be replaced with the username during login. For example, cn=${user},ou=users,dc=example,dc=com

Azure Active Directory

Azure Active Directory URL

The URL should be in the format [protocol]://[hostname]:[port].

Okta Multi Factor Authentication

Okta Domain URL

The URL assigned to the organization. The URL should be in <http or https>:// <url> format.

Test Login Method

The Test Login Method page allows you to test user authentication against the Login Method.

User

The user ID of the user.

Password

The password for the user.

Login Method Details

The Login Method Details page shows the properties for the Login Method, when the Login Method was created and when it was last modified. The page also shows the Settings, Admin Users, Web Users, and the Web User Templates using this Login Method. Follow the instructions below to view Login Method Details:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Login Methods link.
3. In the "Login Methods Management" on page 647 page, click the  Action icon next to the Login Method, and then click the  View icon.

LDAP Login Method Details

The LDAP Login Method Details page shows the properties for the LDAP Login Method, when the LDAP Login Method was created and when it was last modified. The page also shows the Settings, Admin Users, Web

Users, Web User Groups, and the Web User Templates using this login method. Follow the instructions below to view Login Method Details:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu bar, select **Users**, and then click the Login Methods link.
3. In the "Login Methods Management" on page 647 page, click the  Action icon next to the Login Method, and then click the  View icon.

CHAPTER 8

Logs and Reports

Logs, reports, and log settings are available to authorized Admin Users from the Logs drop-down menu.

Logs are useful for troubleshooting errors and monitoring events such as file transfers and server activity. The logs can be sorted by column, as well as exported to a CSV formatted file.

The Audit Log Rules page can be used to turn off logging for specific event types.

The log file locations and parameters for all logs maintained by Managed File Transfer are defined in the log settings.

Reports

The Reports feature in Managed File Transfer allows you to quickly create interactive PDF reports that contain system, Project, and Web User activity. "Reports" on page 462 allow you to create scheduled reports using "Project Design" on page 100.

To run a report interactively, you must log in as an Admin User with the appropriate "Admin Roles" on page 583 for that report.

From the main menu bar, point to Logs and then click **Reports**.

Select a report from the list, specify optional parameters, and then click the **Run Report** button. The report is downloaded to your browser's default download directory.

The following image is an example of an Expiring SSL Certificates report:

The following reports are available:

Blacklisted IP Addresses

The Blacklisted IP Addresses report displays a list of blocked IP addresses and the date they were created.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Limit Number of Rows

Limits the number of rows included in the report.

Completed Jobs

The Completed Job report displays a list of completed Jobs, their status, and the Admin User who ran the job.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Status

Filters the Jobs included in the reports based on the status of the Job. The Status will appear as an icon on the report:

✓ Success

✗ Fail

– Canceled

Completed Jobs Statistics

The Completed Jobs Statistics report displays the total number of Jobs processed during the specified date range.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Group By

The hour, day, or month value the report will be grouped by.

Database Statistics

The Database Statistics report displays a list of each database table used by the Managed File Transfer system as well as the number of rows used by each table.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Expiring OpenPGP Keys

The Expiring OpenPGP Keys report displays a list of OpenPGP Keys that will be expiring within the specified date range.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Expiring SSL Certificates

The Expiring SSL Certificates report displays a list of SSL Certificates that will be expiring within the specified date range.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Global Activity Details

The Global Activity Details report displays all activity for the selected features based on the search term provided.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Modules

The modules that will be included in the report. The report results are filtered by the modules the Admin User who is running the report has access to, based on the Admin User's “Admin Roles” on page 583.

Search Term

Specify items to search for. The Global Activity report search field uses the following wildcard searches:

- Multiple character wildcard searching using "*"
- A single character wildcard search for terms that match a single character replaced using "?". For example, to search for "text" or "test" you can use "te?t".
  Fuzzy searches using a tilde "~". A Fuzzy search finds words that are similar to the search term. For example, the search term "Proj~" will return results that contain the word "Project."
- Multiple terms can be combined together with Boolean operators to form a more complex query. for example:
- Searching for Project could result in 3400 hits (items contain the word Project)
- Searching for Deny could result in 100 hits (items contain the word Deny)

- Searching for Project and Deny results in 17 hits (results contain both words Project and Deny)
- Searching for "Project Deny" (with quotes) results in 0 hits (There are no items that contain the words Project and Deny directly after each other)

User

The Admin User or Web User that generated the log entries.

Limit Number of Rows

Limits the number of rows included in the report.

Shared Drive Disk Usage

The Shared Drive Disk Usage report displays the Web Users who are permitted to use the Shared Drive feature, and their total amount of disk usage.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Limit Number of Rows

Limits the number of rows included in the report.

Job Count Summary

The Job Count Summary report displays a pie chart representation of the number of Jobs processed during the specified date range.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Secure Mail Activity

The Secure Mail Activity report displays a list of Secure Mail messages and the Web User(s) who created them, the recipient(s) of the message, the status, and the date the message was last modified.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Limit Number of Rows

Limits the number of rows included in the report.

Status

Filters the results of the report based on the status of the Package.

Secure Mail Disk Usage

The Secure Mail Disk Usage report displays the Secure Mail disk usage for each Web User sorted by size.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Limit Number of Rows

Limits the number of rows included in the report.

Secure Mail Package Sizes

The Secure Mail Package Sizes report displays a list of Secure Mail Packages, their subject (from the Secure Mail Message) and their size.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Limit Number of Rows

Limits the number of rows included in the report.

Security Settings Audit

The Security Settings Audit report will analyze your Managed File Transfer product's security settings and determine if they comply with the Payment Card Industry Data Security Standards (PCI-DSS). For each security setting, the report will indicate if the setting meets the PCI-DSS standard using one of the following statuses:

Pass

The setting meets the PCI-DSS requirement.

Fail

The setting does not meet the PCI-DSS requirement. Recommend steps to correct the setting are provided.

Warning

Further research is required to ensure your system meets the specified requirement. Recommend steps to correct the setting are provided.

Not Applicable

A check on this setting is not required, typically due to Managed File Transfer features that you are not licensed to use.

Fatal

Indicates a configuration problem is preventing Managed File Transfer from accessing the appropriate data.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Service Activity by Module

The Service Activity by Module report displays the number of files and bytes transferred by the selected file transfer modules.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Modules

The file transfer modules that will be included in the report.

Transfer Type

Filters the results of the report based on the type of file transfer, either upload or download.

Limit Number of Rows

Limits the number of rows included in the report.

Service Activity Summary

The Service Activity Summary report displays the number of uploads and downloads for the selected protocols.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Protocol

The protocol(s) that will be included in the report.

Service Errors

The Service Errors report displays all errors for the selected inbound services within the specified date range.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Modules

The file transfer modules that will be included in the report.

Status

Filters the results of the report based on the status of the error, either Warning or Failed.

Limit Number of Rows

Limits the number of rows included in the report.

Trigger Activity

The Trigger Activity report displays a list of executed Triggers, their status, and their associated event types.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Limit Number of Rows

Limits the number of rows included in the report.

Status

Filters the results of the reports based on the status of the executed Trigger. The Status will appear as an icon on the report:

Active

Success

Fail

Web User Logins

The Web User Logins report displays a list of each Web User login, the service they logged in to, and the status of the login attempt.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Protocols

The protocol(s) that will be included in the report.

Status

Filters the results of the reports based on the status of the Web User login. The Status will appear as an icon on the report:

Success

Warning

Fail

Web User Transfer Count Activity

The Web User Transfer Count Activity report displays the number of file transfers per Web User.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Modules

The module(s) to include in the report.

Limit Number of Rows

Limits the number of rows included in the report.

Transfer Type

The transfer type(s) that will be included in the report.

Web User Transfer Size Activity

The Web User Transfer Activity report displays the total size of transferred files by Web User.

Listed below are the settings that can be specified for the report:

Report Title

The title of the report that will appear on the report header.

Orientation

The report page layout, either portrait or landscape.

Date Range

The Date Range allows you to specify the scope of the data to include in the report based on date and time.

Modules

The module(s) to include in the report.

Limit Number of Rows

Limits the number of rows included in the report.

Transfer Type

The transfer type(s) that will be included in the report.

Audit Logs

The Audit Logs page allows admin users to view and search logs for each service the admin user has permission to access.

From the main menu bar, point to Logs and then click **Log Settings**.

To view a log, select it from the left pane to view it in the right pane.

Global Search

The Global Search page searches for audit entries across all selected modules and services. The date range available is dependent on how long the entries are retained in the database, which is configured in the "Log Settings" on page 693.

The Global Search results are filtered by the modules the Admin User has access to, based on the Admin User's "Admin Roles" on page 583.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **Search** from the Global Logs section from the left pane. The Global Log will appear in the right pane.

Filter Criteria

The Global Log can be filtered using the following criteria:

Modules

The services and features to include in the search.

Search Term

Enter one or more words in the field provided. The search string can contain a whole word, a partial word, or a phrase with uppercase and lowercase characters. The Global Search uses the following wildcard searches:

- Multiple character wildcard searching using "*"

- A single character wildcard search for terms that match a single character replaced using "?". For example, to search for "text" or "test" you can use "te?t".
  Fuzzy searches using a tilde "~". A Fuzzy search finds words that are similar to the search term. For example, the search term "Proj~" will return results that contain the word "Project."
- Multiple terms can be combined together with Boolean operators to form a more complex query. for example:
- Searching for Project could result in 3400 hits (items contain the word Project)
- Searching for Deny could result in 100 hits (items contain the word Deny)
- Searching for Project and Deny results in 17 hits (results contain both words Project and Deny)
- Searching for "Project Deny" (with quotes) results in 0 hits (There are no items that contain the words Project and Deny directly after each other)

User

The Admin User or Web User that generated the log entries.

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

Rows

The number of rows to display on the page at a time.

Results

The results will show the audit entries that meet the filter criteria. Click on an audit entry to drill down into more details for that item. Click on the by (user) link to view more information about the user that generated the audit entry

View User Information

Manage User

Opens the “Admin User Management” on page 576 or “Web User Management” on page 589 management page.

Server Log Viewer

The Server Log Viewer is available to Admin Users with the Product Administrator or Auditor role and is located on the Logs drop-down menu. The Log File drop-down list on the Server Log Viewer page displays any files with a .log extension that are located in the default logs directory. The default logs directory is defined on the Global Log tab of the “Log Settings” on page 693. The Log File drop-down list can also contain archived log files stored in the default log file location. If this Managed File Transfer server is a member of cluster, the log file for the specific system is named informaticamft.log.

Download Server Log

Click the **Download Server Log** button to download the complete Server Log to your computer. By default, the file is a plain text file with a .log extension.

Refresh

Click the **Refresh** button to refresh the Server Log, which will load any new entries to the log.

Shared Drive Log

The Shared Drive Log page allows you to query, view and export audit entries for Shared Drive. Entries can be filtered using a wide variety of search criteria.

To view the Shared Drive Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **Shared Drive** from the Service Logs section from the left pane. The Shared Drive Log will appear in the right pane.

Basic Search

Use the following fields to perform a basic search:

Search Field

Enter a search term in the field provided. The Shared Drive Log uses the following wildcard searches:

- Multiple character wildcard searching using "*"
- A single character wildcard search for terms that match a single character replaced using "?". For example, to search for "text" or "test" you can use "te?t".
- Multiple terms can be combined together with Boolean operators to form a more complex query. for example:
- Searching for File could result in 800 hits (items contain the word File)
- Searching for Trashed could result in 15 hits (items contain the word Trash)
- Searching for File AND Trash results in 14 hits (results contain both words File and Trashed)
- Searching for "File Trashed" (with quotes) results in 14 hits (For items that contain the words File and Trashed directly after each other)

Time

Select a time frame to limit the scope of your search. Default value is 'Today'.

Rows

Specify the number of rows to display on the page at a time.

Advanced Search

The Advanced Search provides additional search options for the Shared Drive Log. Use the following fields to perform an advanced search:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The Web User that generated the log entries.

Status

Select Successful or Failed events.

Event Type

An Event Type is assigned to each transaction by Managed File Transfer . This Event Type is passed along in reports and allows for easy reference.

Event ID

An Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

Session ID

The Session ID of the session that initiated the commands.

File Name

Returns transactions that contain the specified File Name.

System Name

The name of the system that processed the transaction. This is commonly used in a clustered environment.

Shared Drive Columns

- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- Start Time - The time the event started. This field is formatted according to the timestamp pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the event finished. This field is formatted according to the timestamp pattern defined in the Global Settings for Managed File Transfer.
- Event Type - The action completed by the Web User.
- Status - Displays the outcome of the transaction, either success or failure.
- System Name - The name of the Managed File Transfer server that processed the event. This name is configured in the [installdirectory]/config/cluster.xml file (where [installdirectory] is the installation directory of Managed File Transfer)
- File Name - The file name associated to the transaction.
- Folder Name - The file name associated to the transaction.
- Moved From - The name of source folder when an item is moved.
- Moved To- The name of the destination folder when an item is moved.
- Renamed To - The new name of an item that was renamed.
- File Size - The size of the file, in bytes.
- Last Modified - The date the item was last modified.

- Session ID - A unique identifier created per Web User connection. All transactions made through this connection are referenced by the same Session ID number.
- Device ID - The ID of the device associated to the session.
- User - The account name of the Web User performing the actions.
- Local IP - The IP address that received the request.
- Local Port - The port that received the request.
- Remote IP - The IP address of the Web User's system that sent the request.
- Remote Port - The port on the Web User's system that sent the request.
- Comment - The Web User comment added, modified, or removed from the item.
- Target Email - The Web User the item was shared with.
- Target User - The target Web User for the transaction.
- Error - Displays the cause of a failed transaction.
- Device Status - Displays the status of the device that attempted the transaction.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

HTTPS Log

The HTTPS Log page allows you to query, view and export audit entries for the HTTPS service. Entries can be filtered using a wide variety of search criteria. The date range available is dependent on how long entries are retained in the database, which is configured in the "Log Settings" on page 693.

To view the HTTPS Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **HTTPS** from the Service Logs section from the left pane. The HTTPS Log will appear in the right pane.

Basic Search

Use the following fields to perform a basic search:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The Web User that generated the log entries. Click the User link to see more details about the Web User.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

Rows Per Page

The number of rows to display on the page at a time.

Advanced Search

The Advanced Search provides additional search options including the Basic Search options for the HTTPS Log. Use the following fields to perform an advanced search:

Event ID

An Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Command

Audit Log search results will be filtered by the selected commands. Click the Select Commands link to select the commands.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

Session ID

The Session ID of the session that initiated the commands.

Physical Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of the Physical Path. The physical path is the absolute or full path location of the file or folder on the file system.

Virtual Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of a Virtual Path. The virtual path is the relative path of the file or folder as it appears to Web Users.

Package ID

Secure mail messages are assigned a unique Package ID when they are created. You can search the HTTPS log can be searched with a Package ID.

Recipient Email

The recipient's email address for events related to Secure Mail (recipient notified via email, recipient read message, recipient downloaded an attachment, etc.).

System Name

The name of the system that processed the transaction. This is commonly used in a clustered environment.

Audit Log Detail Links

- Click the **Find** icon to view Audit Log Details for any entry.
- Click the **Triggers** icon to view Triggers that were started from this event via the Trigger Log page.
- Click the **Web Users** icon to view information about the Web User that performed the action. Click the **Manage User** button in the resulting pop-up to open the Web Users page for that Web User account.

Action Buttons

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.

- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages that meet the filter criteria to a .CSV file on your local computer.

HTTPS Columns

- Package ID - The identification number given to a secure mail package.
- Recipient Email - The email address of the person to whom the secure mail package was sent.
- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- System Name - The name of the Managed File Transfer server that processed the event. This name is configured in the [installdirectory]/config/cluster.xml file (where [installdirectory] is the installation directory of Managed File Transfer)
- Start Time - The time the event started. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the event finished. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- Time (ms) - The duration or total time of the event. This value is displayed in milliseconds.
- Command - The action requested by the User.
- Event Type - The system generated event based on the Command and Status. These event types are referenced by Triggers and Audit Log Rules.
- Status - The status of the transaction.
- Local IP - The IP address that received the request.
- Local Port - The port that received the request.
- Remote IP - The IP address of the Web User's system that sent the request.
- Remote Port - The port on the Web User's system that sent the request.
- Session ID - A unique identifier created per Web User connection. All transactions made through this connection are referenced by the same Session ID number.
- User - The account name of the Web User performing the actions.
- Physical Path - The absolute or full path location of the file or folder on the file system.
- Virtual Path - The relative path of the file or folder as it appears to Web Users.
- File Size - The size of the file, in bytes.
- Remarks - Additional information about the transaction.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

FTP Log

The FTP Log page allows you to query, view and export audit entries for the FTP service. Entries can be filtered using a wide variety of search criteria. The date range available is dependent on how long entries are retained in the database, which is configured in the "Log Settings" on page 693.

To view the FTP Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **FTP** from the Service Logs section in the left pane. The FTP Log will appear in the right pane.

Basic Search

Use the following fields to perform a basic search:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The Web User that generated the log entries. Click the User link to see more details about the Web User.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

Rows Per Page

The number of rows to display on the page at a time.

Advanced Search

The Advanced Search provides additional search options including the Basic Search options for the FTP Log.

Event ID

An Event ID is assigned to each transaction by Managed File Transfer.

Command

Audit Log search results will be filtered by the selected commands.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

Session ID

The Session ID of the session that initiated the commands.

Physical Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of the Physical Path. The physical path is the absolute or full path location of the file or folder on the file system.

Virtual Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of a Virtual Path. The virtual path is the relative path of the file or folder as it appears to Web Users.

System Name

The name of the system that processed the transaction. This is commonly used in a clustered environment.

Audit Log Detail Links

- Click the **Find** icon to view Audit Log Details for any entry.
- Click the **Triggers** icon to view Triggers that were started from this event via the Trigger Log page.
- Click the **Web Users** icon to view information about the Web User that performed the action. Click the **Manage User** button in the resulting pop-up to open the Web Users page for that Web User account.

Action Buttons

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages that meet the filter criteria to a .CSV file on your local computer.

FTP Columns

- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- System Name - The name of the Managed File Transfer server that processed the event. This name is configured in the [installdirectory]/config/cluster.xml file (where [installdirectory] is the installation directory of Managed File Transfer)
- Start Time - The time the event started. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the event finished. This field is formatted according to the Timestamp Pattner defined in the Global Settings for Managed File Transfer.
- Time (ms) - The duration or total time of the event. This value is displayed in milliseconds.
- Command - The action requested by the User.
- Event Type - The system generated event based on the Command and Status. These event types are referenced by Triggers and Audit Log Rules.
- Status - The status of the transaction.
- Local IP - The IP address that received the request.
- Local Port - The port that received the request.
- Remote IP - The IP address of the Web User's system that sent the request.
- Remote Port - The port on the Web User's system that sent the request.
- Session ID - A unique identifier created per Web User connection. All transactions made through this connection are referenced by the same Session ID number.
- User - The account name of the Web User performing the actions.
- Physical Path - The absolute or full path location of the file or folder on the file system.
- Virtual Path - The relative path of the file or folder as it appears to Web Users.
- File Size - The size of the file, in bytes.
- Remarks - Additional information about the transaction.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

FTPS Log

The FTPS Log page allows you to query, view and export audit entries for the FTPS service. Entries can be filtered using a wide variety of search criteria. The date range available is dependent on how long entries are retained in the database, which is configured in the "Log Settings" on page 693.

To view the FTPS Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **FTPS** from the Service Logs section from the left pane. The FTPS Log will appear in the right pane.

Basic Search

Use the following fields to perform a basic search:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The Web User that generated the log entries. Click the User link to see more details about the Web User.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

Rows Per Page

The number of rows to display on the page at a time.

Advanced Search

The Advanced Search provides additional search options including the Basic Search options for the FTPS Log.

Event ID

An Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Command

Audit Log search results will be filtered by the selected commands.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

Session ID

The Session ID of the session that initiated the commands.

Physical Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of the Physical Path. The physical path is the absolute or full path location of the file or folder on the file system.

Virtual Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of a Virtual Path. The virtual path is the relative path of the file or folder as it appears to Web Users.

System Name

The name of the system that processed the transaction. This is commonly used in a clustered environment.

Audit Log Detail Links

- Click the **Find** icon to view audit log details for any entry.
- Click the **Triggers** icon to view Triggers that were started from this event via the Trigger Log page.
- Click the **Web Users** icon to view information about the Web User that performed the action. Click the **Manage User** button in the resulting pop-up to open the Web Users page for that Web User account.

Action Buttons

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages that meet the filter criteria to a .CSV file on your local computer.

FTPS Columns

- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- System Name - The name of the Managed File Transfer server that processed the event. This name is configured in the [installdirectory]/config/cluster.xml file (where [installdirectory] is the installation directory of Managed File Transfer)
- Start Time - The time the event started. This field is formatted according to the timestamp pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the event finished. This field is formatted according to the timestamp pattern defined in the Global Settings for Managed File Transfer.
- Time (ms) - The duration or total time of the event. This value is displayed in milliseconds.
- Command - The action requested by the User.
- Event Type - The system generated event based on the Command and Status. These event types are referenced by triggers and audit log rules.
- Status - The status of the transaction.

- Local IP - The IP address that received the request.
- Local Port - The port that received the request.
- Remote IP - The IP address of the Web User's system that sent the request.
- Remote Port - The port on the Web User's system that sent the request.
- Session ID - A unique identifier created per Web User connection. All transactions made through this connection are referenced by the same Session ID number.
- User - The account name of the Web User performing the actions.
- Physical Path - The absolute or full path location of the file or folder on the file system.
- Virtual Path - The relative path of the file or folder as it appears to Web Users.
- File Size - The size of the file, in bytes.
- Remarks - Additional information about the transaction.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

SFTP Log

The SFTP Log page allows you to query, view and export audit entries for the SFTP service. Entries can be filtered using a wide variety of search criteria. The date range available is dependent on how long entries are retained in the database, which is configured in the "Log Settings" on page 693.

To view the SFTP Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **SFTP** from the Service Logs section from the left pane. The SFTP Log will appear in the right pane.

Basic Search

Use the following fields to perform a basic search:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The Web User that generated the log entries. Click the User link to see more details about the Web User.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

Rows Per Page

The number of rows to display on the page at a time.

Advanced Search (SFTP)

The Advanced Search provides additional search options including the Basic Search options for the SFTP Log.

Event ID

An Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Command

Select from the following commands to search for the SFTP log:

- Login
- Download
- Upload
- Mkdir
- Change Password
- Logout
- Delete
- Rename
- Chmod
- Checksum
- Connect
- Disconnect
- Key Exchange

The Audit Log search results is filtered by the selected commands.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

Session ID

The Session ID of the session that initiated the commands.

Physical Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of the Physical Path. The physical path is the absolute or full path location of the file or folder on the file system.

Virtual Path

A drop-down list provides conditions (Begins With, Ends With, Contains, or Equals) that can be used to search for a known portion of a Virtual Path. The virtual path is the relative path of the file or folder as it appears to Web Users.

System Name

The name of the system that processed the transaction. This is commonly used in a clustered environment.

Audit Log Detail Links

- Click the **Find** icon to view audit log details for any entry.
- Click the **Triggers** icon to view Triggers that were started from this event via the Trigger Log page.
- Click the **Web Users** icon to view information about the Web User that performed the action. Click the **Manage User** button in the resulting pop-up to open the Web Users page for that Web User account.

Action Buttons

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages that meet the filter criteria to a .CSV file on your local computer.

SFTP Columns

- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- System Name - The name of the Managed File Transfer server that processed the event. This name is configured in the [installdirectory]/config/cluster.xml file (where [installdirectory] is the installation directory of Managed File Transfer)
- Start Time - The time the event started. This field is formatted according to the timestamp pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the event finished. This field is formatted according to the timestamp pattern defined in the Global Settings for Managed File Transfer.
- Time (ms) - The duration or total time of the event. This value is displayed in milliseconds.
- Command - The action requested by the User.
- Event Type - The system generated event based on the Command and Status. These event types are referenced by triggers and audit log rules.
- Status - The status of the transaction.
- Local IP - The IP address that received the request.
- Local Port - The port that received the request.
- Remote IP - The IP address of the Web User's system that sent the request.
- Remote Port - The port on the Web User's system that sent the request.
- Session ID - A unique identifier created per Web User connection. All transactions made through this connection are referenced by the same Session ID number.
- User - The account name of the Web User performing the actions.
- Physical Path - The absolute or full path location of the file or folder on the file system.
- Virtual Path - The relative path of the file or folder as it appears to Web Users.
- File Size - The size of the file, in bytes.
- Remarks - Displays the SSH handshake level information. For example, details of cipher, key exchange algorithm, and so on.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

AS2 Log

The AS2 Log page allows you to query, view and export audit entries for the AS2 service. Entries can be filtered using a wide variety of search criteria. The date range available is dependent on how long entries are retained in the database, which is configured in the "Log Settings" on page 693.

To view the AS2 Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **AS2** from the Service Logs section from the left pane. The AS2 Log will appear in the right pane.

Basic Search

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

The Web User that generated the log entries. Click the User link to see more details about the Web User.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

MDNs Pending Approval

This option will filter results for messages that require a manual MDN receipt.

Note: Automatic and Manual Asynchronous MDN preferences are set on the AS2 tab of the "HTTPS Configuration" on page 521 page.

Rows Per Page

The number of rows to display on the page at a time.

Advanced Search

The Advanced Search provides additional search options including the Basic Search options for the AS2 Log.

Command

Audit Log search results will be filtered by the selected commands.

Message ID

The Message ID, if known, of the received message.

From ID

The From ID, if known, of the received message. This is the AS2 From ID of the Web User who sent the message.

Event ID

An Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

Session ID

The Session ID of the session that initiated the commands.

System Name

The name of the system that processed the transaction. This is commonly used in a clustered environment.

Audit Log Detail Links

- Click the **Find** icon to view Audit Log Details for any entry.
- Click the **Triggers** icon to view Triggers that were started from this event via the Trigger Log page.
- Click the **Web Users** icon to view information about the Web User that performed the action. Click the **Manage User** button in the resulting pop-up to open the Web Users page for that Web User account.

Action Buttons

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages that meet the filter criteria to a .CSV file on your local computer.

Available Options

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages that meet the filter criteria to a .CSV file on your local computer.

AS2 Columns

- Subject - The subject name of the message.
- To ID - The name or ID used by the recipient.
- Signature Algorithm - The MD5 or SHA1 signature algorithm that was used to sign the message.
- MDN Type - The type of *MDN*.
- MDN Sent - Indicates if the MDN was sent.
- MIC Algorithm - The algorithm used for the Message Integrity Code.
- Message ID - The ID number of the message.
- From ID - The name or ID used by the sender (Managed File Transfer).

- Encryption Algorithm - The algorithm used for encrypting the AS2 Message.
- Compressed - If compression was used on the message.
- MDN Signed - Indicates if the MDN was signed with a certificate.
- MIC - The Message Integrity Code.
- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- System Name - The name of the Managed File Transfer server that processed the event. This name is configured in the [installdirectory]/config/cluster.xml file (where [installdirectory] is the installation directory of Managed File Transfer)
- Start Time - The time the event started. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the event finished. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- Time (ms) - The duration or total time of the event. This value is displayed in milliseconds.
- Command - The action requested by the User.
- Event Type - The system generated event based on the Command and Status. These event types are referenced by Triggers and Audit Log Rules.
- Status - The status of the transaction.
- Local IP - The IP address that received the request.
- Local Port - The port that received the request.
- Remote IP - The IP address of the Web User's system that sent the request.
- Remote Port - The port on the Web User's system that sent the request.
- Session ID - A unique identifier created per Web User connection. All transactions made through this connection are referenced by the same Session ID number.
- User - The account name of the Web User performing the actions.
- Physical Path - The absolute or full path location of the file or folder on the file system.
- Virtual Path - The relative path of the file or folder as it appears to Web Users.
- File Size - The size of the file, in bytes.
- Remarks - Additional information about the transaction.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

MLLP Log

The MLLP Log page allows you to query, view and export audit entries for the MLLP service. Entries can be filtered using a wide variety of search criteria. The date range available is dependent on how long entries are retained in the database, which is configured in the “Log Settings” on page 693.

To view the MLLP Log, log in as an Admin User with the **Auditor** role.

From the main menu bar, select **Logs** > **Audit Logs**. Select **MLLP service** from the Service Logs section in the left pane. The MLLP Log will appear in the right pane. Success and failure events are displayed.

Basic Search

Use the following basic properties to search for logs:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

Message ID

A Message ID is assigned to each message processed by Managed File Transfer.

Status

There are three status types by which to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

Rows Per Page

The number of rows to display on the page at a time.

Advanced Search

Use the following advanced properties to search for logs:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

Message ID

A Message ID is assigned to each message processed by Managed File Transfer.

Status

There are several status types by which to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

Event ID

A Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Ack Type

The acknowledgement type associated with the message. Select one of the following acknowledgement types:

- Application Accept (AA) acknowledgement.
- Application Error (AE) acknowledgement.
- Application Reject (AR) acknowledgement.
- Commit Accept (CA) acknowledgement.
- Commit Error (CE) acknowledgement.
- Commit Reject (CR) acknowledgement.

Local IP

The IP address of the Managed File Transfer listener that received the commands.

Remote IP

The IP address of the remote system that initiated the commands.

System Name

The name of the system that processed the transaction. This is used when running Managed File Transfer in a clustered environment.

Trigger Log

The Trigger Log keeps track of the Trigger Execution history. The date range available when searching the Trigger Log is dependent on the Days to keep Trigger Logs setting on the Triggers tab of the "Log Settings" on page 693. Follow the instructions below to view the Trigger Log:

To view the Trigger Log, log in as an Admin User with the Trigger Manager or Auditor role.

From the main menu bar, point to Logs and then click **Audit Logs**. Select **Shared Drive** from the Service Logs section from the left pane. The Shared Drive Log will appear in the right pane.

In the **Trigger Log** page, specify the desired search criteria and then click the **Search** button.

Click the  icon to view "View Trigger Log Details" on page 689.

Basic Search

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

Trigger Name

The Trigger name can be specified to help narrow the search results. Leave blank to include all triggers.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

MDNs Pending Approval

This option will filter results for messages that require a manual MDN receipt.

Note: Automatic and Manual Asynchronous MDN preferences are set on the AS2 tab of the "HTTPS Configuration" on page 521 page.

Results per Page

The number of rows to display on the page at a time.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the **Export** options, only the visible columns are saved to the exported file.

Advanced Search

The Advanced Search tab provides the additional search criteria:

Event ID

An Event ID is assigned to each transaction by Managed File Transfer. This Event ID is passed along in reports and allows for easy reference.

Service

The Services are the protocols that were used for transferring the files. Select which Service type results you wish to see in your Trigger Log.

Event Type

The Event Type can be specified to limit search results. Leave blank if unknown or to return more results.

Columns

Click the **Columns** button to change the visible columns.

Export

If you use one of the Export options, only the visible columns are saved to the exported file.

Trigger Columns

- Trigger Name - The name of the trigger.
- Service - The service on which the event took place. .
- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- Event Type - The system generated event based on the Command and Status.
- Start Time - The time the Trigger started. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- End Time - The time the Trigger finished. This field is formatted according to the Timestamp Pattern defined in the Global Settings for Managed File Transfer.
- Status - The Status field reports if the Trigger was successful, failed or is still in progress.
- Time (ms) - The duration or total time of the Trigger. This value is displayed in milliseconds.

View Trigger Log Details

Follow the instructions below to view Trigger Log Details:

1. Log in as an Admin User with the Trigger Manager or Auditor role.
2. From the main menu bar, point to **Workflows** and then click **Triggers**.
3. In the Trigger Manager page, click the  Action icon and then choose  View History.
4. The Trigger Execution History page appears. Click the  Log icon to open the Trigger Log Details page.
5. When finished viewing the Trigger Log Details, click the **Done** button.

File Audit Log

When a file is processed by a Managed File Transfer Project, all file activity, resources, and services used for the file are recorded in the File Audit Log. This Log allows you to search for file activity using a variety of criteria, such as:

- File Name
- Date and time the file was processed
- The Admin User who submitted a Job that processed the file
- The source and destination file paths
- File events, such as when a file is read, written, transferred, renamed, or deleted
- If the event that included the file was successful or failed
- The type of protocol that was used to transfer the file (FTP, FTPS, SFTP, HTTPS, etc.)
- The Job Number
- The Resource Name that handled the file (SFTP Server, Network Location, etc.)
  To view the File Audit Log in Managed File Transfer, log in as an Admin User with the Auditor role.

  From the main menu bar, point to Logs and then click **Audit Logs**. Select **File Audit** from the Job Logs section in the left pane. The File Audit Log will appear in the right pane.

  Search for file audit activity using the following search tools:

Basic Search

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

Run User

The Admin User account that was used to submit the Job.

Status

There are three status types that can be used to filter the logs:

- Successful - Returns records where the event completed normally
- Warning - Returns records where the event produced a warning
- Error - Returns records where the event encountered a problem

File Name

The name of the file used by a Project.

Advanced Search

The Advanced Search provides additional search options including the Basic Search options for Completed Jobs.

File Event

Select the type of processing that was done on a file.

Destination File Name

The name of the file when it was created, copied, or moved to a destination directory.

Protocol

The type of protocol that was used to transfer the file from the source directory to the destination directory.

Columns

Click the **Columns** button to change the visible columns.

Source File Path

The path to the file before it was processed by a Project.

Destination File Path

The path to the file after it was processed by a Project.

Alternative Searches

You can perform the following searches:

Search by Job Number

Search logs according to the job number, a unique number given to each Project at runtime.

Search by Resource Name

Specify logs according to the resource that was used in the processing of the Job.

Search by Event ID

Specify logs according to the event ID, the unique number assigned to the event. This number is sequential to the order in which the events started. .

Table Navigation Tools

The following table navigation tools are available:

- "Audit Log Details" on page 699 the Audit Log Details by selecting the View icon.
- "Job Log and Details" on page 186 the Job Log by selecting the Job ID link.
- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Export Page** button to save only the results on the visible page to a .CSV file on your local computer.
- Click the **Export Results** button to save the results from all pages to a .CSV file on your local computer.

  Note: The default saved Job Log file name is "JobLogsYYYYMMDD.csv" (where YYYYMMDD is the current year, month, and day).
- Click the **Columns** button to select which Completed Jobs properties are displayed in the table. The following properties are available:
- Event Type - The type of processing that was done to the file.
- Start Time - The date and timestamp of when the job started executing.
- Source File Name - The name of the file in the source directory.
- Status - The outcome of the job (Successful, Failed or Canceled).
- Task Name - The Managed File Transfer Project Task name used to process the file.

- Run User - The Admin User account that was used to submit the job.
- Time(ms) - The amount of time the job took to complete (in milliseconds).
- Job Number - A unique Job ID number given to each Project at runtime.
- Event ID - A unique number assigned to the event. This number is sequential to the order in which the events started.
- Source File Path - The path where the file originated.
- Source File Size - The size of the file before the Job was executed.
- Source Resource Name - The Managed File Transfer Resource that was used to access the file.
- Source Protocol - The protocol used to access the file.
- Source Server Host - The host name of the server used to access the file.
- Source Server User - The Web User account that was used to transfer a file.
- Destination File Name - The name of the file in the destination directory.
- Destination File Path - The path where the file is located after the Job completed.
- Destination File Size - The size of the file after the Job was executed.
- Destination Resource Name - The Managed File Transfer Resource where the file was created or transferred.
- Destination Protocol - The protocol used to transfer the file.
- Destination Server Host - The host name of the server used to transfer the file.

File Audit Log Details

Each time a File is processed by Managed File Transfer, all file activity, resources, and services used for the file are recorded in the File Audit Log. The File Audit Log Details page provides an overview of the file activity.

Audit Events Log

The MFT administrator can use the Audit Events log to monitor and track the actions performed on MFT resource types, the admin user, or the web user.

To view the Audit Events, log in as an Admin User. From the main menu bar, point to Logs and then click **Audit Logs**. Select **Audit Events**. The Audit Events log appears in the right pane.

In the **Audit Events** page, specify the desired search criteria and then click the **Search** button.

Click the icon to view "Audit Event Details" on page 693.

Basic Search

Date Range

Enter the scope of your search based on date and time.

User

Enter the user name to help narrow the search results. Leave blank to include all users.

Object Type

Enter the type of resource, the admin user, or the web user to help narrow the search results. Leave blank to include all object types.

Object Name

Enter the name of the resource type, name of the admin user, or name of the web user used in a project.

Action Type

Enter the action performed for the resource, admin user, or web user.

Advanced Search

The Advanced Search tab provides the additional search criteria:

Date Range

The Date Range allows you to specify the scope of your search based on date and time.

User

You can search for an event based on the beginning, ending, or any character the user name contains.

Object Type

You can search for an event based on the beginning, ending, or any character the object, or resource types, the admin user, or the web user contains.

Object Name

You can search for an event based on the beginning, ending, or any character the object, or resource types, the admin user, or the web user contains.

Action Type

You can search for an event based on the beginning, ending, or any character the action type contains.

Audit Event Details

All actions performed on Resources with respect to creation, deletion, and update are audited along with their configuration in the Audit Events log.

Perform the following actions to view the audit events log details:

1. Log in as an Admin User.
2. From the main menu bar, point to Logs and then click Audit Logs.
3. Select Audit Events.
4. In the Audit Events page, click the icon to view the audit event details.
5. After viewing the details, click the **Done** button.

Log Settings

The Log Settings page provides central control over all log settings in Managed File Transfer. The log settings for each service and function within Managed File Transfer can be configured on the respective tab.

To administer Logs, log in as an Admin User with the **Product Administrator** role.

From the main menu bar, point to Logs and then click **Log Settings**.

Global Log

The Global Log tab covers the log settings used by Managed File Transfer for server logs.

Logs Directory

The location of the server logs for Managed File Transfer. By default, this location is relative to the Managed File Transfer installation directory. If Managed File Transfer is installed in `/informatica/B2B/MFT/server`, then the default location for the logs directory is `/informatica/B2B/MFT/server/userdata/logs`.

Note: When running in clustered mode, this path must point to a location on the network that is the same for all other systems in the cluster.

Global Log Level

The global log will record information and error messages that pertain to global activity such as when services start/stop or when administrative Users are created and login. The default setting Normal writes standard information to the log. If Debug is selected, a higher level of detail is recorded for events. Debug should only be used for troubleshooting an issue since it can impact performance and increase the size of the log file.

Log File Extension

The default log file extension is .log. If you wish to specify another extension, type it in this box. The default file name is gaservices.log. When running in clustered mode, the system name is appended to the log file name (for example, gaservices_PRD01.log). Regardless of the extension, the log files can be opened in any text editor.

Maximum Log Size

Specify the maximum size the log file can reach, in MB (megabytes), before a rotation takes place. A rotation renames the active log file with a numeric suffix (for example, gaservices.log.1), when the log file reaches the specified file size. At this point a new log file is started without the loss of any log entries. The purpose of log file rotation is to prevent log files from growing indefinitely and becoming difficult to manipulate.

Note: Changing any of the settings on the Global Log tab requires a restart of Managed File Transfer.

Syslog

Enabled

If selected, options are available to send Managed File Transfer logs to an enterprise Syslog server. By default, logging to a Syslog server is not enabled.

Host

The host name or IP address of the Syslog server to which various log events are sent.

Port

The port number on which the Syslog server is listening for incoming connections and/or log events. The Port value must be a number between 1 and 65535.

Protocol

The transfer protocol used for communicating with the Syslog server. UDP connections are faster as they simply push data to the Syslog server, but do not have the error control capability of TCP. If using UDP and a packet is lost or received in the wrong order, nothing is recorded in the server log. When using TCP, if a packet fails while being sent to the Syslog server, an error message is logged in the [installdirectory]/tomcat/logs folder (where [installdirectory] is the installation directory of Managed File Transfer). The TCP connection will keep resending the packet until successful. The default setting is UDP.

Facility

The facility name is a way of determining which process of the machine created the message. The default setting is User.

Application ID

The Application ID is the name that is assigned to this application. All entries sent to the Syslog server will contain the Application ID to help identify it in the Syslog. The default setting is gaservices.

Application Log Level

The Application Log Level is the severity level of the application message that is sent to the Syslog server. The default setting is Error (Syslog level 2). For example, only entries in the Managed File Transfer "Server Log Viewer" on page 671 marked ERROR would be replicated to the Syslog. If the Application Log Level was set to Info, then all Server Log entries marked INFO would be replicated to the Syslog.

Audit Trail Log Level

The Audit Trail Log Level is the severity level of the "Audit Log Details" on page 699 message that is sent to the Syslog server. The default setting is Error (Syslog level 7). The Audit Logs focus on the security aspect of file transfers related to FTP, FTPS, SFTP, HTTPS, and AS2. Successful transfers are logged with the severity set to INFO and failed transfers are logged with the severity level set to ERROR.

Job Logs

The Job Logs tab contains the following fields.

Job Log Format

The format of all Job logs created by Managed File Transfer. The default setting is Text.

- Text:The logs will be written in plain text format.
- HTML: The logs will formatted with HTML tags for viewing through a web browser.

Job Log File Extension

The file extension to use for the Job logs created by Managed File Transfer.

Days to Keep Job Logs

The number of days to keep Job logs. All Job logs that are older than the specified value will be deleted automatically. A value of 0 (zero) will keep the Job logs indefinitely. If a Job created temporary workspace directories, they are also deleted at this point.

Days to Keep Job File Audit Logs

The number of days the audit log will be kept for a File. All Job File logs that are older than the specified value will be deleted automatically. A value of 0 (zero) will keep the Job File logs indefinitely.

Archive Purged Records

The log for each Job File can be archived after the specified retention period. Logs are saved as a CSV formatted file in a sub-folder of the Logs Directory, specified on the Global Log tab. The sub-folder location for the archived logs is: `[installdirectory]/userdata/logs/Jobs/year/[month]/[date].csv`. For example, if the Job File log is set to archive, the folder location might look like: `[installdirectory]/userdata/logs/Jobs/2015/12/20151231.csv`. The purge process runs every 24 hours.

Services

The Services tab specifies the log retention period and purging options for each service type.

Days To Keep Audit Log Records (per service)

The number of days the audit log will be kept for a particular service. The log for each service can be viewed from the Logs menu.

Archive Purged Records

The log for each service can be archived after the specified retention period. Logs are saved as a CSV formatted file in a sub-folder of the Logs Directory, specified on the Global Log tab. The sub-folder location for the archived logs is: `[installdirectory]/[Log Directory]/[service]/[year]/[month]/[date].csv`. For example, if the HTTPS service log is set to archive, the folder location might look like: `[installdirectory]/userdata/logs/HTTPS/2012/12/20121231.csv`. The purge process runs every 24 hours.

Secure Mail

A Package will be marked as inactive when it is deleted, revoked, reaches the maximum download limit, or expires. The purge settings are based on the date the Package becomes inactive or reaches the maximum retention date. A daily process checks for packages that need to be purged based on their settings below. If a Web User account is deleted, all packages associated with that account will be set to inactive and deleted as part of the purge process.

Retention Period for Drafts

Days to Keep Draft Messages - Secure Mail messages are in draft status until they are successfully sent. Draft messages can be retained on the Managed File Transfer server for the specified number of days after a messages has been saved or modified. The allowable range to keep draft messages is between 0 and 999 days. A value of 0 prevents the draft messages from being purged .

Retention Period for Active Messages

Days to Keep Packages: Active packages have been successfully sent and can be viewed by their recipients. Active packages can be retained on the Managed File Transfer server for the specified number of days after a message as been sent. The allowable range to keep active packages is between 0 and 999 days. A value of 0 prevents the Active messages from being purged.

Retention Period for Inactive Packages

- Days To Keep File Attachments: The files will be retained on the Managed File Transfer server for the specified number of days after a Package has been inactivated. The days to keep file attachments must be less than or equal to the days to keep records for inactive packages. The allowable range to keep inactive file attachments is between 1 and 999 days. By default, files for a Package are stored in the following location: [installdirectory]/userdata/packages/[creationdate]/[PackageID]. The default Package location is defined on the Services tab in the "Global Settings" on page 752.
- Days to Keep Package Records: For auditing purposes, the Package information can be retained between 1 and 999 days after a Package has been inactivated. The days to keep records must be greater than or equal to the days to keep file attachments for inactive packages. It is recommended to keep records for the same number of days as the Days to Keep Audit Log Records setting for the HTTPS service on the Services tab.

  Note: When a Package is marked as deleted in the "Package Manager" on page 571 or the File Transfer Portal, the files are deleted immediately and are not affected by this setting.

Shared Drive

The Shared Drive tab specifies the log retention period and purging options for Shared Drive events.

Days to Keep Audit Log Records

This is the number of days the Shared Drive Logs will be maintained. Shared Drive logs older than the specified duration are deleted.

Archive Purged Records

he log for each Shared Drive event can be archived after the specified retention period. Logs are saved as a CSV formatted file in a sub-folder of the Logs Directory, specified on the Global Log tab. The sub-folder location for the archived logs is: `[installdirectory]/userdata/logs/Shared Drive/year/[month]/[date].csv`. For example, if the Shared Drive log is set to archive, the folder location might look like: `[installdirectory]/userdata/logs/SharedDrive/2015/12/20151231.csv`. The purge process runs every 24 hours.

Triggers

The Triggers tab has the following fields:

Days to Keep Trigger Logs

This is the number of days the Trigger Logs will be maintained. Trigger logs older than the specified duration are deleted.

Audit Log Rules

In some situations, not all events need to be logged from trusted connections. The purpose of the Audit Log Rules is to help minimize the size of your logs. The options on the Audit Log Rules page determine which "Event Types" on page 799 can be excluded from the logs. The audit log rules can be configured to filter specific services or exclude logging events for certain IP addresses.

To administer Audit Log Rules, log in as an Admin User with the **Product Administrator** role.

From the main menu bar, point to Logs and then click **Log Exemptions**. The Audit Log Rules page appears.

Filter the audit log rule list by selecting the Event Type from the drop-down list. Selecting an Event Type will only display those events on the page. Show all Events by selecting the blank line at the top of the Event Type drop-down list.

Page Toolbar

The following actions are available from the page toolbar:

- "Audit Log Rule Configuration" on page 698 an audit log rule by clicking the **Add Rule** link in the page toolbar.
  - Disable all audit log rules by clicking the Disable Audit Log Rules link in the page toolbar. Audit log rules will be suspended until the Enable Audit Log Rules link in the page toolbar is clicked (even if Managed File Transfer is restarted).
  - Test if a specific event will be logged by clicking the Test Audit Log Rules link in the page toolbar and then provide the requested information in the resulting Test Audit Log Rules box.

Audit Log Rules Actions

The following actions are available by selecting the Actions icon:

- "View Audit Log Rule" on page 699 details for an audit log rule by clicking the icon
- "Audit Log Rule Configuration" on page 698 an audit log rule by clicking the icon
  - Delete an audit log rule by clicking the icon
- "Audit Log Rule Configuration" on page 698 an audit log rule by clicking the icon

Audit Log Rule Configuration

The Audit Log Rule page allows you to configure filters that exclude certain event types from being added to the log for the specified IP addresses. Specify the name, event type to exclude and IP addresses, then click the **Save** button to save the audit log rule.

Name

A unique name for the audit log rule. The maximum length of the name is 128 characters.

Event Type

The "Event Types" on page 799 that will be excluded from the log.

Service

An audit log rule can be configured differently for each service type. The audit log rule can apply to all services or only the selected services.

Exclude For

Logging can be excluded for the specified event type on all IP addresses or only specific addresses. When specifying IP addresses, type an IP address in either single IP, IP range or *CIDR* notation format. Type each IP address entry on a new line or separate addresses with commas. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255). The maximum number of characters for this field is 2000.

Note: A single IPv4 address is comprised of four sets of three numbers from 0 to 255, separated by periods. A single IPv6 address is comprised of eight sets of four hexidecimal numbers, separated by colons. An IP range includes all the addresses between two specified addresses. The addresses are separated by a hyphen. An IP address in CIDR notation is an IP address followed by a "prefix." The prefix notates a range of IP addresses without the need to type all the sets.

View Audit Log Rule

The View Audit Log Rule page displays the parameters for the rule, including when the rule was created and by whom. Click the **Done** button to return to the Audit Log Rules page.

Follow the steps below to view the details for the Audit Log Rule:

1. Log in as an Admin User with the Product Administrator role.
2. From the main menu, point to Logs and then click **Audit Log Rules**.
3. In the "Audit Log Rules" on page 698 page, click the  icon beside the rule you wish to view. Then from the drop-down, click  **View**.

Audit Log Details

The Audit Log Details page displays the audit details of a specific entry in the Audit Log Search Results.

To view the Audit Log Details for an action:

1. Log in as an Admin User with the **Auditor** role.
2. From the main menu bar, point to Logs and then click to open one of the service logs.
3. In the list of service log results, click the  icon beside an entry to view the Audit Log Details.
   - Click the  icon to view the "View Trigger Log Details" on page 689, if a Trigger ran.
   - Click the **Done** button to return to the list of audit entries.

CHAPTER 9

Encryption

This chapter includes the following topics:

Encryption Overview

Data Risks

Unless otherwise protected, all data transfers, including electronic mail and FTP, travel openly over the Internet and can be monitored or read by others. Given the volume of transmissions and the numerous paths available for data travel, it is unlikely that a particular transmission would be monitored at random. However, programs, such as "sniffer" programs, can be set up at opportune locations on a network to simply look for and collect certain types of data (for example, user names, passwords, credit cards numbers, social security numbers, etc).

Encryption

Encryption, or cryptography, is a method of converting information into unintelligible code. The process can then be reversed, returning the information into an understandable form. The information is encrypted (encoded) and decrypted (decoded) by what are commonly referred to as "cryptographic keys." These keys are actually values, used by a mathematical algorithm to transform the data. The effectiveness of encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected.

Because encryption renders information unreadable to an unauthorized party, the information remains private and confidential, whether being transmitted or stored on a system. Unauthorized parties will see nothing but an unorganized assembly of characters. Furthermore, encryption technology can provide assurance of data integrity as some algorithms offer protection against forgery and tampering. The ability of the technology to protect the information requires that the encryption and decryption keys be properly managed by authorized parties.

Key Systems

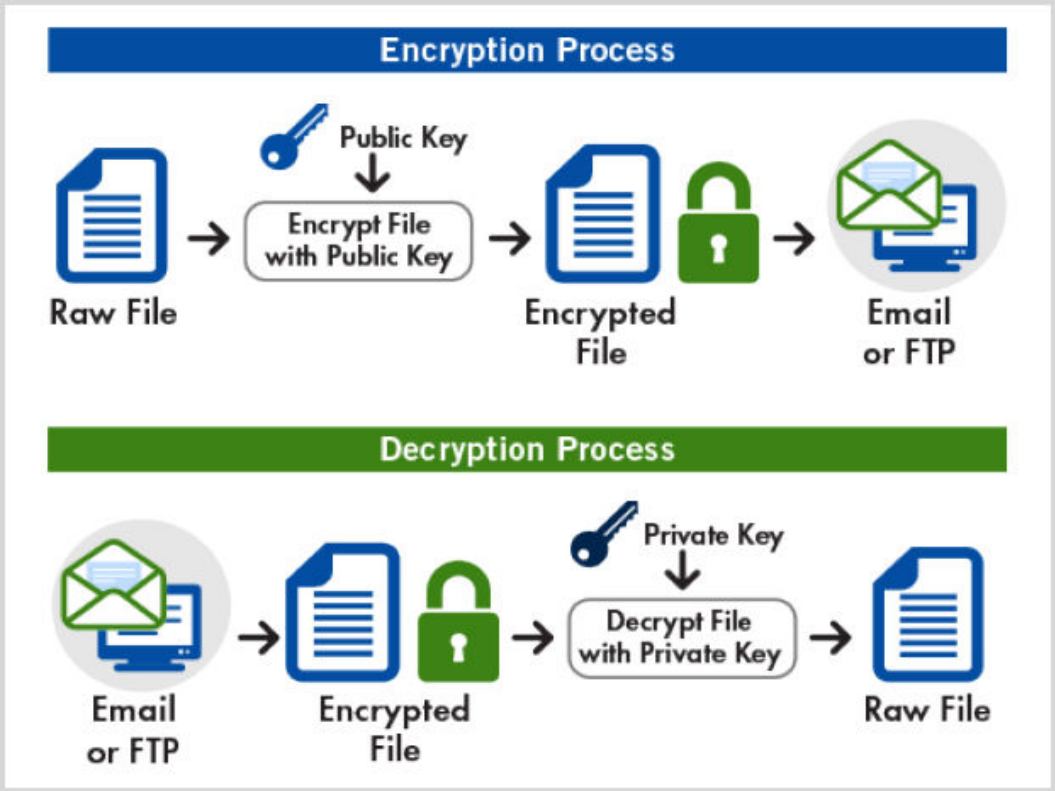
There are two types of cryptographic key systems, *symmetric* and *asymmetric*.

With a symmetric key system (also known as secret key or private key systems), all parties have the same key. The keys can be used to encrypt and decrypt messages, and must be kept secret or the security is compromised. For the parties to get the same key, there has to be a way to securely distribute the key to each party. While this can be done, the security controls needed can make this system impractical for widespread and commercial use on an open network like the Internet. Asymmetric key systems can solve this problem.

In an asymmetric key system (also known as a public key system), two keys are used. One key is kept secret, and therefore is referred to as the "private key." The other key is made widely available to anyone that needs it, and is referred to as the "public key." The private and public keys are mathematically related so that information encrypted with the public key can only be decrypted by the corresponding private key.

Asymmetric Encryption Diagram

The following image shows the encryption process:



The private key, regardless of the key system utilized, is typically specific to a party or computer system. It is mathematically impossible for the holder of any public key to use it to figure out what the private key is.

Regardless of the key system utilized, physical controls must exist to protect the confidentiality and access to the key(s). In addition, the key itself must be strong enough for the intended application. The appropriate encryption key may vary depending on how sensitive the transmitted or stored data is, with stronger keys utilized for highly confidential or sensitive data. Stronger encryption may also be necessary to protect data that is in an open environment, such as on a Web server, for long time periods. Because the strength of the key is determined by its length, the longer the key, the harder it is for high-speed computers to break the code.

Encryption Options in Informatica Managed File Transfer

Managed File Transfer provides several different encryption standards for protecting the privacy and integrity of your organization's data. These encryption standards are described below:

Encryption standard	Key Type	Encryption
"Compress and Send a File with SSH Authentication" on page 254	Symmetric	File

"Compress and Send a File with SSH Authentication" on page 254	Symmetric	File
"OpenPGP Encryption" on page 705	Asymmetric	File
"AS2 (S/MIME over HTTP(S))" on page 716	Asymmetric	File/Connection
"Quick Start for Secure Email" on page 719	Asymmetric	File/Connection
"SCP Task" on page 427	Asymmetric	Connection
"SFTP (SSH File Transfer Protocol)" on page 711	Asymmetric	Connection
"FTPS (FTP over SSL)" on page 714	Asymmetric	Connection
"HTTPS Task" on page 512	Asymmetric	Connection

Key Type

ZIP implements a Symmetric key type, which means that the same password can be used to encrypt and decrypt the file. The other standards (listed above) implement an Asymmetric key type, in which one key will be used to encrypt the data and a different key will be used to decrypt the data.

File Encryption

ZIP and OpenPGP can encrypt the files themselves, protecting the data at rest. Secure Email and AS2 are able to encrypt files before they are sent to protect sensitive information over an unsecured connection.

Connection Encryption

The entire connection (pipe) between the client and server can be encrypted using SSL or SSH. Any commands, messages and data flowing over the connection will be encrypted.

Choosing the Right Encryption Method

There are several factors to consider when choosing the encryption standards to implement. The flexibility in Managed File Transfer allows you to choose the encryption standard for each individual transfer. For instance, you may want to use a simple encryption standard (such as ZIP) when exchanging not-so-sensitive data with a customer, whereas choose a strong encryption standard (such as OpenPGP) when exchanging highly-sensitive data.

The following questions should be asked before choosing the encryption standard to use:

1. How sensitive is the data being exchanged?
2. How will the data be transported (for example, FTP, Email, HTTP)?
3. Are large files being exchanged (which should be compressed)?
4. Should the files be encrypted (before transmission) or should the connection be encrypted?
5. What encryption standards does your trading partner support?
   A trading partner may dictate the encryption standards which they support. For instance, many banking institutions require that their customers encrypt files using the OpenPGP encryption standard.

   Listed below are several sample scenarios and the recommended encryption standard to use.

Scenario 1

You need to send your price list file to your customers over email. You want to make it simple for the customers to open the file. The price list information is not extremely sensitive, but you would like to at least password-protect it.

Recommendation: "Compress and Send a File with SSH Authentication" on page 254 or "Compress and Send a File with SSH Authentication" on page 254

Scenario 2

You need to send your payroll direct deposit information to the bank. This is considered as highly sensitive information. The bank wants you to send this information over a standard FTP connection.

Recommendation: "OpenPGP Encryption" on page 705

Scenario 3

Your trading partner wants to exchange information with you over a secure FTP connection. This trading partner wants to authenticate your company with a password or public key.

Recommendation: "SFTP (SSH File Transfer Protocol)" on page 711

Scenario 4

Your trading partner wants to exchange information with you over a secure FTP connection. This trading partner wants to authenticate your company with a signed certificate.

Recommendation: "FTPS (FTP over SSL)" on page 714

Scenario 5

You need to send purchase orders to your vendors, which you consider as fairly sensitive. The files can be rather large in size and should be compressed. The purchase orders could be sent over standard FTP connections or via Email.

Recommendation: "Compress and Send a File with SSH Authentication" on page 254 or "OpenPGP Encryption" on page 705

Scenario 6

You need to send EDI information securely to a trading partner and you need confirmation that they received the exact document(s) you sent them.

Recommendation: "AS2 (S/MIME over HTTP(S))" on page 716

Scenario 7

You need to send sensitive information in the message body of an email.

Recommendation: "Quick Start for Secure Email" on page 719

HTTPS/AS2 (HTTP over SSL) - Standards

Listed below are the HTTPS versions, standards, algorithms and key store formats supported by Managed File Transfer.

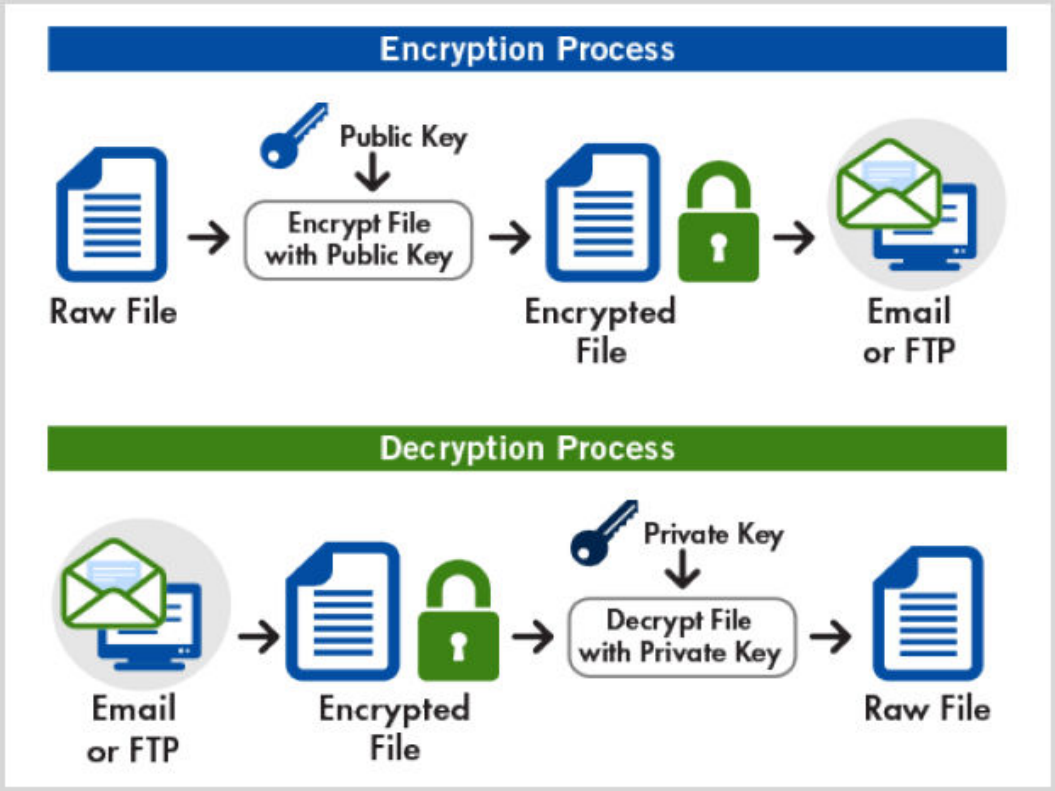
SSL Versions	Authentication and Key Exchange Algorithms
- SSL 2.0 - SSL 3.0 (also known as TLS 1.0)	- Diffie-Hellman - DSA - RSA
SSL Security Protocols	Hash Algorithms
- SSL - TLS	- MD5 - SHA1
Ciphers (Symmetric Encryption Algorithms)	Certificate Key Store formats
- AES-128 - AES-192 - AES-256 - DES - RC4 - Triple DES (DESede)	- JKS (Java Key Store) - PKCS12

OpenPGP Encryption

Managed File Transfer incorporates OpenPGP compliant encryption technology to address the privacy and integrity of data. OpenPGP is an industry standard that uses a combination of asymmetric (public key)

cryptography and symmetric cryptology for providing a high level of data protection, making OpenPGP one of the most popular encryption methods used today.

The following figure shows the encryption process:



OpenPGP also address the issues of data *authentication* and *non-repudiation* with the ability to “sign” files via an embedded *digital signatures*.

Note: The OpenPGP encryption and decryption processes in Managed File Transfer have been tested for compatibility with many other PGP products, including PGP Desktop from PGP® Corporation, E-Business Server from McAfee® and GnuPG.

After encrypting files with OpenPGP, Managed File Transfer can place the resulting files on the Local File System, send them to another server (such as an FTP server) or send them to one or more email recipients. For instance, a “Project Design” on page 100 can be defined to automatically retrieve records from a database, create an Excel document from those records, then encrypt the document and email it to one or more recipients.

Managed File Transfer also allows you create Projects to retrieve encrypted files, decrypt and/or verify the files and import the data from the decrypted files into a database.

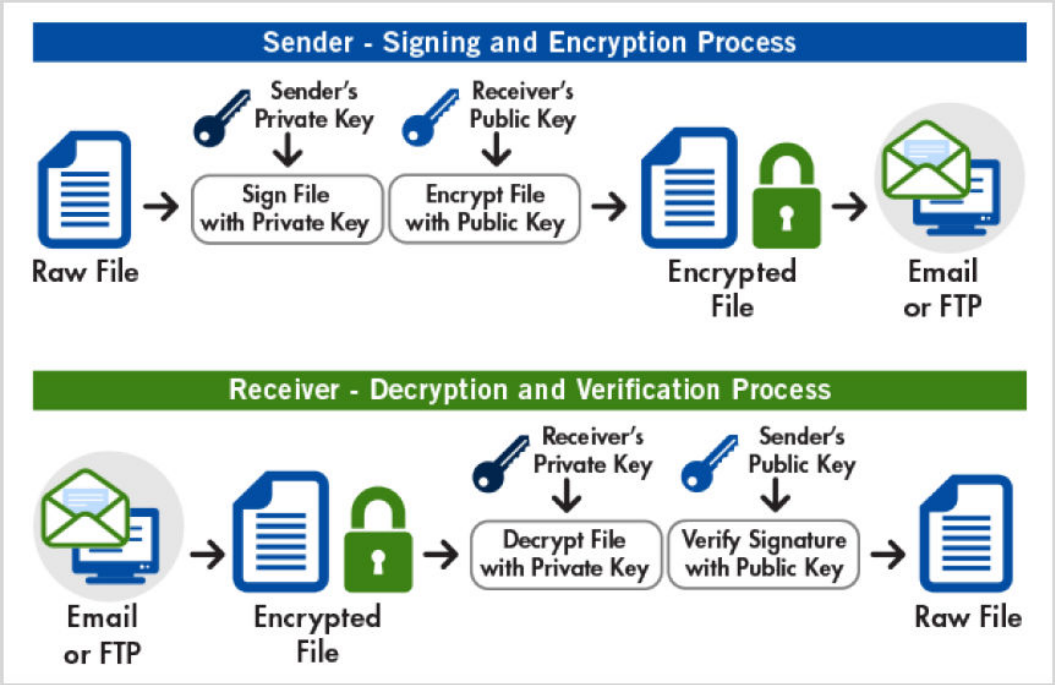
Managed File Transfer includes an integrated “OpenPGP Key Manager” on page 723 to manage your OpenPGP keys. This key management tool can be used to create keys, change keys, export keys and import keys. These keys can then be utilized within Managed File Transfer Projects for performing OpenPGP encryption and decryption.

Digital Signatures

A trading partner may require that you additionally "sign" your files with your Private Key, which will embed a digital signature into those files. The trading partner will then use your Public Key to authenticate the files

after they are received. Digital Signatures allows the trading partner to ensure that you are the true originator of the files.

The following image shows the keys needed to encrypt and sign (embed your digital signature) your files:



Quick Start for OpenPGP Encryption

Follow these steps to send encrypted files to a trading partner.

Step 1: Import your trading partner's Public key

Import your trading partner's Public key into your Key Ring by following the instructions below.

1. Launch the "OpenPGP Key Manager" on page 723 by first logging as a user with the Key Manager role.
2. From the main menu-bar select **Encryption**, and then click **OpenPGP Key Manager**.
3. Click the Import Key(s) menu option in the tool bar.
4. Browse for the trading partner's Public key on your hard disk and select it.
5. Click the **Import** button to import the Public key from the specified file.
6. If the import is successful, the trading partner's Public key will be loaded into your Public Key Ring and will be listed on the page.

Step 2: Create a Resource to point to the OpenPGP Key Ring

If you haven't done so already, create a "OpenPGP Key Rings Resource" on page 91"OpenPGP Key Rings Resource" on page 91 that points to your Key Ring.

1. Log in to Managed File Transfer as a user with the Resource Manager role.
2. Click the Resources menu option.
3. From the list of resource types on the left hand side, click the OpenPGP Key Rings icon.

4. Click the Add OpenPGP Key Ring link in the tool bar.
5. Specify a name for this resource (for example, "Default Key Ring").
6. Specify the location of the public and secret key rings. The default location of the public key ring is [installdirectory]/userdata/keys/pgp/pubring.pkr where [installdirectory] is the installation directory of the Managed File Transfer product. The default location of the secret key ring is [installdirectory]/userdata/keys/pgp/secring.skr
7. Click the **Save** button.
8. This Key Ring resource can now be used in one or more Managed File Transfer Projects to encrypt, decrypt, sign and verify files.

Step 3: Create a Project to encrypt files

1. Log in to Managed File Transfer as a user with the Project Designer role.
2. From the main menu-bar select **Workflows**, and then click **Projects**.
3. Drill down to the folder in which to create the new Project.
4. Click the Create a Project link (located towards the top of the page).
5. The Managed File Transfer Project Designer will open on the page.
6. Type the new Project name and description.
7. Click the **Save** button.
8. The list of folders (containing tasks) will be displayed.
9. Open the File Encryption folder and choose the PGP Encrypt task.
10. On the PGP Encrypt Task Basic tab, specify the following:
    a. Select the Key Ring (OpenPGP Key Ring Resource) that contains the OpenPGP keys.
    b. For the Input File attribute, specify the location of your file to encrypt and sign.
    c. For the Output File attribute, specify the name of the encrypted file to create. Otherwise leave blank and the encrypted file will get a .pgp extension (for example, file.txt becomes file.txt.pgp)
    d. For the Output Directory attribute, specify the directory to place the encrypted file. Leave this field blank to create the encrypted file in the same directory as the input file.
    e. Specify any additional attributes for the task. Field level help can be accessed by clicking the field name.
11. To add a public key to encrypt the file with, click the **Add** button and choose **Add a Public Key** option from the menu.
12. This will display the page titled "Public Key".
13. Click the button next to the Key ID to open the “PGP Key Chooser” and select the public key.
14. Repeat steps 11 through 13 if you need to encrypt the file using multiple public keys.
15. To additionally sign the file (this is only needed if your trading partner requires digital signatures):
    a. Select the PGP Encrypt Task by clicking it in the project outline.

b. Click the **Add** button and choose Add a Secret Key from the context menu.

This will display a page titled "Secret Key".

Click the button (next to the Key ID) to open the “PGP Key Chooser” and select the private key.

Specify a passphrase for your private key. This is the passphrase you used when you first created your key pair.

16. Click the **Save** button to save the task.
17. You can add additional tasks (for example, FTP, Send Mail or HTTP) to the Project for sending the encrypted file to your trading partner's server.
18. When done making changes to the Project, click the Validate link (located towards the top of the page) to validate the syntax of the Project.
19. If the validation was successful, then click the **Save & Finish** button to save the Project and return to the folder.
20. Execute the Project.

Note: Learn more about how to edit Projects by referring to the section named “Project Designer Features” on page 104.

Quick Start for OpenPGP Decryption

Follow these steps to decrypt files.

Step 1: Create a new Key Pair (Public and Private key)

If you haven't done so already, you need to create an OpenPGP Key Pair, which is a combination of a Public and Private key.

1. “Create OpenPGP Key” on page 726 using the OpenPGP Key Manager.
2. “Export an OpenPGP Public Key” on page 727 and send it to your trading partner. They will use your Public key to encrypt any of your files.

Step 2: Create a Resource to point to the OpenPGP Key Ring

If you haven't done so already, create a “OpenPGP Key Rings Resource” on page 91 that points to your Key Ring.

1. Log in to Managed File Transfer as a user with the Resource Manager role.
2. Click the Resources menu option.
3. From the list of resource types on the left hand side, click the OpenPGP Key Rings icon.
4. Click the Add OpenPGP Key Ring link in the tool bar.
5. Specify a name for this resource (for example, "Default Key Ring").
6. Specify the location of the public and secret key rings. The default location of the public key ring is [installdirectory]/userdata/keys/pgp/pubring.pkr where [installdirectory] is the installation directory of the Managed File Transfer product. The default location of the secret key ring is [installdirectory]/userdata/keys/pgp/secring.skr
7. Click the **Save** button.

8. This Key Ring resource can now be used in one or more Managed File Transfer Projects to encrypt, decrypt, sign and verify files.

Step 3: Create a Project to decrypt files

1. Log in to Managed File Transfer as a user with the Project Designer role.
2. From the main menu, click **Workflows**, and then click **Projects**.
3. Drill-down to the folder in which to create the new Project.
4. Click the Create a Project link (located towards the top of the page).
5. The Managed File Transfer Project Designer will open on the page.
6. Type in the new Project name and description.
7. Click the **Save** button.
8. The list of folders (containing tasks) will be displayed.
9. Open the File Encryption folder and choose the PGP Decrypt task.
10. On the PGP Decrypt Task Basic tab, specify the following:
    a. Select the Key Ring (OpenPGP Key Ring Resource) that contains the OpenPGP keys.
    b. For the Passphrase attribute, specify the passphrase of your private (or secret) key. This is the passphrase you used when you first created your Key Pair.
    c. For the Input File attribute, specify the name of the file to decrypt. Otherwise specify a variable for the Input Files Variable to process a list of files that was received from your trading partner (which would have been populated from another task like FTP or HTTP).
    d. For the Output Directory attribute, specify the directory to store the decrypted files.
11. Click the **Save** button to save the task.
12. You can add additional tasks (for example, FTP, Send Mail or HTTP) to the Project for sending the encrypted file to your trading partner's server.
13. When done making changes to the Project, click the Validate link (located towards the top of the page) to validate the syntax of the Project.
14. If the validation was successful, then click the **Save & Finish** button to save the Project and return to the folder.
15. "Executing Projects" on page 181 the Project.

Note: You can learn more about how to edit Projects by referring to the section named "Project Designer Features" on page 104.

OpenPGP - Standards

The OpenPGP standard is a non-proprietary and industry-accepted protocol which defines the standard format for encrypted messages, signatures and keys. This standard is managed by the IETF (Internet Engineering Task Force). See RFC 4880 for more details on the latest OpenPGP standard.

Listed below are the OpenPGP standards and algorithms supported by Managed File Transfer.

RFC Standards - RFC 4880 Asymmetric Encryption Algorithms - Diffie-Hellman - DSA - RSA The key sizes supported are 512, 1024, 2048 and 4096 bits. Ciphers (Symmetric Encryption Algorithms) - AES-128 - AES-192 - AES-256 - Blowfish - CAST5 - DES - IDEA - Triple DES (DESede) - Twofish	Hash Algorithms - MD2 - MD5 - RIPEMD-160 - SHA1 - SHA-256 - SHA-384 - SHA-512 Compression Algorithms - ZIP - ZLIB

SFTP (SSH File Transfer Protocol)

The traditional FTP protocol sends commands and data in “the clear” over the network/internet. This FTP data could be intercepted by an attacker, which could then be viewed and altered before sending it on to the receiver.

If you are sending sensitive data over the internet, then you may want to consider the SFTP (SSH File Transfer Protocol) for securing data. The following image shows a model of the encryption at work:

SFTP creates an encrypted tunnel between two computer systems and will protect against the following attacks:

IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host

IP source routing, where a host can pretend that an IP packet comes from another, trusted host

DNS spoofing, where an attacker forges name server records

Interception of cleartext passwords and other data by intermediate hosts

Manipulation of data by attackers in control of intermediate hosts

SFTP uses a combination of *asymmetric* (public key) cryptology and *symmetric* cryptology to provide strong encryption and optimal performance.

SFTP is supported by most commercial servers and many open source servers (for example, Linux). SFTP is a good protocol to use for transmitting large files since it compresses the data stream prior to encryption.

Managed File Transfer implements current SSH 2.0 protocol standards.

The SSH Handshake process is detailed in the Appendix.

Quick Start for SFTP

Use the appropriate Quick Start guide based on whether your trading partner requires authentication with public key, password, or both.

Quick Start – Using SFTP with Public Key Authentication

Follow these steps to exchange files with a SFTP server using Public key authentication.

1. Create an SSH Key Pair (Public and Private key) in the SSH Key Manager.
2. Export the SSH Public key into a file and send this file to your trading partner.
3. Add an "SFTP Servers Resource" on page 66 in Managed File Transfer. Specify the parameters (host name, port, user name, etc.) for the SFTP server. Associate the SSH Private Key (created in step 1) with the SSH resource.
4. Add an "SFTP Task" on page 413 to a Managed File Transfer Project and choose the SSH resource (created in step 3).
5. You will be able to send and receive files to/from thatSFTP server by adding Put or Get elements to the SFTP task in the Project.

Quick Start – Using SFTP with Password Authentication

Follow these steps to exchange files with a SFTP server using Password authentication.

1. Request your password from the organization that hosts the SFTP server.
2. Add an "SFTP Servers Resource" on page 66 in Managed File Transfer. Specify the parameters (host name, port, user name, etc.) for the SFTP server. Specify the password that you received from the organization that hosts the SFTP server.
3. Add an "SFTP Task" on page 413 to a Managed File Transfer Project and choose the SFTP resource (created in step 2).
4. You will be able to send and receive files to/from that SFTP server by adding Put or Get elements to the SFTP task in the Project.

Quick Start – Using SFTP with both Public Key and Password Authentication

Follow these steps to exchange files with a SFTP server using both Public key and Password authentication.

1. Create and associate a Public and Private Key as outlined in the Using SFTP with Public Key Authentication section above.
2. Follow the steps in the Using SFTP with Password Authentication section.
3. When both portions are complete, you will be able to send and receive files to/from that SFTP server by adding Put or Get elements to the SFTP task in the Project.

SFTP (SSH File Transfer Protocol) - Standards

Listed below are the SFTP versions, standards, ciphers, algorithms and keys supported by Managed File Transfer.

SSH Version

- SSH 2.0

Ciphers (Symmetric Encryption Algorithms)

- Triple DES, key length of 192 bit
- Blowfish, key length up to 448 bit
- AES, key length up to 256 bit
- Poly1305, key length up to 256 bit

MAC algorithms

- MAC-SHA1, key length of 160 bit, digest length of 160 bit
- HMAC-SHA1-96, key length of 160 bit, digest length of 96 bit
- HMAC-MD5, key length of 128 bit, digest length of 128 bit
- HMAC-MD5-96, key length of 128 bit, digest length of 96 bit
- HMAC-SHA2-256, key length of 256 bit, digest length of 256 bit
- HMAC-SHA2-512, key length of 512 bit, digest length of 512 bit
- HMAC-SHA2-256-96, key length of 256 bit, digest length of 96 bit
- HMAC-SHA2-512-96, key length of 512 bit, digest length of 96 bit

Key Exchange algorithms

- Diffie-Hellman, MODP Groups 1, 2, 5 (1536-bit), 14 (2048-bit), 15 (3072-bit), 16 (4096-bit), 17 (6144-bit) and 18 (8192-bit), rsa, Curve25519(256 bit)

SSH Private Keys

- OpenSSH encoded keys
- PEM (privacy enhanced message) encoded keys

SSH Public Keys

- OpenSSH encoded keys

FTPS (FTP over SSL)

The traditional FTP protocol sends commands and data in “the clear” over the network/internet. This FTP data could be intercepted by an attacker, which could then be viewed and altered before sending it onto the receiver.

If you are sending sensitive data over the internet, then you may want to consider the FTPS (FTP over SSL) protocol for securing data.

FTPS creates an encrypted tunnel between two computer systems and will protect against the following attacks:

IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host

IP source routing, where a host can pretend that an IP packet comes from another, trusted host.

DNS spoofing, where an attacker forges name server records

Interception of cleartext passwords and other data by intermediate hosts

Manipulation of data by attackers in control of intermediate hosts

FTPS uses a combination of *asymmetric* (public key) cryptology and *symmetric* cryptology to provide strong encryption and optimal performance.

Both the server and the client can be authenticated (trusted) through the use of X.509 Certificates. In other words, certificates will help ensure that each party is truly who they say they are.

The SSL Handshake process is detailed in the Appendix.

Quick Start for FTPS

Based on if certificates are required for authentication, you can follow one of the “Quick Start” sections below to exchange data with a FTPS server.

Quick Start – When no Certificates are required for authentication

Follow the steps below if no certificates are required:

Add a "FTPS Servers Resource" on page 59 in Managed File Transfer. Specify the parameters (host name, port, user id, password, etc.) for the server. Do not specify any certificates for the resource. This will instruct Managed File Transfer to trust this FTPS server no matter what certificate is sent during the SSL handshake.

1. Add a "FTPS Task" on page 397 to a Managed File Transfer Project and choose the FTPS resource (created in step 1).
   You will be able to send and receive files to/from that FTPS server by adding Put or Get elements to the FTPS task in the Project.

Quick Start – When Certificates are required for authentication

Follow these steps if the FTPS server needs to authenticate your client certificate and/or if you need to authenticate the trading partner's certificate.

Follow these steps if your trading partner requires your public SSL certificate for authenticating your client:

Create a Certificate in the **Default Private Keys** key store.

If your trading partner requires that your certificate is signed by a third party (not self-signed), then follow the steps below:

Generate a Certificate Signing Request (CSR) and send it to an Issuer (your trading partner or a *Certificate Authority (CA)*).

After you receive the signed certificate (reply) from the Issuer, then import the reply into your **Default Private Keys** key store.

You must also import the certificate of the Issuer that signed your certificate into the Key Store.

If this is a certificate chain, where the certificate that signed your certificate was signed by another certificate and so on, then all certificates in the chain must be added to your Key Store.

If your certificate was not signed by a third party (self-signed), then Export your Certificate and send it to your trading partner.

Follow these steps if you want to use your trading partner's public certificate for authenticating their server:

If your trading partner's certificate was not signed by a third party (self-signed), then request the public certificate from your trading partner.

Import their public certificate into the Default Trusted Certificates Key Store.

If this is a certificate chain, where the certificate that signed your certificate was signed by another certificate and so on, then all certificates in the chain must be added to your Key Store.

1. Add a "FTPS Servers Resource" on page 59 in Managed File Transfer. Specify the parameters (host name, port, user id, password, certificates, etc.) for the connection.
2. Add a "FTPS Task" on page 397 to a Managed File Transfer Project and choose the FTPS resource (created in step 3).
3. You will be able to send and receive files to/from that FTPS server by adding Put or Get elements to the FTPS task in the Project.

FTPS (FTP over SSL) - Standards

Listed below are the FTPS versions, standards, algorithms and key store formats supported by Managed File Transfer.

SSL Versions - SSL 2.0 - SSL 3.0 (also known as TLS 1.0) Connection Types - Explicit SSL - Implicit SSL Explicit SSL Security Protocols - SSL - TLS Ciphers (Symmetric Encryption Algorithms) - AES-128 - AES-192 - AES-256 - DES - RC4 - Triple DES (DESede)	Authentication and Key Exchange Algorithms - Diffie-Hellman - DSA - RSA Hash Algorithms - MD5 - SHA1 Certificate Key Store formats - JKS (Java Key Store) - PKCS12

AS2 (S/MIME over HTTP(S))

Applicability Statement 2 (*AS2*) is a method used to securely send files over the Internet. The messages are built using the MIME format and sent over HTTP(S). AS2 messages can be compressed, signed, encrypted and then sent over an SSL tunnel; making AS2 a very secure option for transferring files. AS2 also implements *MDN* (receipts) to ensure the delivery of the message.

For more information on planning and defining an AS2 connection refer to the "Quick Start for AS2" on page 716 section.

Quick Start for AS2

AS2 uses SSL certificates and private keys for encrypting and signing messages over a HTTP(S) connection.

Initial Planning

Contact each of the trading partners with whom you will send AS2 messages:

- Obtain the URL of their AS2 server. If the URL begins with HTTPS and the server certificate used by the AS2 server is not signed by a trusted certificate authority, you will need to obtain and import their server certificate.
- Obtain their AS2 To ID.
- Provide them with your AS2 From ID.
- If you plan to encrypt the messages you send them, obtain and import their public certificate.

- If you plan to sign your messages, provide the trading partner with your public certificate that matches the private key used to sign messages. If you do not have a private key, follow the steps outlined in the Create an SSL Certificate section to create a private key and its associated public certificate.

Import the Trading Partner's Public Certificate(s)

Complete these steps if you plan to encrypt the message or use an HTTPS connection.

1. Log in to Managed File Transfer as an Admin User with the Key Manager role.
2. From the main menu, select the Encryption menu, and click the SSL Certificate Manager link.
3. Select the Default Trusted Certificates key store and click the **Open** button.
4. On the tool bar, click **Import Certificate**.
5. Browse for the location where the trading partner's public certificate was saved and click **Import**.
6. Specify an Alias to identify the certificate.
7. If the import was successful the recipient's public certificate will now reside in your Default Trusted Certificates Key Store.

Define the AS2 Server Resource

1. Log in to Managed File Transfer as an Admin User with the Resource Manager role.
2. On the main menu, click **Resources**.
3. In the Resources page, click the AS2 Server link in the Resource Type panel, and then in the page toolbar, click **Add AS2 Server**.
4. Specify the parameters and the credentials for the AS2 server obtained in the Initial Planning section above.

Define the AS2 Task

1. Login to Managed File Transfer as an Admin User with the Project Designer role.
2. On the main menu bar, click **Projects** and select the folder for the new Project.
3. In the page toolbar, click **Create a Project**, specify a Project Name, and then click **Save**.
4. From within the Project Designer page, expand the Web folder in the Component Library, and then drag the AS2 task to the Project Outline.
5. Within the AS2 Task page:
   a. Select the AS2 Server resource created above from the drop-down list.
   b. Type the path and file name of the Source File or click the icon to browse for the file. A "File Lists and File Sets" on page 116 can also be defined to send multiple files in one message.
   c. Optionally specify the Subject, Content Type and receipt options for this message.
   d. When complete, click the **Save** button.

Encrypting Messages

When sending a message to a trading partner it is highly recommended and sometimes required to encrypt the contents of a message. To add encryption, follow the steps below:

1. In the "AS2 Servers Resource" on page 72 set the **Encrypt Messages** option to Yes.

2. Specify the trading partner's public certificate in the Encryption Certificate Alias field. Type the alias name or click the  icon to browse for the certificate.

Signing Messages

Messages can be easily spoofed making them appear to be sent from someone you trust. Digital signatures added to an AS2 message allow the recipients to verify who you are. To add a digital signature to a message follow the steps below:

1. In the "AS2 Servers Resource" on page 72 set the **Sign Messages** option to Yes.
2. Specify your private key in the Signature Certificate Alias field. Type the alias name or click the  icon to browse for the key. In order for your trading partner to verify your signature, you will need to export and send them the public certificate associated to this private key.

Compressing Messages

Compressing messages reduces the message size and can improve transmission time. To add compression, follow the steps below:

1. In the "AS2 Servers Resource" on page 72 set the **Compress Messages** option to Yes.

Processing Return Receipts

The AS2 Task provides the option of receiving delivery confirmation in the form of a Receipt. If a Receipt is desired, use the Request Receipt drop-down list to select signed or unsigned receipts. Receipts that are signed ensure authenticity. Signed messages and receipts are considered a Non-Repudiation of Receipt (NRR), which is a "legal event" indicating that both party's identities and the message's integrity are valid.

When using receipts, an "AS2 Task Output" on page 124 variable can be defined and used elsewhere in the Project to control how other tasks function based on the receipt message or status. If a receipt is requested, the following Receipt Destinations or types are available:

Synchronous Receipt Types

In a synchronous scenario, the connection remains open between Managed File Transfer and the AS2 server until a receipt is received or a timeout occurs. The following options request synchronous receipts:

Job log

The receipt will be saved to the Project's Job Log.

File

The receipt will be written to a specified file.

Discard

The receipt will be processed and verified, but not stored.

Asynchronous Receipt Type

In an asynchronous scenario, the connection closes immediately after the transmission is complete. When the AS2 server is finished processing the message, the server will open a new connection and send the receipt. The following options request asynchronous receipts:

Email

The receipt is sent to the specified email address. Email receipts may be delayed and possibly not supported by the trading partner's AS2 server.

URL

The receipt will be sent to the specified URL.

Quick Start for Secure Email

Emails can use SSL certificates and private keys for encrypting and signing emails.

Encrypting an Email

Follow the steps below to encrypt an email:

1. Launch the SSL Certificate Manager by first logging in as an Admin User with a Key Manager role.
2. From the main menu bar, select **Encryption**, and then click the SSL Certificate Manager link.
3. Make sure the Default Trusted Certificates Key Store is selected and click the **Open** button.
4. Click the  Import Certificate link in the page toolbar.
5. Browse for the email recipient's public certificate on your local file system and click **Import**.
6. If the import was successful the recipient's public certificate will now reside in your Default Trusted Certificates Key Store.
7. Select **Workflows** from the main menu, click **Projects**, and then navigate to the folder where the new Project should go.
8. Click the  **Create a Project** button, specify a Project Name and click **Save**.
9. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Send Email task to the Project Outline.
10. Within the Send Email task page:
    a. Select the SMTP Server resource from the drop-down list.
    b. Specify a From address, Subject and Message.
    c. Specify a To address. The email address specified here will be used when performing an auto-lookup against the Default Trusted Certificate Key Store to find the recipient's public certificate. If a certificate is not found that contains that email address an error is displayed during execution. The auto-lookup feature will use the first certificate in the Key Store that matches that email address. If this is not desired, the a Trusted Key Alias can be specified on the Send Email task's sub-element, TO.
    d. Click the Encrypt tab and set the Encrypt Message attribute to true.
    e. Click the **Save** button.

Signing an Email

Email messages can be forged easily making them appear to be sent from someone you trust. Digital signatures can be added to an email to allow the recipients to verify you are who you say you are. To add a digital signature to an email follow the steps below:

1. If a Private Key already exists in the Default Private Keys Key Store skip to the next step. If not, follow the steps outlined in the Create an SSL Certificate section to create a Private Key.

2. Select **Workflows** from the main menu, click **Projects**, and then navigate to the folder where the new Project should go.
3. Click the **Create a Project** button, specify a Project Name and click **Save**.
4. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Send Email task to the Project Outline.
   Within the Send Email task page:
   a. Select the SMTP Server resource from the drop-down list.
   b. Specify a From address. The email address specified here will be used when performing an auto-lookup against the Default Private Keys Key Store to find the sender's private key. If a key is not found that contains that email address an error is displayed during execution. The auto-lookup feature will use the first key in the Key Store that matches that email address. If this is not desired, a Private Key Alias can be specified on the Send Email task's From sub-element.
   c. Specify a To address, Subject and Message.
   d. Click on the Advanced tab and set the Sign Message attribute to true.
   e. Click on the **Save** button.

Decrypting an Email

Follow the steps below to decrypt an S/MIME email:

1. When the sender encrypts the email they must use the public Certificate you provided them. The corresponding Private Key to that public Certificate must reside in the Default Private Keys Key Store in Managed File Transfer. If a Private Key already exists and the exchange of Certificates has already taken place skip to step 6. If not, continue on with step 2.
2. Create a Private Key by following the steps outline in the Create an SSL Certificate section. Make sure to place the Private Key in the Default Private Keys Key Store.
3. After a Private Key is generated select the checkbox next to the corresponding Key Alias and click the **Export** button.
4. From the Export Entry page select the Head Certificate item and click **Export**.
5. Send the Certificate to the sender that will be encrypting the emails.
6. Select **Workflows** from the main menu, click **Projects**, and then navigate to the folder where the new Project should go.
7. Click the **Create a Project** button, specify a Project Name and click **Save**.
8. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Retrieve Email task to the Project Outline.
   Within the Retrieve Email task page:
   a. Select the Mail Box resource from the drop-down list.
   b. Specify a Destination Directory. This directory will contain all attachments received. It is recommended to use a workspace so that each execution of the Project will have a clean working directory.

c. Click on the **Save** button.
When the Project is executed the messages will be retrieved from the "Mail Boxes Resource" on page 79 server. If the email message is encrypted using S/MIME, the Retrieve Email task will try to automatically decrypt it. The first step performed when decrypting is an auto-lookup against the Default Private Keys Key Store to find a Private Key that contains an email address that matches the recipients email address. If one does not exist an error is display to the page and recorded in the Job Log. The auto-lookup feature can be replaced by specifying a Private Key Alias on the Advanced tab of the Retrieve Email task.

Verifying an Email's Digital Signature

When retrieving email messages some may be digitally signed from the sender. In order for you to process these messages the sender's public certificate will need to imported into Managed File Transfer. Follow the steps below to encrypt an email:

1. Launch the SSL Certificate Manager by first logging in as a user with a Key Manager role.
2. From the Tools menu, click **SSL Certificate Manager** item from the main menu bar.
3. Make sure the Default Trusted Certificates Key Store is selected and click the **Open** button.
4. Click the Import Certificate menu option in the tool bar.
5. Browse for the sender's public certificate on your local file system and click **Import**.
6. If the import was successful the sender's public certificate will now reside in your Default Trusted Certificates Key Store.
7. Select **Workflows** from the main menu, click **Projects**, and then navigate to the folder where the new Project should go.
8. Click the **Create a Project** button, specify a Project Name and click **Save**.
9. From within the Project Designer page, expand the Email folder in the Component Library, and then drag the Retrieve Email task to the Project Outline.
10. Within the Retrieve Email task page:
    a. Select the Mail Box resource from the drop-down list.
    b. Specify a Destination Directory. This directory will contain all attachments received. It is recommended to use a workspace so that each execution of the Project will have a clean working directory.
    c. Click the **Save** button.
    When the Project is executed it will connect to the Mail Box specified and retrieve any messages waiting to be processed. If the messages contains a digital signature the signature will be verified against the Default Trusted Certificates Key Store. If the sender's certificate is not found then an error will be displayed indicating that the sender could not be verified.

    Note: After importing the sender's certificate review the certificate's Issuer. If the certificate was issued by a certificate that does not exist in the Default Trusted Certificates Key Store the signature verification will fail.

SSL Handshake Process

A SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client by using public-key techniques, and then allows the client

and the server to cooperate in the creation of symmetric keys used for encryption and decryption of the data. Optionally, the handshake also allows the client to authenticate itself to the server.

The following steps outline the handshake process:

1. The client sends the server its cipher settings (cryptographic algorithms and key sizes) and other information that the server needs to communicate with the client using SSL.
2. The server sends the client its cipher settings and other information. The server also sends its own certificate and may optionally request the client's certificate.
3. The client uses the certificate sent by the server to authenticate the server. If the server can be successfully authenticated, the client proceeds to step 4.
4. Using all data generated in the handshake thus far, the client will create a pre-master secret key for the session. The client encrypts with the server's public key (obtained from the server's certificate, sent in step 2), and then sends the encrypted pre-master secret key to the server.
5. If the server has requested client authentication, the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case, the client sends both the signed data and the client's own certificate to the server along with the encrypted pre-master secret key.
6. If the server has requested client authentication, the server attempts to authenticate the client. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret key, and then performs a series of steps (which the client also performs, starting from the same pre-master secret key) to generate the master secret key.
7. Both the client and the server use the master secret key to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity.
8. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.
9. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.
10. The SSL handshake is now complete and the session begins. The client and the server use the session keys to encrypt and decrypt the data they send to each other.

SSH Handshake Process

There are two layers involved in a SFTP connection: the **Transport layer** and **Authentication layer**. The Transport layer is used to establish the encryption algorithm and to create a secure connection between the Client and Server. The Authentication layer is used to determine whether the Client is authorized to connect to the Server.

Transport Layer

When the SFTP Client (the trading partner) first connects to Managed File Transfer (the Server), the encryption algorithm will be negotiated, along with various other connection parameters. Once the encryption algorithm is determined, then the following steps are performed:

1. The Server will send its public key to the Client.
2. The Client will generate a random session key and will encrypt it with the Server’s public key.

3. The Client will then send the encrypted session key to the SFTP server.
4. The Server will decrypt the session key with the Server's private key. From then on, all data will be encrypted with that session key.

Authentication Layer

After the Transport Layer is established, the Server will attempt to authenticate the Client. The Client can be authenticated using one of two options -- Public Key or Password.

Option 1: Public Key authentication

Before using Public Key authentication, a User on the Client system will need to generate a SSH Key pair (a private key and public key). The private key should be stored on the machine where the Client (such as Managed File Transfer) is located. The public key should be sent to the organization that hosts the Server.

The following steps are performed during the authentication layer of a SFTP connection:

1. The Server will encrypt a random number with the Client's public key and will send it to the Client.
2. The Client will use its private key to decrypt the random number. This decrypted number will then be sent back to the Server.
3. The Server will permit the connection with the Client if the random number is correct.
   Option 2: Password authentication

   The organization that hosts the Server will provide a password to the User at the Client system. This password will need to be specified when the Client makes a connection to the Server. The following steps will be performed during the authentication layer of the SFTP connection:
4. The Client will pass the password to the Server. This password is encrypted through the Transport Layer.
5. The Server will permit the connection with the Client if the password is correct.

Exchanging Data

After the encryption method is established (in the Transport Layer) and authentication is completed (in the Authentication Layer), then Client and the Server can begin to exchange data over the encrypted tunnel.

OpenPGP Key Manager

Managed File Transfer includes an integrated Key Manager for creating and managing public and private keys for OpenPGP. Projects can then utilize these keys to perform OpenPGP encryption, decryption, *signing* and *verification* processes.

A **Public Key** is used to encrypt information and to verify digital signatures. The owner's public key should be shared with its trading partners.

A **Private Key** is used by the owner to decrypt and to digitally sign files. The private key, typically protected by a password, should be kept secret by the owner and should NOT be shared with any one. Since a private key is mathematically related to its public key, the information encrypted with the public key can be decrypted by its corresponding private key.

A **Key Pair** is the combination of a private key and its corresponding public key.

A Key Ring (otherwise known as a key store) is a small binary file which can store one or more OpenPGP keys. Public keys are stored in **Public Key Rings** and private keys are stored in **Secret Key Rings**.

Default key rings are provided in Managed File Transfer. The location of the default public key ring file is **[installdirectory]/userdata/keys/pgp/pubring.pkr** and the location of the default secret key ring file is **[installdirectory]/userdata/keys/pgp/secring.skr** where [installdirectory] is the installation directory of the Managed File Transfer product.

For instance, you could store all of your trading partner's public keys in the pubring.pkr file and store your private key(s) in the secring.skr file.

When to Use Public and Private Keys

Several scenarios are listed below, each indicating the types of keys that will be needed by your organization and trading partners.

Requirement	What your organization needs	What your trading partner needs
Encrypt files, which will be sent to a trading partner	The trading partner's public key to encrypt the files	Their private key to decrypt the files
Encrypt and Sign files, which will be sent to a trading partner	• The trading partner's public key to encrypt the files • Your organization's private key to sign the files	• Their private key to decrypt the files • Your organization's public key to verify the files signatures
Decrypt files, which will be received from a trading partner	Your organization's private key to decrypt the files	Your organization's public key to encrypt the files
Decrypt and Verify the digital signatures of files, which files will be received from a trading partner	• Your organization's private key to decrypt the files • The trading partner's public key to verify the signatures on the files	• Your organization's public key to encrypt the files • Their private key to sign the files

Work with OpenPGP Keys

The **OpenPGP Key Manager** page opens the default public and secret key rings. This page lists all keys in the current key ring and allows you to create, import and export keys as well as create new key rings.

To work with OpenPGP keys, log in as an Admin User with the **Key Manager** role. From the Encryption menu, click **OpenPGP Key Manager**.

The following details are displayed for keys listed on the page:

- Key ID - The unique hexadecimal identifier for the key (generated by the product).
- User - The name and email address of the key's owner.
- Description - The type of key. A "Key Pair" is a combination of a public and private key.
- Key Type - The algorithm used to generate the key.
- Key Size - The size (in bits) of the key.
- Expiration Date - The date the OpenPGP key will expire.

Search an OpenPGP key by typing the key ID or user name in the Filter By field. The search string can contain a whole word, a partial word, or a phrase with uppercase and lowercase characters.

Page Toolbar

The following actions are available from the page toolbar:

- Add a new key pair by clicking the **New Key** button.
- Import a key by clicking the **Import Key(s)** button.
- Create a new key ring by clicking the **New Key Ring** button.
- Open a key ring by clicking the **Open Key Ring** button.
- Set preferences for the key ring that is currently open by clicking the **Preferences** button.

Open PGP Key Manager Actions

The following actions are available by selecting the Actions icon:

- "View an OpenPGP Key" on page 729 the details for a key by clicking the **View** button.
- "Change Passphrase" on page 728 for a private key by clicking the Change **Passphrase** button.

  - Delete a key by clicking the **Delete** button.
- "Export an OpenPGP Public Key" on page 727 by selecting the entry and clicking the **Export Public Key** button. This is needed if you need to share a public key with your trading partner.
- "Export an OpenPGP Key Pair" on page 728 by selecting the entries and clicking the **Export Key Pair** button. This will export both the public and private key, which is only needed if you need to share those keys with another key ring within your organization. The private keys should not be shared with a trading partner.

  Note: The secret key ring, private keys and passphrases should be kept confidential and should NOT be shared with trading partners. Only public keys should be shared.

Footer Actions

The following actions are available when you select one or more items from the table:

- Delete one or more selected key pairs.
- Export Public Keys. This is needed if you need to share a public key with your trading partner.
- Export Key pairs. This will export both the public and private key. This is only needed if you need to share the keys with another key ring in your organization. Do not share private keys with a trading partner.

Open an OpenPGP Key Ring

You can open key rings in Managed File Transfer by following the instructions below:

1. Log in as an Admin User with the **Key Manager** role.
2. From the main menu, select **Encryption**, and then click the OpenPGP Key Manager link.
3. Select the **Open Key Ring** link in the page toolbar and specify the location of the key rings to open.

Create an OpenPGP Key Ring

Create a new key ring in Managed File Transfer:

1. Log in as an Admin User with the **Key Manager** role.
2. From the main menu, select **Encryption**, and then click the OpenPGP Key Manager link.
3. Click the **New Key Ring** link in the page toolbar and specify the location and file name of the key rings to create.

Create OpenPGP Key

OpenPGP public and private keys are always created as a pair (Key Pair). You will need to generate a Key Pair for either of the following conditions:

If your trading partners need to send you encrypted files.

If the trading partners need to verify the digital signature on files which are sent from your organization.

Follow the instructions below to create a new Key Pair.

1. Log in as an Admin User with the **Key Manager** role.
2. From the main menu, select **Encryption**, and then click the OpenPGP Key Manager link.
3. Click the **New Key** link and define the values for the Key Pair.
4. Click the **Save** button to add the Key Pair.
   The private key portion will be placed in the secret key ring and the public key portion will be placed in the public key ring.

   After creating a Key Pair, the public key portion can then be "Export an OpenPGP Public Key" on page 727 and sent to your trading partners.

   Note: Typically the same public key can be shared with all of your trading partners. The secret key ring, private keys and passphrases should be kept confidential and should NOT be shared with trading partners.

Full Name

The full name of the entity (person or organization) who will be the owner of this key. This typically should be the name of your organization (for example, "ABC Company")

Email Address

The email address to associate with the key. This typically would either be your individual email address or a general email address for your organization (for example, "info@abccompany.com). It is not required to enter a real email address, however it would make it easier for trading partners to lookup your key using your email address.

Passphrase

The passphrase (password) to protect the Secret (Private) key portion of the Key Pair. This passphrase should be recorded in a safe place. You will not be able to decrypt files without supplying this passphrase. You should not share this passphrase with your trading partners.

Confirm Passphrase

Retype the passphrase to confirm.

Key Type

The algorithm to use to generate the key value. Valid values are *RSA* and *Diffie-Hellman/DSS*. It is generally recommended to use Diffie-Hellman/DSS unless your trading partner dictates otherwise.

Key Size

The length (in bits) of the key. Valid values are 512, 1024, 2048 or 4096 bits. Large key sizes will provide strong protection, but will slow the performance of encryption/decryption processes.

Expiration Date

The date when this key will expire. Leaving this field blank will create a key pair that will never expire.

Export an OpenPGP Public Key

After creating an OpenPGP Key Pair, you will need to share the public key portion with your trading partner(s). They can use that public key to encrypt files bound to your organization. Your trading partners can additionally use this public key to verify your *digital signature* on any signed files you send to them.

The public key will need to be exported from your Key Ring into a separate file, which you can then send to your trading partner(s) over FTP, email or other means.

Follow the steps below to export a public key from your Key Ring:

Log in as an Admin User with the **Key Manager** role.

From the main menu, select **Encryption**, and then click the OpenPGP Key Manager link.

Select the key to export by clicking the checkbox next to the entry.

Click the **Export Public Key(s)** button.

1. The Public Key will automatically download to your browser's default directory.
   After exporting the public key, you can send this exported file to your trading partner.

   Note: Generally the same public key can be shared with all of your trading partners. Since a public key can only be used to encrypt information (not decrypt), most organizations are not concerned who has possession of their public key.

Export an OpenPGP Key Pair

After creating an OpenPGP Key Pair, you can export both the public and private key, which is only needed if you need to share those keys with another key ring within your organization. The private keys should not be shared with a trading partner.

Follow the steps below to export a Key Pair from a Key Ring:

Log in as an Admin User with the **Key Manager** role.

From the main menu, select **Encryption**, and then click the OpenPGP Key Manager link.

Select the key to export by clicking the checkbox next to the entry.

Click the **Export Key Pairs** button.

1. The Key Pair will automatically download to your browser's default directory.

Import an OpenPGP Key

You will need your trading partner's public key for either of the following conditions:

If you need to send encrypted files to the trading partner.

If you need to verify the trading partner's digital signature on files which they send you.

The trading partner will send you their public key as a small binary file. The public key will need to be imported from this file into your public Key Ring.

After you receive the public key and save it to the hard disk, then follow the steps below to import the public key into your Key Ring:

Log in as an Admin User with the **Key Manager** role.

From the main menu, select **Encryption**, and then click the OpenPGP Key Manager link.

Click the **Import Key(s)** menu option in the tool bar.

Browse for the trading partner's public key on your hard disk and select it.

Click the **Import** button to import the public key from the specified file.

If the import is successful, the trading partner's public key will be loaded into your public key ring and will be listed on the page.

If you (or the trading partner) wants to verify the fingerprint of the key you imported, then click the icon next to the key. The fingerprint will be shown on the page, which you can read off to the trading partner (which is normally done over the phone).

Change Passphrase

An OpenPGP key passphrase can be changed using the **Change Passphrase** page. Log in as an Admin User with the **Key Manager** role and follow the instructions below to change the passphrase for an OpenPGP private key:

1. From the Encryption menu, click **OpenPGP Key Manager**.

2. Click the  icon next to the key to change.
3. Enter the current passphrase for the private key.
4. Enter the new passphrase and the confirmation passphrase.
5. Click the **Change** button when finished.
6. You will need to change any "Project Design" on page 100 (which use this OpenPGP key) to use the new passphrase.

View an OpenPGP Key

An OpenPGP key can be viewed using the **Key Details** page. Follow the instructions below to view the properties for an OpenPGP key:

1. Log in as an Admin User with the **Key Manager** role.
2. From the Encryption menu, click **OpenPGP Key Manager**.
3. Click the  icon next to the key to view.
4. This page will show the properties for the key, such as the key type, key size, when it was created, the *fingerprint* and preferences for the encryption, hash and compression algorithms.
5. Click the **Done** button when finished viewing the key details.

Change OpenPGP Key Preferences

The preferences can be changed for the OpenPGP Key Manager within Managed File Transfer. For instance, if you are using different key rings than those supplied by Managed File Transfer, then you can set their locations here as the defaults. Or you can indicate the preferred algorithms to store in any newly created keys.

Follow the steps below to change the preferences:

Log in as an Admin User with the **Key Manager** role.

From the Encryption menu, click **OpenPGP Key Manager** item from the main menu bar.

Click the  **Preferences** menu option in the tool bar.

If needed, specify the locations of the key rings to use as the default. These key rings will automatically be opened when launching the OpenPGP Key Manager.

If needed, select the algorithms and change their orders. These selected algorithms will be stored with any new public keys that are created. Generally you should not have to change these algorithms, unless your trading partner is using an older version of PGP software and it does not recognize your public key.

Click the **Save** button to apply any changes.

Note: It is recommended to keep AES128, AES192 and AES256 at the top of the list of selected encryption algorithms, as they are stronger than the other algorithms.

Default Public Key Ring

The location of the public key ring file that should be opened by default when launching the OpenPGP Key Manager. If a relative location is specified (without the proceeding slash), it will be relative to the Managed File Transfer installation directory.

Default Secret Key Ring

The location of the secret key ring file that should be opened by default when launching the OpenPGP Key Manager. If a relative location is specified (without the proceeding slash), it will be relative to the Managed File Transfer installation directory.

Preferred Encryption Algorithms

The preferred encryption algorithms to store in any newly created OpenPGP public keys. . It is recommended to keep the AES algorithms at the top of the list since they are stronger than the other algorithms.

Preferred Hash Algorithms

The preferred hash algorithms to store in any newly created OpenPGP public keys.

Preferred Compression Algorithms

The preferred compression algorithms to store in any newly created OpenPGP public keys.

SSL Certificate Manager Administration

SSL certificates (otherwise known as X.509 certificates) are digital identification documents that allow SSL-enabled servers (e.g. FTPS, HTTPS, etc.) and clients to authenticate each other. A certificate can be thought of as the digital equivalent of a passport.

A certificate will contain information about the entity (organization) which the certificate represents, including the following details:

- The name of the entity which signed/issued the certificate, otherwise known as the Issuer.
- The expiration date of the certificate.
- The *Public key* of the entity which the certificate represents.
-

The *digital signature* of the Issuer. This signature is created using the Issuer's *Private key* and ensures the validity of the certificate.

Issuing Entities

Your trading partner may require that you send them your certificate before allowing you to connect to their SSL-enabled server. Depending on your trading partner's authentication requirements, there are three different approaches in which a certificate can be signed and issued:

You can issue your own certificate. Also known as a Self-Signed certificate. This is the lowest level of trust.

Your trading partner can issue your certificate.

A Certificate Authority (CA) can issue your certificate. This is the highest level of trust.

A certificate authority (CA) is a trusted organization that issues Public key certificates. The job of a CA is very similar to that of a notary public. You must provide proof identity to the CA in order to obtain a certificate from the CA. Once the CA is confident that you represent the organization that you say you represent, then the CA will sign the certificate attesting to the validity of the information contained within the certificate. A CA will generally charge a fee for this service. Examples of popular CA's are VeriSign™, Entrust™ and Equifax™.

Certificate Chains

Multiple certificates can be linked in a certificate chain. When a certificate chain is used, the first certificate is always that of the sender. The next is the certificate of the entity that issued the sender's certificate. If there are more certificates in the chain, each is that of the authority that issued the previous certificate. The final certificate in the chain is the certificate for a root CA. A root CA is a public certificate authority that is widely trusted (such as VeriSign).

Certificate Key Stores

Certificates must be stored in a Key Store before they can be used in an application such as Managed File Transfer. A Key Store is a binary file that can contain both certificates and Private keys. Typically you will have a Key Store to hold your own client certificate(s) and Private keys, and have a separate Key Store to hold the certificates for the servers that you trust.

Open SSL Key Store

To open a SSL Key Store, log in as an Admin User with the **Key Manager** role.

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. From the Certificate Manager toolbar, click the **Open Key Store** button.

Available Options

- "Create SSL Key Store" on page 739 a New Key Store by clicking the **New Key Store** link in the page toolbar.
- "Change Key Store Preferences" on page 740 Preferences for the Key Store by clicking the Preferences link in the page toolbar.

Default Trusted Certificate

A Certificate that was imported from a trusted trading partner or *Certificate Authority*.

Alternatively, select a store from the list to open and then click the **Open** button:

Default Private Keys

A combination of a Private key and Certificate most likely generated within your organization.

Other

A user defined SSL instance.

After choosing the Key Store to open, the "SSL Certificate Manager" on page 732 page will list any Certificates/keys contained in the Key Store.

Note: If browsing for a Key Store location, verify your Web browser allows pop-ups. The Key Selection page opens in a pop-up window.

SSL Certificate Manager

To administer SSL Certificates in the SSL Key Store:

1. Log in as an Admin User with the **Key Manager** role.
2. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.

   Note: Many more SSL Certificates are available than shown here. An SSL Certificate shown in red indicates it is expired.

SSL Certificate Manager Actions

The following actions are available from the SSL certificate Manager homepage

- "Create SSL Certificate" on page 734 a new Certificate by clicking the **New**button and then click **New Certificate**. It is recommended to create any new Certificates in the privateKeys Key Store (not the trustedCertificates Key Store).
- "Import SSL Certificate" on page 737 a Trusted Certificate by clicking the **Import** button and then click **Certificate(s)**. It is recommended to import trusted certificates in the trustedCertificates Key Store (not the privateKeys Key Store).
- "Import SSL Private Key" on page 738 a Private Key by clicking the **Import** button and then click **Private Key**. It is recommended to import Private Keys in the privateKeys Key Store (not the trustedCertificates Key Store).
- "Create SSL Key Store" on page 739 a New Key Store by clicking the **New** button and then clicking Key Store
- "Open SSL Key Store" on page 731 a Key Store by clicking the Open Key Store link in the toolbar.
- "Change Key Store Password" on page 740 the Password for a Key Store by clicking the **Change Password** button.
- "Change Key Store Preferences" on page 740 the Preferences for the Key Manager by clicking the **Preferences** button.
- Refresh the Certificate Manager list by clicking the **Refresh** button.
- Search SSL certificates by typing the alias, subject, or the issuer in the **Filter By** field. The search string can contain a whole word, a partial word, or a phrase with uppercase and lowercase characters.

Certificate Manager Actions

The following actions are available by selecting the Actions icon:

- "View SSL Certificate/Private Key" on page 738 the details for a Certificate and/or Private Key by clicking the icon.
- "Export SSL Certificates and Private Keys" on page 737 a certificate by selecting the entry and clicking the **Export** button. This is used only in a special circumstance if you need to share the public certificate with a trading partner.
  - Change the Alias (name) of a certificate by clicking the icon. Specify the new Alias name and click the **Rename** button.
  - Delete a Certificate by clicking the icon.
- "Generate CSR (Certificate Signing Request)" on page 736 (Certificate Signing Request) by the **Generate CSR** button. This is used if you need to have a *Certificate Authority (CA)* sign the certificate.
- "Import CA Reply" on page 737 a reply from a Certificate Authority by clicking the **Import CA Reply** button.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Certificates.

Manage SSL Private Keys

To administer SSL Private Keys in the SSL Key Store:

1. Log in as an Admin User with the **Key Manager** role.
2. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
3. Select the Default Private Keys Key Store, and then click the **Open** button.

   Note: An SSL Key shown in red indicates it is expired.

Page Toolbar

The following actions are available from the page toolbar:

- "Create SSL Certificate" on page 734 a new Certificate by clicking the **New** button and then click **Certificate**.
- "Import SSL Certificate" on page 737 a Certificate by clicking the **Import**button and then click **Certificate**. It is recommended to import trusted certificates in the trustedCertificates Key Store (not the privateKeys Key Store).
- "Import SSL Private Key" on page 738 a Private Key by clicking the **Import** button and then click **Private Key**. It is recommended to import Private Keys in the privateKeys Key Store (not the trustedCertificates Key Store).
- "Create SSL Key Store" on page 739 a New Key Store by clicking the **New** lbutton and then click **Key Store**.
- "Open SSL Key Store" on page 731 a Key Store by clicking the Open Key Store link in the toolbar.

- "Change Key Store Password" on page 740 the Password for a Key Store by clicking the **Change Password** button.
- "Change Key Store Preferences" on page 740 the Preferences for the Key Manager by clicking the **Preferences** button.
  - Refresh the Certificate Manager list by clicking the **Refresh** button.

Certificate Manager Actions

The following actions are available by selecting the Actions icon:

- "View SSL Certificate/Private Key" on page 738 the details for a Certificate and/or Private Key by clicking the icon.
- "Export SSL Certificates and Private Keys" on page 737 a certificate by selecting the entry and clicking the **Export** button. This is used only in a special circumstance if you need to share the public certificate with a trading partner.
  - Change the Alias (name) of a certificate by clicking the icon. Specify the new Alias name and click the **Rename** button.
  - Delete a Certificate by clicking the icon.
- "Generate CSR (Certificate Signing Request)" on page 736 (Certificate Signing Request) by the **Generate CSR** button. This is used if you need to have a *Certificate Authority (CA)* sign the certificate.
- "Import CA Reply" on page 737 a reply from a Certificate Authority by clicking the **Import CA Reply** button.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected Certificates.

Create SSL Certificate

Follow the instructions below to create a new SSL Certificate:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. Select the **Open Key Store** button and select a Key Store. Certificates are commonly created in the Default Private Keys Store.
3. In the **Certificate Manager** page, click the **New** link in the page toolbar and then click **Certificate**.
4. On the **Create SSL Certificate** page, complete the requested information.
5. When complete, click the **Save** button to create the Certificate.
6. After the Certificate is created, perform one of the following:
   - If your trading partner(s) will accept a "self-signed" Certificate, it can be "Export SSL Certificates and Private Keys" on page 737 and sent to your trading partner(s).
   - If your trading partner(s) requires a signed Certificate by a *Certificate Authority (CA)*, then you need to generate a "Generate CSR (Certificate Signing Request)" on page 736 (CSR).

Key Type

The algorithm to use to generate the key value for the Certificate. Valid values are *RSA* and *DSA*. It is generally recommended to use RSA unless your trading partner dictates otherwise.

Key Size

The length (in bits) of the key. Valid values are 1024, 2048 or 4096 bits. In most cases a 1024 bit key size is sufficient. Larger key sizes will provide strong protection, but will slow the performance of encryption/ decryption processes.

Signature Algorithm

The algorithm to use for *signing* the *Public key* portion of the certificate. **SHA1withRSA** is recommended in most cases, unless your trading partner dictates otherwise.

Select one of the following values:

- SHA1withRSA
- SHA224withRSA
- SHA256withRSA
- SHA384withRSA
- SHA512withRSA
- MD2withRSA
- MD5withRSA
- RIPEMD128withRSA
- RIPEMD160withRSA
- RIPEMD256withRSA

Alias

A unique name to assign the Certificate (for example, "Infa_certificate_for_FTPS transfers"). This name will help you and your trading partners to quickly identify the Certificate within a Key Store. It is not recommended to use spaces in the Alias. Instead, an underscore can be used to separate words.

Common Name

A unique name that your trading partner's SSL-enabled server could use to help verify your identity. The Common Name should typically be a value that another organization would most likely not use. It is recommended to use your organization's URL (e.g. "www.yourcompanyname.com") as the Common Name since that is unique to your organization. It is not recommended to use spaces in the Common Name.

Organization Unit

The department name (for example, "IS Department") or branch name (for example, "Orlando office") in your organization that would use this Certificate. This information will be stored in the Certificate for identification purposes.

Organization

The name of your organization, which will be stored in the Certificate for identification purposes.

Locality

The city or town (for example, "Omaha") in which your organization is located, which will be stored in the Certificate for identification purposes.

State

The state or province (for example, "Nebraska") in which your organization is located. It is recommended that you do not use abbreviations for the state or province. Instead, spell the complete name. This information will be stored in the Certificate for identification purposes.

Country

The country (for example, "United States") in which your organization is located. It is recommended that you do not use abbreviations for the country. Instead, spell the complete name. This information will be stored in the Certificate for identification purposes.

Email Address

Your email address or general email address of your organization, which will be stored in the Certificate for identification purposes.

Expiration Date

The date on which the Certificate will expire. If the date is not overridden, the default expiration date will be three (3) years from the creation date.

Generate CSR (Certificate Signing Request)

The Generate CSR function allows you to create a signing request for your Certificate, that you will send to a *Certificate Authority (CA)* for signing. This function is needed if your trading partner(s) require your Certificates to be signed by a CA (not self-signed). Signed Certificates are also required for HTTPS web sites.

Follow the instructions below to generate a CSR:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. Select the  **Open Key Store** button and choose a Key Store. Certificates are commonly created in the Default Private Keys Store.
3. In the **Certificate Manager** page, select the  icon for the Certificate and then click the  Generate CSR button. If no Certificates exist, "Create SSL Certificate" on page 734 a SSL Certificate.
4. Using the File Download box, save the file on your local computer. The file name is constructed by the system using the Certificate's Alias with a .csr extension.
5. Send this file to a Certificate Authority (CA) for signing.
   The Certificate Authority (CA) will review your CSR and return a reply. The reply will contain the *digital signature* of the CA. This reply can be imported using the "Import CA Reply" on page 737 function.

Import CA Reply

This function allows you to import a Reply (signed certificate) from a *Certificate Authority (CA)*. This Reply is in response to a "Generate CSR (Certificate Signing Request)" on page 736 (Certificate Signing Request) that you generated earlier. If the CSR was approved, the Reply will contain the *digital certificate* of the CA.

Follow the instructions below to import a CA Reply:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. Select the **Open Key Store** button and choose a Key Store.
3. In the **Certificate Manager** page, select the icon for the Certificate and then click the **Import CA Reply** button.
4. On the **Import CA Reply** page, click to select the location where the CA Reply file is located.
5. In the Input File box, type the location for the file or click the **Browse** button to browse for the file.
6. Click the **Import** button to import the Reply.

   Note: If the Reply contains an approval from the CA, then your Certificate will be signed with the digital signature of the CA. You can verify this signature by viewing the details for your Certificate (click the icon next to the Certificate).

Export SSL Certificates and Private Keys

Follow the instructions below to export an SSL Certificate or Private Key:

1. Log in as an Admin User with a Key Manager role.
2. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
3. Click the **Open Key Store** button and choose the Key Store that contains the Certificate to export. You will most likely want to export Certificates from the Default Private Keys Key Store, since that is typically where your organization's Certificates should be stored.
4. In the **Certificate Manager** page, select the icon for the Certificate and then click the **Export...** button.
5. In the Export Entry box, select the export type:

   1. When complete, click the **Export** button.
   2. Follow the prompts to save the exported file to the local hard drive.
   3. The name of the file will be constructed using the Certificate's Alias with the appropriate extension.

Import SSL Certificate

Managed File Transfer supports importing DER or PEM encoded certificates and files that contain multiple certificates. When a file contains multiple certificates (not a private key or CA reply), each certificate is imported individually. The alias name for the second and subsequent certificates will be appended with a sequential number. Import certificate(s) by following the steps below:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. Click the **Open Key Store** button and choose the Key Store to open.

3. In the **Certificate Manager** page, click the **Import** link in the toolbar and then click  **Certificate**.
4. On the **Import Certificate** page, click to select the location where the certificate file is located.
5. In the Input File box, type the location for the file or click the **Browse** button to browse for the file.
6. Type an alias name to assign to the certificate. The name must not already exist in the Key Store.
7. Click the  **Import** button to import the certificate.
   If the import is successful, the certificate will load into the Key Store and will be listed on the page.

   Note: If you (or the trading partner) want to verify the fingerprint of the Certificate you imported, click the  icon next to the Certificate. The fingerprint will be displayed on the page. You can read the certificate to the trading partner (normally done over the phone).

Import SSL Private Key

SSL Private Keys can be imported into the Private Key Store to provide secure authentication with the servers used by trading partners or within an organization.

Import From

The Private Key can be imported either from a file on the end user's PC or from a file on the Managed File Transfer server.

Input File

The Input file is the file containing the SSL Private Key. Click the **Browse** button to navigate to the file.

Password

The Password field is used for opening the imported key file. It is the password that was used to encrypt the file when it was "Export SSL Certificates and Private Keys" on page 737. The password is used to decrypt the private key information in the file.

Alias

The Alias name is used to identify the private key after a successful import.

Format

The format of the private key being imported. The available options are PKCS12 and PEM formats. A PEM formatted file may only contain one private key entry and an error occurs if it contains more than one private key. If a PKCS12 formatted file contains more than one private key, everything after the first key is ignored.

Note: After the private key is imported to the current key store, its password will be set to the password of the key store if the current key store is a JKS type key store.

View SSL Certificate/Private Key

Follow the instructions below to view the properties for a SSL Certificate/Private Key:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.

2. Select the **Open Key Store** button and choose a Key Store to open.
3. In the **Certificate Manager** page, select the Action icon for the Certificate and then click the View icon to view the certificate.
4. The View Certificate page displays information about the Certificate/Private Key such as the type, size, expiration date, signature algorithm, fingerprint values, to whom the Certificate/Private Key is issued, and who issued it.
5. Click the **Done** button when finished viewing the details.

Create SSL Key Store

Follow the steps below to create a new Key Store for containing SSL Certificates:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. In the **Certificate Manager** page, click the **New** link in the toolbar and then click **Key Store**.
3. Type the requested information in the appropriate boxes.
4. Click the **Save** button to create the Key Store.

Key Store Type

From the drop-down menu, click to select the Key Store Type. Managed File Transfer supports both *JKS* and *PKCS12* Key Store types.

Key Store Location

The path and file name to contain this Key Store. A file extension of ".jks" is recommended for JKS type Key Stores and ".p12" is recommended for PKCS12 type Key Stores. If you do not have a preference, it is recommended to create Key Stores in the **[installdirectory]/userdata/keys/x509/** folder, where [installdirectory] is the installation directory of Managed File Transfer.

Password

Type the password to protect the Key Store. This password should be recorded in a safe place. You will not be able to open the Key Store without supplying this password. You should not share this password with your trading partners.

Confirm Password

Re-enter the password to confirm.

Provider

The *JCE Service Provider* is used to create this Key Store. It is recommended to use the **Auto Detect** option unless problems are encountered when attempting to create the Key Store. If you need specify a provider, from the drop-down list select the appropriate option:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM

- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509
- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM
- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509

Change Key Store Password

Follow the steps below to change an SSL Key Store password:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. Click the  **Open Key Store** button and choose the Key Store to open.
3. In the **Manage SSL Key Store** page, click the  **Change Password** link in the toolbar.
4. On the **Change Key Store Password** page:
   a. Specify the current password for the Key Store. If working with one of the default Key Stores provided in Managed File Transfer, the default password is **default**.
   b. Specify the new password for the Key Store and type it again in the confirmation field.
   c. If changing the password for a default Key Store, indicate if you would like to automatically change the Key Store "Change Key Store Preferences" on page 740 to use this new password. Otherwise, you will need to manually change these preferences later.
5. Click the **Change** button to apply the new password.

   Note: The new password should be recorded in accordance with the IT Security Policy of your company. You will not be able to open the Key Store without supplying this password. The passwords for Key Stores should be kept confidential and should NOT be shared with trading partners.

Change Key Store Preferences

The preferences allow you to specify the locations, passwords and properties of the default Key Stores containing the Trusted Certificates and Private Keys/Certificates. This option simplifies working with Key Stores as you will not continually need to specify their locations/passwords when performing key management functions.

Note: Only change the preferences if you change passwords on the Key Stores or if you do not want to use the default Key Stores provided in Managed File Transfer.

Follow the steps below to view and/or change the SSL Certificate preferences:

1. From the main menu, select **Encryption**, and then click the **SSL Certificate Manager** link.
2. On the Certificate Manager page, click the  Preferences link in the toolbar.
3. Make any needed changes to the preferences.
4. Click the **Save** button to save the Preferences.

Key Store Location

The location of the default Key Store that contains trusted SSL certificates. If a relative location is specified (without the proceeding slash), it will be relative to the Managed File Transfer installation directory.

Key Store Type

The type of this Key Store. Managed File Transfer supports both *JKS* and *PKCS12* Key Store types.

Key Store Password

The password for accessing this Key Store.

Provider

The *JCE Service Provider* to use for opening this Key Store. It is recommended to use the **Auto Detect** option unless problems are encountered when attempting to open the Key Store.

Note: The location of the default Key Store (shipped with Managed File Transfer) for holding Private Keys/ Certificates is **[installdirectory]/userdata/keys/x509/privateKeys.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

The location of the default Key Store (shipped with Managed File Transfer) for holding Trusted Certificates is **[installdirectory]/userdata/keys/x509/trustedCertificates.jks** where [installdirectory] is the installation directory of the Managed File Transfer product.

Default Private Keys

A combination of a Private key and Certificate most likely generated within your organization.

SSH Key Manager

Informatica Managed File Transfer includes an integrated Key Manager for creating SSH public and private keys that can be used for authenticating SFTP connections.

To administer SSH keys, log in as an Admin User with the **Key Manager** role.

From the main menu, select **Encryption**, and then click the SSH Key Manager link.

Page Toolbar

The following actions are available from the page toolbar:

- "Create SSH Key Pair" on page 742 a new SSH Key Pair by clicking the **New Key** button.
  - Import a "Import Public SSH Key" on page 743 or "Import Private SSH Key" on page 743 Key by clicking the **Import** button.
  - Open a "Open Public SSH Key" on page 744 or "Open Private SSH Key" on page 744 Key file by clicking the **External Key Files** button.

SSH Key Manager Actions

The following actions are available by selecting the Actions icon:

- Rename an SSH key by clicking the icon.
- Delete an SSH key by clicking the icon.
- Export a public or private SSH key by clicking the **Export** button. Public keys can be exported in OpenSSH or Secure Shell formats.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected SSH Keys.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.
- Click the **Columns** button to select the SSH Key properties that are displayed in the table.

Create SSH Key Pair

When you create an SSH key pair, a private key and a public key are generated and stored in the SSH Key Manager. Private keys can be used in the SFTP service configuration whereas public keys are used for Web User authentication.

Follow the instructions below to create a new SSH key:

1. Log in as an Admin User with the **Key Manager** role.
2. From the main menu, select **Encryption**, and then click the SSH Key Manager link.
3. On the SSH Key Manager page, click the **New Key** link in the toolbar.
4. Complete the required field values for the SSH key pair.
5. Click the **Save** button to create the SSH key pair.

Name

The name identifies the key on the SSH Key Manager page. The maximum length of the name is 64 characters.

Key Type

The algorithm to use when generating the key. Valid values are *RSA* and *DSA*. It is generally recommended to use RSA.

Key Size

The length (in bits) of the key. Valid values are 512, 1024, 2048 or 4096 bits. Large key sizes will provide strong protection, but will slow the performance of encryption/decryption processes.

Passphrase

This is the password that protects the private key portion of the SSH Key Pair and should be recorded in a safe place.

Confirm Passphrase

Retype the passphrase to confirm.

Comment

A description to store with the key. This typically should contain the name of your organization (for example, "ABC Company SSH Key"), which will allow others to quickly identify the key.

Public Key File Format

The format in which to store the public key. Valid values are OpenSSH or SecureShell. It is generally recommended to use OpenSSH unless your trading partner dictates otherwise.

Note: Private Keys and passphrases should be kept confidential and should NOT be shared with trading partners.

Import Public SSH Key

You can import the SSH keys in OpenSSH or SecureShell format into Managed File Transfer.

Follow the steps below to import a public SSH key:

1. From the main menu, select **Encryption**, and then click the SSH Key Manager link.
2. In the **SSH Key Manager** page, click the **Import** drop-down, and then click **Public Key**.
3. Type the name of the key file in the Input File box or click the icon to browse for an SSH public key.
4. Provide a name to identify the SSH key in the SSH Key Manager.
5. Click the **Import** button to import the SSH public key.

Import Private SSH Key

Follow the steps below to import a private SSH key:

1. From the main menu, select **Encryption**, and then click the SSH Key Manager link.
2. In the **SSH Key Manager** page, click the **Import** drop-down and then click **Private Key**.
3. Type the name of the key file in the Input File box or click the icon to browse for a private SSH Key.
4. Provide a name to identify the SSH key in the SSH Key Manager and specify a password.
5. Click the **Import** button to import the SSH private key.

Open Public SSH Key

Follow the instructions below to work with a public SSH key file that is not installed in the Managed File Transfer key manager:

1. From the main menu, select **Encryption**, and then click the SSH Key Manager link.
2. In the **SSH Key Manager** page, click the **External Key Files** drop-down and then click **Open Public Key File**.
3. Type the name of the public key file in the Public Key File box or click the icon to browse for a public SSH key. If browsing for a public key file, verify your Web browser allows pop-ups. The key selection page opens in a pop-up window.
4. Click the **Open** button to open the public SSH key.
5. The public SSH key opens and is displayed on the page.
6. Click the corresponding **Download** button to save the public key on your local computer.

Open Private SSH Key

Follow the instructions below to work with a private SSH key that is not installed in the Managed File Transfer key manager:

1. From the main menu, select **Encryption**, and then click the SSH Key Manager link.
2. In the **SSH Key Manager** page, click the **External Key Files** drop-down and then click **Open Private Key File**.
3. Type the name of the key file in the Private Key File box or click the icon to browse for a private SSH key. If browsing for a key file, verify your Web browser allows pop-ups. The key selection page opens in a pop-up window.
4. In the Passphrase box, type the passphrase for the selected private SSH key.
5. Click the **Open** button to open the private SSH key.
6. The private SSH key opens and is displayed on the page.
7. Click the **Download** button to save the private key on your local computer.

Encrypted Folders

The Encrypted Folders page allows authorized users to create and manage encrypted folders for use within Managed File Transfer. Encrypted folders ensure your data is kept safe from unauthorized access outside of the Managed File Transfer product. Files added to an encrypted folder will have AES 256-bit encryption applied automatically. Files downloaded from an encrypted folder will be decrypted automatically. The encryption and decryption will be performed on all subfolders within the encrypted folder.

The files in the encrypted folder can be accessed through the HTTPS, FTP, FTPS, SFTP, and AS2 services from an authorized Web User, through a Project, Trigger, and the File Manager.

Managed File Transfer supports encrypted local folders and network folders using native operating system's mounting/mapping capabilities or the Network Shares Resource functionality provided in Managed File Transfer.

Accessing the files in the encrypted folder outside of Managed File Transfer (for example, Windows Explorer) will not encrypt or decrypt the data. Therefore, the files in an encrypted folder should only be accessed from Managed File Transfer.

Managed File Transfer does not support the ability to append data to a file once it has been added to an encrypted folder, or resume a file upload to an encrypted folder if the file upload was paused or interrupted.

Folder Restrictions

To prevent encryption of vital Managed File Transfer system resources, Managed File Transfer has restrictions on which folders can be encrypted:

- You cannot encrypt a root drive. For example, you would not be able to encrypt C:\.
- You cannot encrypt the Managed File Transfer install directory, or any parent directory of the install directory.
- The only directory within the Managed File Transfer install directory where encryption is allowed is the default "Global Settings" on page 752 [INSTALL_DIR]/userdata/webdocs.
- You cannot encrypt a child folder of a directory that is already encrypted.
- You cannot encrypt a parent folder of a directory that contains an encrypted child directory.

Encrypted Folder Management

To manage encrypted folders, log in as an Admin User with the **Product Administrator** role.

From the main menu, select **Encryption**, and then click the Encrypted Folders link.

Encrypted Folder Options

- "Add Folder" on page 745 a new encrypted folder by clicking the  Add Folder link in the page toolbar.
- "View Encrypted Folder" on page 747 the encrypted folder details by clicking the  View Folder link in the Actions column.
- "Remove Folder" on page 746 encryption on an existing encrypted folder by clicking the remove folder button in the Actions column.

Add Folder

The Encrypt Folder wizard guides you through the folder activation process.

Encrypt Folder - Step 1

Select the folder path to the target folder using the  button and then click **Next**.

Encrypt Folder - Step 2

To create a new encrypted folder, choose Random to create an Encryption Key and Seed UUID, and then click **Next**.

To provide access to an encrypted folder that is managed by another Managed File Transfer installation, choose Manual, and then enter the Encryption Key and Seed UUID from the other "View Encrypted Folder" on page 747. If the existing folder contains encrypted content, uncheck the Encrypt Contents checkbox. Then click **Next**.

Note: In a "Clustering" on page 772 environment, each Managed File Transfer server automatically shares the Encryption Key and Seed UUID, which allows each server to have access to the encrypted folder.

Encrypt Folder - Step 3

If the selected folder is empty, click the **Activate** button to encrypt the folder.

If the selected folder contains files or sub-folders, you will want to consider the following points before proceeding:

- Create a backup of the folder before you start encryption. It is strongly recommended you use the optional backup folder option to backup the selected folder before it is encrypted.
- If existing Web Users have access to the target folder, stop all services (HTTPS, FTP, FTPS, SFTP, and AS2) before continuing. The folder and files will become unavailable during the encryption process.
- The 'Created On' timestamp property for existing files in the target folder will be updated to the current system date/time during encryption. However, the last modified date will not be changed.
- The ownership of any existing files in the target folder will be changed to the user profile that started the Managed File Transfer application.

1. Ensure the **Create a Backup of the Folder** option is checked.
2. The Backup Location field is automatically populated with a backup directory. You can specify a different location by using the  button.
3. The **Backup Compression** option is set to ZIP by default. Choose NONE if you do not want to compress your backup.
4. Click Next to continue.

Encrypt Folder - Step 4

If the selected folder contains files and sub-folders, review and confirm your configuration. Click the **Activate** button to encrypt the folder.

The Folder Activation Progress window appears. The length of time to encrypt a folder will vary depending on the size of the folder. Click Done when the encryption is finished.

Remove Folder

The Remove Folder wizard allows you to remove encryption from a folder encrypted by Managed File Transfer. All files located in the specified folder will be decrypted during the deactivation process.

Decrypt Folder - Step 1

If the selected encrypted folder is empty, click the **Deactivate** button to decrypt the folder.

If the selected encrypted folder contains files or sub-folders, you have the option to decrypt the contents when deactivating the folder. Click Next.

Decrypt Folder - Step 2

If the selected encrypted folder contains files or sub-folders, you will want to consider the following points before proceeding:

- Create a backup of the encrypted folder before you start decryption. It is strongly recommended you use the optional backup folder option to backup the selected folder before it is decrypted.
- The backup directory will contain a .ga_keyfile. This file contains the encrypted key used for the folder encryption, and is stored in the backup directory to aid in data recovery.
- If existing Web Users have access to the encrypted folder, stop all services (HTTPS, FTP, FTPS, SFTP, and AS2) before continuing. The encrypted folder and files will become unavailable during the decryption process.
- The 'Created On' timestamp property for existing files in the encrypted folder will be updated to the current system date/time during encryption. However, the last modified date will not be changed.
- The ownership of any existing files in the decrypted folder will be changed to the user profile that started the Managed File Transfer application.

1. Enable the **Create a Backup of the Folder** option.
2. The Backup Location field will automatically populate with a backup directory. You can specify a different location by using the  button.
3. The **Backup Compression** option is set to ZIP by default. Choose NONE if you do not want to compress your backup.
4. Click Next to continue.

Decrypt Folder - Step 3

If the selected encrypted folder contains files and sub-folders, review and confirm your configuration. Click the **Deactivate** button to decrypt the folder.

The Folder Deactivation Progress window appears. The length of time to decrypt a folder will vary depending on the size of the folder. Click Done when the decryption is finished.

View Encrypted Folder

The View Encrypted Folder page allows you to view the properties of encrypted folders.

1. To access the View Encrypted Folder page, log in as an Admin User with the Product Administrator role.
2. From the main menu, select **Encryption**, and then click the Encrypted Folders link.
3. View the encrypted folder details by clicking the  View Folder link in the Actions column.
   The following fields are displayed on the View Encrypted Folder page:

Folder Path

The folder path to the encrypted folder.

Encryption Key

The encryption key used to encrypt and decrypt data.

Seed UUID

The unique ID used as the seed during encryption and decryption operations.

Activated By

The Managed File Transfer' User who activated the encrypted folder.

Activated On

The date the encrypted folder was activated.

Encryption Tool

The Encryption Tool provides a method to encrypt a phrase that can then be used in a variable to pass to a *Project*.

To access the Encryption Tool, log in as an Admin User with Project Designer or Resource Manager role.

Input

Type the plain text that should be encrypted and click the **Encrypt** button.

Encrypted Password

The encrypted value is available in this box after the input is encrypted.

Encryption Tool using Command Line Utility

Use the password encryption script to encrypt a Managed File Transfer password.

Run the password encryption utility and enter the password in the following syntax:

- On Windows operating systems: `MFT_HOME/server/mft-tools/mftpasswd.bat -c <command> [--configFile <configFile>] [-dp <decryptionPassword>] [-ep<encryptionPassword>] [-es <encryptString>] [-l <"url">] [-p <password>] [-pj <jdbcPassword>]<encryptionPassword>] [-es <encryptString>] [-l <"url">] [-p <password>] [-pj <jdbcPassword>][-u <loginName>] [-uj <username>]`
- On UNIX operating systems: `MFT_HOME/server/mft-tools/mftpasswd.sh -c<encrypt> -es<string to encrypt>`

The following table describes the repository utility options and arguments:

Options	Argument	Required	Description
- c, --command	command	Yes	Command to run encryption. Enter one of the following commands: - encrypt. encrypts a password using the default Informatica secret key and a custom secret key. - reEncrypt. Re-encrypt all passwords configured in Resources and Projects.
-l, --url	"url"	-	JDBC URL for the repository or the operational data store. You must enclose the URL in quotation marks. For example: `... -l "jdbc:informatica:oracle://oracle_1:1521;SID=orcl"...`
-uj, --user	user	-	User name for the database account to use when the utility connects to the repository or to the operational data store.
-pj, --jdbcPassword	jdbcPassword	-	Password for the database account to use when the utility connects to the repository or to the operational data store.
--configFile	propertyFile	-	Optional for reEncrypt command. Points to the location of the configuration property file. If not specified, Managed File Transfer loads the file from the following location: `<INSTALL>/MFT/server/config/database.xml`
-u, --user	loginName	Yes	Required for reEncrypt command. User name of administrator user with read and write access to Resources and Projects in Managed File Transfer.
-p, --password	password	Yes	Required for reEncrypt command. Password of the administrator user with read and write access to Resources and Projects in Managed File Transfer.
-dp, --decryptionPassword	decryptionPassword	-	Optional for reEncrypt command. Password to initialize decryption Cipher. Decrypt all passwords with decryption Cipher.
-ep, --encryptionPassword	encryptionPassword	-	Optional for reEcrypt command. Password to initialize encryption Cipher. Encrypt all passwords with encryption Cipher.
-es, --encryptString	encryptString	Yes	Required for encrypt command. The password to encrypt.

Windows operating system example:

```
mftpasswd.bat -c reEncrypt -u sys -p sys -l "jdbc:informatica:sqlserver://
localhost:1433;DatabaseName=dbname;"-uj jdbcUser -pj jdbcPassword -dp decryptionKey -ep
encryptionKey
```

CHAPTER 10

System

The System menu provides access to change many of the settings for how Managed File Transfer operates within your environment.

Note: The System menu is only available to Users with the Product Administrator role.

File Manager

The Managed File Transfer File Manager allows authorized users to work with files through their browser. This intuitive interface makes it very easy for Users to explore, download and upload files (as authorized) without the need for special client software. These remote files can be located on the Managed File Transfer server or mapped drives.

A particular User could only be able to download files from an assigned directory, whereas another User could be granted permissions to upload/rename/delete files, as well as have permissions to other directories on the server.

Note: Learn more about User permissions in Role Management and "Add Admin User" on page 577 setup section.

Accessing the File Manager

To work with Roles, log in as an Admin User with the **File Manager** role.

From the main menu, select **System**, and then click the File Manager link.

The File Manager page will be shown, opening the "home directory" that is specified for your User account.

Page Toolbar

The following actions are available from the page toolbar:

Jump directly to a folder by specifying its path next to the Location heading and press Enter, or click the  icon.

Move up to the parent folder by clicking the  icon in the toolbar.

Return to the "home directory" by clicking the  icon in the toolbar.

Create a new folder (under the current folder) by clicking the  icon in the toolbar. Type the name for the folder in the dialog box and click the **Create** button.

Refresh the current folder by clicking the icon in the toolbar.

Upload files by clicking the **Upload** button to open the "Upload Files" on page 752 page.

Working With Files

Download a file by clicking the file name.

Sort the files by name, last modified date or size by clicking the column headings.

File Actions

The following actions are available by selecting a file's Actions icon:

Rename a file by clicking the icon. Type a new file name in the dialog box and click the **Rename** button.

Delete a file by clicking the icon.

Copy a file by clicking the icon. Specify the destination directory in the dialog box and click the **Copy** button.

Move one or more files by clicking in icon. Specify the destination directory in the dialog box and click the **Move** button.

Working With Folders

Open a sub-folder by clicking the folder name.

Sort the files by name, last modified date or size by clicking the column headings.

Folder Actions

The following actions are available by selecting a folder's Actions icon:

Rename a folder by clicking the icon. Type a new folder name in the dialog box and click the **Rename** button.

Delete a folder by clicking the icon.

Copy one or more folders by clicking the icon. Specify the destination directory in the dialog box and click the **Copy** button.

Move one or more files by clicking in icon. Specify the destination directory in the dialog box and click the **Move** button.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected files or folders.
- Copy one or more files and folders to another directory.
- Move one or more files or folders from the current directory to another directory.

Upload Files

Authorized users can upload files by clicking the **Upload** button in the File Manager. Follow the instructions below to upload files:

1. From the main menu, select **System**, and then click the File Manager link.
2. In the File Manager page, click the **Upload** button in the page toolbar.
3. In the Upload Files box, click the **Select Files** button to browse for and select the file(s) to upload. You can also drag-and-drop files from your desktop directly on to this page.
4. Indicate the action to take if the file (with the same name) already exists in the folder which you are uploading into.
   - **Rename** will automatically rename the uploaded file (appending a unique sequential number) so that both files are maintained.
   - **Overwrite** replaces the existing file with the one being uploaded.
   - **Skip** does not upload the duplicate file. It skips the file and proceeds to the next file in the list.
   - **Error** will stop the upload without processing the remaining files.
5. Any messages will be shown in the Upload Summary column.
6. Click the **Close** button when finished.

Global Settings

Global Settings are used to control the overall behavior and attributes of Managed File Transfer. These settings can be viewed and modified by an Admin User with the Product Administrator role.

From the main menu, select **System**, and then click the Global Settings link.

General

Environment

The environment is the name you define for this installation of Managed File Transfer. The environment name is displayed on the top right side of the page and in the browser's title bar. It is also included in system alerts and registration notification emails. This allows quick determination of the Managed File Transfer server to which you are connected (if multiple Managed File Transfer servers exist).

Admin Site URL

Specify the URL for Managed File Transfer. The URL will be displayed in system alerts and registration notification emails.

Locale

The environment (based on a specific language or dialect) that defines conventions such as time and numeric formatting. If a Locale is not specified, the Locale will default to the locale settings of the host operating system.

Date Pattern

You can define the date pattern to use for formatting dates on pages and reports in Managed File Transfer. View the "Date and Time Patterns" on page 794 reference for more information.

Time Pattern

Define the pattern for formatting how the time is displayed on pages and reports in Managed File Transfer. View the "Date and Time Patterns" on page 794 reference for more information.

Timestamp Pattern

The Timestamp pattern is used when the date and time are always displayed together. This setting can differ from the separate Date Pattern or Time Pattern in Managed File Transfer. The Timestamp option is useful in logs or reports when you need exact and detailed date and time information. For more information see the "Date Pattern" on page 753 reference.

Note: Changing any of the settings on the **General** tab, except the Environment and Admin Site URL, requires a restart of Managed File Transfer.

Data

Specify the folder locations for storing Documents, Secure Mail Packages, WebDocs, the Shared Drive audit Index, Projects, Workspaces, and Monitors.

Note: When Managed File Transfer is running in a clustered environment, all directory paths must be absolute (a fully qualified path) and accessible by all systems in the cluster.

Documents Directory

This is the location where files are uploaded and downloaded through the File Manager. By default, this location is relative to the Managed File Transfer installation directory. If Managed File Transfer is installed in `/opt/Informatica/B2B/MFT`, then the default location for the documents directory is `<installdirectory>/userdata/documents`. A separate folder is created within this directory for each Admin User.

Changes to the Documents Directory setting will require a restart of Managed File Transfer.

Packages Directory

The packages directory is the location where "Secure Mail" on page 568 packages are stored. By default, this location is relative to the Managed File Transfer installation directory. If Managed File Transfer is installed in `/opt/Informatica/B2B/MFT`, then the default location for the Packages directory is `<installdirectory>userdata/packages`. A separate folder is created within this directory for each day Secure Mail packages are created.

WebDocs Directory

When a Web User is configured to use the default Home Directory, this is the location that will be used along with a sub-folder based on the Web User account name. Click the  icon to browse for a different folder on the server or to select a "Network Shares" on page 52 resource. Changing the WebDocs Directory path will create and remap all Web User folders using the default ${homeDirectory} to the new Home Directory

location. Changing the WebDocs Directory setting will not move existing files to the new location. A confirmation message confirms this action.

Index Directory

This is the location where Shared Drive and the Global Log audit log indexes are stored. By default, this location is relative to the Managed File Transfer installation directory. If Managed File Transfer is installed in `/opt/Informatica/B2B/MFT`, then the default location for the Packages directory is `<installdirectory>/userdata/index`.

Projects Directory

The location on the network where the Project definitions will be stored. If an absolute path is not specified, this location will be relative to the Managed File Transfer installation directory. The default location is [installdirectory]/userdata/projects.

Workspace Directory

The location on the network where any Project workspaces will be created. If an absolute path is not specified, this location will be relative to the Managed File Transfer installation directory. The default location is [installdirectory]/userdata/workspace.

Changes to the Workspace Directory setting will require a restart of Managed File Transfer.

Monitors Directory

The location on the network where snapshots for the folder Monitors are stored. If an absolute path is not specified, this location will be relative to the Managed File Transfer installation directory. The default location is [installdirectory]/userdata/monitors.

Bandwidth

The Bandwidth settings control the maximum amount of network resources used for Web User transfers (inbound services connections) and designated FTP, FTPS, SFTP, and SCP Resources (client connections). Bandwidth limits enabled here are automatically applied to Web Users. However, the bandwidth limits for FTP, FTPS, SFTP, or SCP client connections will only be applied if the Throttle Bandwidth field is set to ' Yes' on the Connection tab for those Chapter 3, “Resources” on page 42, or if the Throttle Bandwidth field on the Server Tab's Connection pane in “FTP Tasks” on page 381 is set to 'Yes'.

Note: The Bandwidth settings do not apply for file transfers performed through the “File Manager” on page 750.

Inbound Transfer Speed

The inbound transfer speed controls how much overall bandwidth is available for file uploads for Web Users and designated FTP/S, SFTP, and SCP Resources in the Managed File Transfer application. The options below are available when the Bandwidth Limited option is selected.

Max Transfer Rate

The maximum transfer rate is the amount of bandwidth available to inbound Web User and designated FTP, FTPS, SFTP, and SCP transfers. The value can be qualified as kilobytes per second (KB/s), megabytes per second (MB/s) or gigabytes per second (GB/s).

Limit by Time of Day

When the Bandwidth Limited option is selected, you can optionally specify during which hours the bandwidth limit applies.

Limit by Day of Week

The bandwidth limit can be enforced every day or only during the days specified.

Outbound Transfer Speed

The outbound transfer speed controls how much overall bandwidth is available for file downloads for Web User and designated FTP, FTPS, SFTP, and SCP Resources in the Managed File Transfer application. The options below are available when the Bandwidth Limited option is selected.

Max Transfer Rate

The maximum transfer rate is the amount of bandwidth available to outbound Web User and designated FTP, FTPS, SFTP, and SCP transfers. The value can be qualified as kilobytes per second (KB/s), megabytes per second (MB/s) or gigabytes per second (GB/s).

Limit by Time of Day

When the Bandwidth Limited option is selected, you can optionally specify during which hours the bandwidth limit applies.

Limit by Day of Week

The bandwidth limit can be enforced every day or only during the days specified.

SMTP Settings

The SMTP settings indicate the mail server and other settings that Managed File Transfer should use for sending notification emails to Users and Web Users. The Test SMTP Connection button allows testing of the SMTP connection settings.

Host

The host name or IP address (for example, mail.company.com or 192.168.1.3) of the SMTP server.

Note: The SMTP host name is typically found in the account settings of your email application. For instance, in Microsoft Outlook, the SMTP host name is found in the "Outgoing mail (SMTP) server" setting for your email account.

Port

The port number to use for connecting to the SMTP server. The specified value must be between 0 and 65535. The standard default port for email is 25.

User

If required by the SMTP server - the user name (login name) to use for connecting to the SMTP server. If the user name is left blank, then it is assumed that the SMTP server does not require authentication for its email clients.

Password

If required by the SMTP server - the password to use for connecting to the SMTP server.

From Name

The name that appears on emails when they are sent by Managed File Transfer. This is the default name, but some functions within Managed File Transfer can override this value.

From Email

The email address used by Managed File Transfer. Some message functions within Managed File Transfer can override this value.

Connection Type

The connection to the SMTP server can be encrypted using implicit or explicit SSL or O365. The default setting is Normal, which uses a standard or non-encrypted connection.

Client ID

Enter the client ID of the application. It is mandatory if the connection type is O365.

Client Secret

Enter the Client Secret of the application. The Client Secret is mandatory if the connection type is O365 and application is confidential.

Maximum Connections

By default, Managed File Transfer uses one SMTP connection for sending email. When multiple functions send email at the same time, messages will queue until the connection is available. Increasing the number of connections provides the ability to send multiple email messages concurrently.

Test SMTP Connection

The test option allows you to test the SMTP Settings for Managed File Transfer before saving. To test the current SMTP settings, click the **Test SMTP Connection** button. A popup opens where you can specify a To Email Address, the From Name and the From Email. By default, the From Name and From Email are based on the settings on the SMTP Settings tab, but can be modified to verify that another email account can be used as the sender. A successful test sends a brief email to the recipient. After a successful test, click the **Save** button to save the values on the SMTP Settings tab.

Note: Changing any of the settings on the SMTP Settings tab requires a restart of Managed File Transfer.

HTTP Proxy Settings

The HTTP Proxy Settings are only needed if your system uses a proxy server to make HTTP connections. These settings are primarily utilized when a Product Administrator checks for new product updates from the update server.

Proxy Type

The type of proxy, if any, used by Managed File Transfer. A direct connection indicates the server connects directly to the Internet and does not use a proxy. An HTTP proxy is for high-level protocols like HTTP or FTP. If a SOCKS proxy is used, Managed File Transfer supports both V4 and V5.

Proxy Host

The host name (or IP address) of the proxy server on your network.

Proxy Port

The port number of the proxy server on your network. The default proxy port is 80.

Proxy Username

The user name (login name) to use for connecting to the proxy server.

Proxy Password

The password to use for connecting to the proxy server.

Projects Settings

Enable File Locking

File locking allows you to protect the integrity of files while they are being processed by Managed File Transfer.

If enabled, Project tasks in Managed File Transfer that read local or network files will attempt to acquire a "shared" lock on the files before processing them. This shared lock will prevent other applications from locking a file (for write access) while it is in use by Managed File Transfer.

If enabled, Project tasks that write or modify files will attempt to acquire an "exclusive" lock on the files before processing. This exclusive lock will prevent other applications from locking a file (for read or write access) while it is in use by Managed File Transfer.

File Lock Timeout

The amount of time (in seconds) that the File Lock process in Managed File Transfer will wait to obtain a lock on a file. A value of -1 indicates that there is an unlimited wait time. A value of 0 indicates that a lock attempt will only be tried once. Otherwise, specify a value up to 86,400 seconds (24 hours).

Note: If a lock cannot be obtained within the specified timeout period, then an error will be generated in the Project task which is attempting to obtain the lock.

Encryption key

You can encrypt any content The Managed File Transfer stores the data in repositories. Managed File Transfer uses a keyword to create an encryption key to encrypt sensitive data. The **Encrypt** button in Resources allows you to create an encryption key.

Secret Key Password

Use the Secret Key password to digitally sign the file(s). The secret key password entered here replaces the default secret key password used for encryption. After you enter the new secret key password, stop the MFT service, run the re-encryption tool from the command line and then start the MFT service for the changes to take effect.

Runtime Settings

Jobs

Maximum Concurrent Batch Jobs

The maximum number of threads that are allocated for active batch Chapter 4, “Workflows” on page 100. Each active Job utilizes a separate thread (a slice of CPU) in Managed File Transfer. Therefore, if the Maximum Concurrent Batch Jobs is set to 50, then up to 50 batch Jobs can be active at one time. Once the Maximum Concurrent Batch Jobs is reached, any new batch Jobs will be placed in the “Work with Queued Jobs” on page 220 until threads become available. This setting does not apply to Jobs that run interactively or Jobs launched by a “Monitors” on page 197.

When running Managed File Transfer in a “Clustering” on page 772 environment, this setting applies to each system in the cluster. For example, if the Maximum Concurrent Batch Jobs is set to 50 and there are three systems in the cluster, a total of 150 batch Jobs could be run concurrently.

Thread Keep Alive Time

The amount of time (in seconds) in which an idle thread will wait before it is destroyed. When a Job completes, the thread it utilized will remain idle until another Job uses it, or until the "Thread Keep Alive Time" is reached.

Note: Increasing the Maximum Concurrent Batch Jobs or the Thread Keep Alive Time will likely cause Managed File Transfer to consume more CPU and memory. However, more batch Jobs will be able to execute at one time and Jobs will start up quicker since they will not have to create new threads as frequently.

Monitors

Maximum Concurrent Monitors

The maximum number of threads that are allocated for active Monitors. "Monitors" on page 197 are used for scanning folders and running Projects when the Monitor conditions are met. Each Monitor utilizes a separate thread (a slice of CPU) in Managed File Transfer. Therefore, if the Maximum Concurrent Monitors value is set to 20, then up to 20 Monitors can be active at one time. Once the Maximum Concurrent Monitors value is reached, any new Monitors will be queued until threads become available.

When running Managed File Transfer in a clustered environment, this maximum setting applies to each system in the cluster. For example, if the Maximum Concurrent Monitors is set to 20 and there are three systems in the cluster, a total of 60 Monitors can be run concurrently.

Thread Keep Alive Time

The amount of time (in seconds) in which an idle thread will wait before it is destroyed. When a Monitor completes, the thread it utilized will remain idle until another Monitor uses it or until the "Thread Keep Alive Time" is reached.

Note: Increasing the Maximum Concurrent Monitors and the Thread Keep Alive Time will likely cause Managed File Transfer to consume more CPU and memory. However, more Monitors will be able to run at one time and they will start faster since they will not have to create new threads as frequently.

Admin Server Configuration

The Admin Server Configuration page provides options to configure Listeners for the Managed File Transfer server.

To manage Listeners, log in as an Admin User with the Product Administrator role.

From the main menu, select **System**, and then click the Admin Server Configuration link.

Page Toolbar

The following actions are available from the page toolbar:

- Save your changes by clicking the **Save** button.
- Save your changes and return to the Service Manager page by clicking the Arrow icon and then click the **Save And Finish** button.
- Return to the Dashboard page without saving your changes by clicking the **Cancel** button.

Shutdown Port

The TCP/IP port number on which Managed File Transfer waits for a shutdown command. This connection must be initiated from the same server or computer that is running this instance of Managed File Transfer.

Admin Configuration Options

- "Listener Configuration" on page 760 to a server by clicking the **Add Listener** link in the page toolbar.

- "Listener Configuration" on page 760 a Listener by clicking the Listener name in the left column.

Listener Configuration

Listeners will monitor for IP traffic and route traffic based on configured settings. The default listener settings supplied in Managed File Transfer should meet the needs for most installations. The Admin Listeners are used to specify connection timeouts, SSL settings, and ports to access Managed File Transfer through an Internet browser.

Note: If you wish to Delete a Listener entry, when on the Admin Listener page, click the  Delete link in the page toolbar.

General

Name

Providing an identifiable name for the listener helps identify it in the Configuration Outline list.

Port

Listeners monitor specific port numbers. Set the port number that the listener will monitor.

Protocol

Sets the protocol to handle incoming traffic. The default value is HTTP/1.1.

Local Address

This is the IP address of the server hosting the port to which you are listening. If available, you can also select it from the drop-down list.

Enable Lookups

When lookups are enabled, the server will search for and report servers by their DNS name. If lookups are not used only the IP address is returned.

Disable Upload Timeout

Lengthy uploads may decrease server performance or be the result of an error. Select whether uploads are subject to timeouts.

Compression

File compression may increase transfer rates, but lower processing speeds. By default, compression is set to On and will compress only text data. If set to Off, no compression is used on files and if compression is set to Force, compression is used for all files.

No Compression User Agents

This option allows a user with the System Administrator role, in certain instances, to specify the header data of a browser for which files will never be compressed.

Connection Timeout

The number of seconds this connection will remain open before closing if no requests are sent. The default is 60 seconds.

Maximum Threads

The maximum number of threads created by the connection for request processing on this Listener. This determines the maximum number of simultaneous requests that can be handled. The default is 200 threads.

Minimum Spare Threads

This is the number of threads that will be created when this listener is first started. The default is four (4) threads.

Note: Changing the Thread values can alter performance. Too few Maximum Threads and transfers may lag, but too many threads may limit performance of other applications. Modify these values to obtain the optimal performance for your configuration requirements.

Server Header

When a User makes a connection to Managed File Transfer via HTTP or HTTPS, the server replies back to the client with the name and version of the server in one of the headers. The Server Header field can be used to customize the server information that is returned. This setting should only be specified when attempting to hide the true identity of the server for security purposes.

Proxy Name

The Proxy Name attribute can be used when Managed File Transfer is run behind a proxy server. This attribute modifies the value returned to web applications that call the request.getServerName() method, which is often used to construct absolute URLs for redirects. Without configuring this attribute, the value returned would reflect the server name on which the connection from the proxy server was received, rather than the server name to whom the client directed the original request.

Proxy Port

The Proxy Port attribute can be used when Managed File Transfer is run behind a proxy server. This attribute modifies the value returned to web applications that call the request.getServerPort() method, which is often used to construct absolute URLs for redirects. Without configuring this attribute, the value returned would

reflect the server port on which the connection from the proxy server was received, rather than the server port to whom the client directed the original request.

SSL

SSL Enabled

From the drop-down list, select the appropriate option:

- Yes - A Secure Socket Layer is used to secure transmissions
- No - Transmissions are not secured with SSL

SSL Protocol

Specify the appropriate option:

- SSL - A traditional Secure Socket Layer protocol is used to secure the transmission
- TLS - A new version of SSL, Transport Layer Security will be used to secure the transmission (default)

Enabled SSL Protocols

Specify a comma separated list of SSL/TLS protocol versions to allow. For example, to enable TLS 1.1, TLS 1.2, and TLS 1.3, specify TLSv1.1, TLSv1.2, and TLSv1.3. Likewise, to enable all versions of SSL/TLS, specify SSLv3,TLSv1,TLSv1.1,TLSv1.2 or TLSv1.3..

Algorithm

This field displays the certificate encoding algorithm. The field is pre-populated based on your installation. The available options are:

- IbmX509 - Only used for IBM based installations
- SunX509 - Used for Sun and most other installations

Client Authentication

This determines how the client will authenticate with the server.

- None - The SSL connection runs without checking certificates and the User is authenticated with a password. If any of the information being transmitted requires a certificate, the connection will fail.
- Optional - The SSL connection looks for a valid certificate, but continues with password authentication if a certificate is not present.
- Required - The SSL connection will not connect or authenticate a User unless a valid certificate is available.

Enabled Cipher Suites

By default all Cipher Suites are enabled to provide the most options between different clients and servers. Although encrypted, the cipher suite automatically selected by the connection may not be the most secure.

This list allows you to limit which ciphers are used. Follow the instructions below to select which Cipher Suites are used:

1. In the left column, click to select (highlight) the Cipher Suites to use. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Cipher Suites are selected, click the → arrow between the group boxes to move the Cipher Suites from left to right.

Key Store File

This file contains the private key and associated certificates that a client uses to authenticate to a server. There are default Key Store files provided with Managed File Transfer or you can create your own. Type the name or click the  icon to browse for the file.

Key Store Password

The password to use for accessing the key store.

Key Store Type

The type of key store. Managed File Transfer supports both the JKS (Java Key Store) and PKCS12 (Public-Key Cryptography Standards) key store types.

Key Store Provider

Based on your installation, not all the providers may be available. The correct Key Store Provider is loaded during the installation. However, if you need specify a provider, select the appropriate option from the drop-down list:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM
- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- SUN - The classic Java cryptographic service
- SUNJSSE - The Java Secure Socket Extension provides an RSA layer to the cryptology
- SUNJCE - The Java Cryptographic Extension is the export compliant variation of the SUN provider
- SUNMSCAPI - The Java implementation of the Microsoft Cryptography API
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509

Key Alias

The key alias identifies a key pair and its associated certificate from all the ones within a Key Store. If no alias is specified, the Key Store opens the first file in the key store. Type the name or click the  icon to browse for an Alias.

Export Head Certificate

Exports the head certificate of the selected Key Alias to your internet browser's default download directory.

Trust Store File

The Trust Store File contains the public keys and certificates used by a server to authenticate a client. There are default Trust Store files provided with Managed File Transfer or you can create your own. Type the name or click the  icon to browse for the file.

Trust Store Password

The password to use for accessing the Trust Store.

Trust Store Type

The type of trust store. Managed File Transfer supports both the JKS (Java Key Store) and PKCS12 (Public-Key Cryptography Standards) trust store types.

Trust Store Provider

Based on your installation, not all the providers may be available. The correct trust store provider is loaded in the installation. However, if you need specify a provider, select the appropriate option from the drop-down list:

- IBMJCE - The IBM Java Cryptographic Extension is the export compliant variation of the SUN provider for IBM
- IBMi5OSJSSE Provider - The IBM i5/OS Java Secure Socket Extension provides an RSA layer to the cryptology for IBM systems running the i5/OS
- SUN - The classic Java cryptographic service
- SUNJSSE - The Java Secure Socket Extension provides an RSA layer to the cryptology
- SUNJCE - The Java Cryptographic Extension is the export compliant variation of the SUN provider
- SUNMSCAPI - The Java implementation of the Microsoft Cryptography API
- BC - The Bouncy Castle provider is a new export compliant set of algorithms for the Java Framework including RSA, DSA, x509

Redirection

HTTP/HTTPS traffic can be automatically redirected to the intended protocol, host and/or port. The redirect process substitutes the appropriate portion of the URL (`[protocol]://[host][:port]`). For example, if a user typed the address "secure.example.com" (which translates to http://secure.example.com on port 80), the connection could be redirected to https://secure.example.com:9001 by specifying the HTTPS protocol and providing the port used for SSL traffic.

Enable

When redirection is enabled, traffic is redirected using the values in the following fields.

Redirect Host

The host name or IP address to which HTTP/HTTPS traffic should be redirected. If no redirect host is specified, Managed File Transfer uses the URL or address portion of the original request (for example, if the request is made to secure.example.com, that value will be attached to the specified port or protocol).

Redirect Port

The redirect port is the port to which HTTP/HTTPS traffic should be redirected. If not specified, the default port for HTTP is 80 and HTTPS is 443.

Redirect Protocol

The protocol on which traffic should be redirected. Select the protocol from the drop-down list. The default value is HTTPS.

Database Configuration

The database that you selected when you installed Managed File Transfer includes most everything which Managed File Transfer needs to operate, including user-defined Global settings, user account information, permissions, server configuration information and more. The database also stores the audit log entries for each of the protocols.

The Database Configuration page displays the current database configuration and provides options to edit the current database configuration or migrate the embedded Managed File Transfer database to an external database. If pending database changes exist, a summary of the changes are displayed below the current configuration. The page also provides configuration options for the backup and tuning settings for the embedded Managed File Transfer database.

To manage the database, log in as an Admin User with the **Product Administrator** role.

From the main menu, select **System**, and then click the Database Configuration link.

Available Options

- "Edit Database Configuration" on page 766 the Database Configuration settings by clicking the Edit Configuration link in the toolbar
- "Switch Database" on page 767 (migrate) the current Managed File Transfer database to an another database by clicking the Switch Database link in the page toolbar
- "Database Backup" on page 770 the Database Backup settings by clicking the Backup link in the toolbar
- "Database Tuning" on page 771 the Database Tuning settings by clicking the Tuning link in the toolbar
- "Database Statistics" on page 772 the Database Statistics by clicking the Statistics link in the toolbar

  Note: The Backup and Tuning sub-menu options are only available if using the embedded Derby database.

Edit Database Configuration

The Database Configuration page allows a User (with the Product Administrator role) to change the database user credentials and connection settings for the current database used by Managed File Transfer.

Note: If you need to switch (migrate) the connection to a new or different database, then use the Switch Database process. Listed below is the Edit Database Configuration page, which is accessible from the **Database Configuration** option from the Administration menu. After making any changes on this page, you can press the **Save** button to apply the changes. Please note that any changes will not be recognized until after a restart of Managed File Transfer.

JDBC Driver

The JDBC driver used to connect to the target database.

JDBC URL

The connection URL string for the database. This URL should contain the host name (or IP address) of the database server. Depending on the type of database server, you may additionally need to specify the database port number, database name and other properties in the URL. The URL string must be formatted properly. Use the "JDBC URL Wizard" on page 791 to generate this URL string correctly. Click the  button (located on the right side of the field) to launch this wizard.

User

The name of the user to connect (log in) to the database server.

Password

The password to use for connecting to the database server. After typing the password, you can optionally click the **Encrypt** button, which will encrypt the password.

Is Password Encrypted?

Indicates whether or not the password is encrypted. Select **Yes** if you clicked the Encrypt button for the Password.

Minimum Connections

The minimum number of connections which Managed File Transfer will maintain with the database.

Maximum Connections

The maximum number of connections which Managed File Transfer can make to the database at any time.

Maximum Idle Connections

The maximum number of idle connections that can remain open at any time.

Maximum Wait Time

The time (in milliseconds) which a database connection request will wait for a connection before the request fails.

Note: The database settings are stored in a file named database.xml, located in the [installdirectory]/config folder (where [installdirectory] is the default installation location of Managed File Transfer). When changes are made to the database configuration, a backup of the current file is saved to [installdirectory]/config/backups with a date and timestamp appended to the filename. (for example, database-2012-11-30-13-49-24.xml).

Switch Database

The Managed File Transfer database can utilize (connect to) one of the following database types for storing its configuration settings and application data:

- Microsoft SQL Server - SQL Server 2008 R2 and later
- Oracle - 11g R2 and later

The Switch Database function provides a guided process for changing the Managed File Transfer connection to one of these supported databases. This function creates the necessary tables and indexes, as well as migrating the existing Managed File Transfer data to the new database.

The Switch Database process is comprised of six steps. No changes will be applied until clicking the Finish button on the final step. After the Switch Database Wizard completes, you will need to restart Managed File Transfer in order to connect to the new database.

Note: A database switch may take several minutes to execute if you plan to migrate the existing data from the current database. The data migration time will depend on the amount of data in the current database.

Warning: Only perform the database switch when no other users are using Managed File Transfer. The migration will stop Monitors, Scheduled Jobs, and Projects from executing. Additionally, all services, Web User sessions, and the Managed File Transfer Gateway connection will be stopped.

Step 1 - Select Target Database

Select a Database Server from the list of available database server types and then click **Next**.

Step 2 - Prerequisites

Based on the selected database server, some prerequisites may need to be completed before proceeding. The required steps are listed on the page for the selected database server. To ensure a smooth database conversion, complete the prerequisites before continuing.

Microsoft SQL Server

The Microsoft SQL Server database supports either SQL Server Authentication or Windows Authentication (Integrated Security).

Configure SQL Server With SQL Server Authentication

1. Open the Microsoft SQL Server Management Studio.
2. Log in to the target database as a database administrator.

3. Create a new database named GADATA.
4. Create a new database login named GADATA and set the default database for this login to the database created in the step 3.
5. Create a new user named GADATA under the database created in step 3. During this user creation, make sure to attach this user to the login created in step 4. Set the default schema for this user as GADATA (we will create this schema in the later steps), and assign this user the role of db_owner.
6. Create a new schema named GADATA under the database created in step 3. While creating this schema, make sure to set the schema owner as gadata that was created in step 5.

Configure SQL Server with Windows Authentication (Integrated Security)

To use Windows Authentication with Managed File Transfer, you must select the Integrated Security option from the Step 3 - Connection Information page, as well as install the sqljdbc_auth.dll file. When the Integrated Security option is set, Managed File Transfer will add the integratedSecurity=true flag to the JDBC URL used to connect to the database. The SQL server driver will ignore the username and password specified in the switch database configuration and use the Log On information configured in the Windows Service. Use the following instructions configure Windows Authentication:

1. Open the Microsoft SQL Server Management Studio.
2. Log in to the target database as a database administrator.
3. Create a new database named GADATA.
4. Download the JDBC driver pack from Microsoft's website. The sqljdbc_auth.dll file is included in the driver pack.
5. Place the sqljdbc_auth.dll in the Managed File Transfer [installdirectory]\jre\bin folder.
6. Open Windows Services, right-click on the Managed File Transfer Service, and then select Properties. The credentials that start the Windows service will need to be given permission on the SQL Server for Integrated Security.
7. Restart the Managed File Transfer Service.
8. Return to Microsoft SQL Server Management Studio, and create a new schema named GADATA under the database created in step 3. While creating this schema, make sure to set the server authentication to SQL Server and Windows Authentication mode.

MySQL

1. Create a new database (also called schema) by running the statement CREATE DATABASE GADATA CHARSET=UTF8.
2. Create a new database user by running the statement CREATE USER GADATA IDENTIFIED BY 'password'.
3. Grant full permissions to the new database created in step 1 to the user created in step 2, by running the statement GRANT ALL ON GADATA.* to 'GADATA'.

Oracle

1. Create a new database named GADATA.
2. Create a new database user named GADATA.
3. Grant all privileges to the new database created in step 1 to the user created in step 2.

Step 3 - Connection Information

Based on the selected database server, provide the requested connection information. The connection credentials are verified after clicking the **Next** button. If there are connection errors, a description of the connection error is displayed on the page. Connection errors must be corrected before continuing. The example below shows a connection being made to a DB2 database.

Step 4 - Customize JDBC URL

Based on the database server selected and the connection information from Step 3, a JDBC URL is automatically composed. If needed, the JDBC URL can be modified on this page or through the "JDBC URL Wizard" on page 791 by clicking the  button.

Step 5 - Select Operations

Table Creation and Data Population

With the connection configuration complete, select how the Switch Database process will migrate the database. The first option will make a copy of the existing Managed File Transfer data to the new database. The second option will create a new database configured for use by Managed File Transfer with the default data, just as it was when it was first installed. The third option will not configure the new database or populate any data.

Note: The third option is commonly used when configuring Managed File Transfer on a clustered, HA or DR system. These installations only need to point their connection to the Production database in use by the running system.

Character Encoding

If supported by the external database, the option to use either the default encoding of the external database server (using CHAR/VARCHAR for all character columns) or the National Character Set (using NCHAR/NVARCHAR for all character columns) appears. The National Character Set is typically used for double-byte languages, such as Chinese or Japanese, and will use more space for character fields.

Step 6 - Review Changes

When all the required information for the database change is specified, those settings will then be displayed for review. If you wish to change any of these settings, then click the **Previous** button to return to the page where the change is needed.

If the settings are correct, click **Finish** to perform the database switch. The Switch Database process will stop any services and close all open connections. When using the Managed File Transfer cluster feature, all changes made to one system in the cluster are propagated to all other systems in the cluster.

Switch Database Complete

After clicking the Finish button, a Progress box opens to display the switch database progress. When complete, click the **Done** button.

The new database connection will be utilized after Managed File Transfer is restarted.

Database Backup

The Managed File Transfer Database Backup page provides the options to automatically schedule database backups or manually backup the Managed File Transfer database. These database backup options are only available if the embedded Derby database is used.

Last Backup Time

This field displays the last backup time for the Managed File Transfer database.

Next Backup Time

This field shows the next scheduled time the backup will take place.

Enable Database Backup

Indicates whether or not the Managed File Transfer internal database should be backed up automatically on a scheduled basis. The automatic backup runs without the need to shut down Managed File Transfer. It is highly recommended that the database backup remains enabled. If data needs to be recovered, there is less chance for loss.

Backup Directory

The database backup files are created in the [installdirectory]/userdata/database/backups folder, where [installdirectory] is the installation directory for Managed File Transfer.

Keep Backups For

The number of days (1–30) to keep the database backup files. Backup files older than the specified number of days will be automatically deleted following each backup process. By default, database backup files are retained for 7 days.

Schedule Type

The Backup schedule can be run Hourly or Daily. The schedule options toggle based on this selection.

Options

Run Every

This number indicates the number of delay hours or days between database backups.

Run Time

When the Backup schedule is set to Daily, the time of day the backup runs is set here.

Manually Backing Up the Informatica Managed File Transfer Database

To backup the Managed File Transfer database manually:

1. From the main menu, select **System**, and then click the Database Configuration link.
2. In the tool bar, click **Backup** and then click the **Backup Now** button.
3. When the system completes the backup process, a message displays the backup location and file name. For example, `<installdirectory>/userdata/database/backups/informaticamft20150304114913.zip`.

Database Tuning

Tuning the Managed File Transfer database will compress the indexes, which keeps queries running at maximum speed. The Database Tuning page provides options to schedule database tunings or manually tune the database. A consistency check can also be performed to ensure that the database tables are not corrupt.

These database tuning options are only available when using the embedded Managed File Transfer Derby database.

Last Tuning Time

This field displays the last tuning time for the Managed File Transfer database.

Next Tuning Time

This field shows the next scheduled time the tuning will take place.

Enable Database Tuning

Specify whether or not the Managed File Transfer internal database should be tuned automatically on a scheduled basis. The automatic tuning runs without the need to shut down Managed File Transfer. If a database backup and tuning are scheduled at the same time, the backup will run first. The automatic tuning option both tunes the database and runs a Consistency Check.

Schedule Type

The tuning schedule can be run Daily or Weekly. The schedule options toggle based on this selection.

Options

Run Every

This number indicates the number of delay days or weeks between database tunings.

Run On

If the weekly schedule is selected, this is the day of the week the database tuning is performed.

Run Time

This is the time that the automatic database tuning will take place.

Manually Tuning the Informatica Managed File Transfer Database

Tuning the database compresses the indexes, which keeps queries running at maximum speed. To tune the Managed File Transfer database manually:

1. From the main menu, select **System**, and then click the Database Configuration link.
2. In the toolbar, click **Tuning** and then click the **Tune Database Now** button.
3. In the confirmation box, click the **Continue** button.
4. When the system completes the tuning process, a message displays how long the tuning process took.

   Note: Tuning the database will acquire a lock on all database tables. This means that connections to the database may fail while tuning is taking place. You should only tune the database when the system is not in use. The time it takes to tune the database is solely based on the number of records stored in the database and may take several minutes to complete.

Running a Informatica Managed File Transfer Database Consistency Check

A consistency check runs a verification on the tables to ensure they are not corrupt. To run a consistency check on the Managed File Transfer database:

1. From the main menu, select **System**, and then click the Database Configuration link.
2. In the toolbar, click **Tuning** and then click the **Check Database Consistency** button.
3. When the system completes the consistency check process, a message displays how long the consistency check took.

Database Statistics

The Database Statistics page displays the current database table names and row counts for each table used by Managed File Transfer. At the bottom of the list, click the **Done** button to return to the Database Configuration page or click the **Refresh** button to update the database statistics.

Clustering

Clustering allows two or more Managed File Transfer installations (systems) to work together to provide file transfer services for the enterprise. This provides greater scalability by allowing workloads to be distributed across multiple Managed File Transfer systems. The active-active cluster configuration provides high

availability in that if one of the Managed File Transfer systems fail, then the remaining Managed File Transfer systems in the cluster will continue to process workloads and file transfer requests.

The following features are available in Managed File Transfer, when running in a cluster:

- Two or more Managed File Transfer systems within a cluster can connect to the same external database at the same time. This allows these systems to share security settings, trading partner user accounts, configurations, audit logs and other tables.
- The System Name (specified in cluster.xml) will appear on the Managed File Transfer login page, on the top-right corner of the dashboard and any cluster-related pages. This name will also be recorded in audit log records to indicate which system was servicing a trading partner's session during each event. The system name is accessible in Triggers using the 'event.systemName' variable.
- The Active Sessions page displays all trading partner sessions (IP address, user name, login date, audit activity) for any system in the cluster. Within this page, sessions can also be terminated (killed) on any system in the cluster.
  Informatica Managed File Transfer Gateway configurations can be viewed, updated, started and stopped from any Managed File Transfer system within the cluster.
- Auto blacklist features for "Denial of Service" and "Brute Force" attacks are cluster-aware. This allows each system (in the cluster) to share security activity with each other to determine when to block attacking IP addresses from the cluster.
- The Max Sessions setting for a Web User account will limit the total number of that user's sessions for all systems within the cluster. For instance, if the Max Sessions for a Web user is set to 2 and if they are logged into 2 different systems in the cluster, then they will not be able to open any additional sessions in the cluster at that time.
- Batch jobs will be executed by any available systems in the cluster. If a particular system becomes too busy, other systems in the cluster will pick up any jobs from the job queue for execution.
- The "Active Jobs" on page 221 page will display all jobs which are executing across all systems in the cluster. Within this page, jobs can be held/released/cancelled on any system in the cluster.
- File monitor jobs (for scanning folders) will be distributed evenly across all systems in the cluster to optimize performance.

System Roles

The first system started in the cluster assumes the Coordinator role and additional systems become Participants in the cluster. If the system acting as the Coordinator becomes unresponsive, the first Participant in the cluster will assume the Coordinator role.

Coordinator Duties

- Executes all background jobs (for example, purging processes and Web User password expiration notifications).
- Keeps track of all IP addresses that are being monitored for auto-blacklisting.
- Accepts file transfer connections from Web Users.
- Distributes the processing of Monitors (for scanning folders) evenly across all systems in the cluster.
- Maintains the Scheduler and determines which jobs to execute.
- If there are active jobs running on a Participant system when it shuts down, the Coordinator will set the status of those jobs to canceled.
  Participant Duties

  Monitors active systems to detect if the Coordinator has left the cluster.
- Accepts file transfer connections from Web Users.

Clustering Prerequisites

The following are requirements for operating Managed File Transfer in a cluster.

- All Managed File Transfer installations in the cluster must be on the same product version.
- It is also recommended that the operating systems and Java versions match for each system for simplifying configurations.
- The same folder locations must be specified for the Logs Directory, Documents Directory, WebDocs Directory as well as the Packages Directory when Secure Mail is enabled.
- All systems must be configured to use the same external database (SQL Server, Oracle).
- The system clock on each Participant system must be within five minutes from the system clock on the Coordinator system. This time is compared in UTC and ignores time zone differences between systems.
- The cluster.xml file (located in [installdirectory]/config), needs to be configured to enable clustering.

  systemNameA unique name to identify this system in the cluster. The maximum system name length is 20 characters.

  clusterBindAddressThe IP address on which Managed File Transfer will use to communicate with other systems in the cluster. This IP address must be valid for the local system.

  clusterBindPortThe port number which Managed File Transfer will use to communicate with other Managed File Transfer systems in a cluster. For example, if the cluster bind port is 9006, the XML would look like <entry key="clusterBindPort">9006</entry>.

  clusterLogLevelThe log level of "info" will record all standard log messages from each system in the cluster. When the log level is set to "verbose" the log will also record all of the system-to-system messages used to manage the cluster.

  clusterEnabledThis must be set to "true" for Managed File Transfer to be cluster aware.

  - If using the Managed File Transfer Gateway for reverse proxy, the load balancing feature needs to be added to Managed File Transfer Gateway and the Load Balancer Rules configured in Managed File Transfer.
    Additional cluster configuration information is available in the Managed File Transfer Installation Guide.

Project Execution

Projects submitted in batch mode are placed in a shared queue for any available system to pick up for execution, which could be a coordinator or participant system. Typically the system that submits the batch job will process it unless the Maximum Concurrent Batch Jobs limit (specified in the Global Settings) is reached on that system. In this case, another available system in the cluster will execute the job.

Note: Projects executed in interactive mode will always run on the system they were submitted on.

Monitor Execution

File Monitors repeatedly scan for new, modified or deleted files. When a file condition is detected, a Project is executed to process this event. When Managed File Transfer is running in a clustered environment, the execution of these Monitors are evenly distributed across all available systems in the cluster.

The total number of Monitors that can run on any system in the cluster at one time is determined by the "Maximum Concurrent Monitors" setting on the Runtime tab found on the Global Settings page.

Cluster Manager

The Cluster Manager page displays all systems in a Managed File Transfer cluster. The page shows details for each system such as the system name, the current role and whether or not they are active. The page will automatically refresh when the Auto Refresh option is selected.

To view all systems in the cluster, log in as an Admin User with the **Product Administrator** role.

From the main menu, select **System**, and then click the Cluster Manager link.

Custom Tasks

Managed File Transfer includes over 60 Chapter 5, "Task Reference" on page 227 to satisfy most of the business processes needed for managed file transfer. In some cases you may need a custom task in order to provide additional functionality. For example, a custom task could be built to integrate with other internal applications through a proprietary connection.

The Custom Tasks page provides a method to install and manage these custom tasks. Once a task is installed, a user with the Project Designer role will be able to add the custom task to Projects.

To work with Custom Tasks, log in as an Admin User with the Product Administrator role.

From the main menu, select **System**, and then click the Custom Tasks link.

Page Toolbar

The following actions are available from the page toolbar:

- "Install Custom Task" on page 775 a custom task by clicking the Install Custom Task link in the page toolbar.

  - Click the **Done** button to return to the previous page.

Custom Tasks Actions

- "Edit Custom Task" on page 776 a custom task by clicking the icon.

  The following actions are available by selecting the Actions icon:

- "View Custom Task" on page 776 the task information by clicking the icon.
- "Edit Custom Task" on page 776 a custom task by clicking the icon.

  - Uninstall the custom Task by clicking the icon.

Install Custom Task

To install a Custom Task follow the steps below:

1. Copy the Java Archive (.jar) file(s) containing the custom task to the [installdirectory]\userdata\lib folder.

2. Restart Managed File Transfer.
3. Log in as an Admin User with the Product Administrator role.
4. From the main menu, select **System**, and then click the Custom Task link.
5. Click the Install Custom Task link in the sub-menu.
6. In the Install Custom Task page, specify the Implementation Class name and then click **Next**.
   - Implementation Class - The Fully Qualified Class Name (FQCN) is composed of the package name and the classname of the custom task. The format is [packageName][ClassName]. The package and class name are provided by the task vendor.
7. In the following Install Custom Task page, type a name for the custom task and a description.
8. Click Install to add this custom task to Managed File Transfer.

Edit Custom Task

The Edit Custom Task page provides options to edit the custom task details and to deprecate the task. When a task is deprecated it will appear in the Component Library inside the **Miscellaneous** > **Outdated Tasks** folder. When finished making changes to the custom task, click the **Save** button.

Name

The name which will be displayed when selecting a task from the **Application** > **Custom Tasks** folder in the Component Library from the Project Designer.

Description

An optional description of the task.

Deprecated

If this task has been replaced by a newer version, you can indicate to have this task deprecated. Projects can still use this task, but it will be available in the Component Library inside the **Miscellaneous** > **Outdated Tasks** folder.

View Custom Task

The Custom Task Details page displays information about when the custom task was created, modified and more. When finished viewing the custom task details, click the **Done** button.

System Alerts

When system alerts are enabled, Managed File Transfer can email Product Administrators when the system is started, shut down, when memory is reaching a set threshold, the Managed File Transfer license is set to expire, or when changes are made to an Managed File Transfer Cluster. Web User Managers can receive alerts when a Web User is deactivated for any reason. Key Managers can receive alerts when SSL certificates or OpenPGP Keys are set to expire, and Trigger Managers can receive alerts when a trigger fails. Product

Administrators can add additional email addresses to notify others when an event occurs. System Alert notifications are based on "System Alert Email Templates" on page 829 that are defined in xml files and can be modified to meet your specifications.

To modify System Alerts, log in as an Admin User with the Product Administrator role.

From the main menu, select **System**, and then click the System Alerts link.

Page Toolbar

The following actions are available from the page toolbar:

- Save changes by clicking the **Save** button.
- Close the System Alerts page without saving changes by clicking the **Cancel** button.

General Settings

System Alerts Enabled

When enabled, Managed File Transfer will send email alerts for selected system events.

Email Subject Prefix

You can add a prefix to the subject line of all Managed File Transfer email alerts.

System Alert Settings

The following system events can be configured to generate email alerts to administrators:

Administration

The Administration tab notifies Product Administrators when Managed File Transfer is started or shut down, when the JVM memory falls below a specified threshold, or when the Managed File Transfer license is about to expire.

Informatica Managed File Transfer Started

- Notify Product Administrators - An email message will be sent to Admin Users with the Product Administrator role when Managed File Transfer is started.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

Informatica Managed File Transfer Shutdown

- Notify Product Administrators - An email message will be sent to Admin Users with the Product Administrator role when Managed File Transfer is properly shutdown.

  Note: Shutdown alerts cannot be sent if the server is improperly shut down.

- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

JVM Memory

- Available Memory Less Than - Set a minimum threshold for the JVM memory that is available to Managed File Transfer. An alert will be sent every 5 minutes while the Managed File Transfer JVM memory is below the set threshold. A value of 0 will disable this alert.
- Notify Product Administrators - An email message will be sent to users with the Product Administrator role when the JVM memory falls below the set threshold.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

License Expiring

- License Expiring Within - Set the number of days before your license expires to begin receiving daily email reminders until the license is renewed. A value of 0 will disable this alert.
- Notify Product Administrators - An email message will be sent to Admin Users with the Product Administrator role when a Managed File Transfer license is set to expire within the set threshold.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

Web Users

The Web Users tab allows Web User Managers to receive alerts when a Web User is deactivated for any reason.

Web User Deactivated

- Notify Web User Managers - An email message will be sent to Admin Users with the Web User Manager role when a Web User is deactivated.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

SSL Certificates

The SSL Certificates tab notifies Key Managers when SSL Certificates are set to expire.

SSL Certificate Expiring

- SSL Certificate Expiring Within - Set the number of days before an SSL certificate is set to expire. Daily email reminders will be sent until the certificate is renewed.
- Notify Key Managers - An email message will be sent to Admin Users with the Key Manager role when an SSL certificate is set to expire within the set threshold.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

OpenPGP Keys

The OpenPGP Key tab notifies Key Managers when OpenPGP Keys are set to expire.

OpenPGP Key Expiring

- OpenPGP Key Expiring Within - Set the number of days before an OpenPGP Key is set to expire. Daily email reminders will be sent until the key is renewed.
- Notify Key Managers - An email message will be sent to Admin Users with the Key Manager role when an OpenPGP Key is set to expire within the set threshold.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

Triggers

The Trigger tab allows Trigger Managers to receive alerts when a trigger fails.

Trigger Failed

- Notify Trigger Managers - An email message will be sent to Admin Users with the Trigger Manager role when a trigger fails.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

Gateway

The Gateway tab notifies Product Administrators when the connection between Managed File Transfer and Managed File Transfer Gateway™ has been established or when the connection has been broken.

Gateway Connected

- Notify Product Administrators - An email message will be sent to Admin Users with the Product Administrator role when Managed File Transfer has connected to Gateway.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

Gateway Disconnected

- Notify Product Administrators - An email message will be sent to Admin Users with the Product Administrator role when Managed File Transfer has disconnected from Gateway.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

Clustering

The Clustering tab notifies Product Administrators when changes occur to an Managed File Transfer "Clustering" on page 772. Notifications will be sent when the following cluster events occur:

- A new system has joined the cluster
- A system has left the cluster
- A cluster has started and the first system has assumed the Coordinator role
- The Coordinator has left the cluster and a Participant has assumed the Coordinator Role

Cluster Membership Changes

- Notify Product Administrators - An email message will be sent to Admin Users with the Product Administrator role when changes occur to an Managed File Transfer Cluster.
- Notify Additional Email Addresses - Add one or more email recipients to the email alert. Separate multiple email addresses with commas.

IP Filter

IP filters, otherwise known as Whitelists and Blacklists, provide an additional layer of security to ensure Web Users are accessing Managed File Transfer from authorized locations. These filters control which IP addresses or address ranges have access to the various protocols (HTTPS, AS2, FTP, FTPS, SCP and SFTP) within Managed File Transfer. Both IPv4 and IPv6 addresses are supported by the IP Filter and can be specified on the Global or Web User level.

Note: IP filtering only applies to Web Users and not Admin Users.The Global IP filter is only configurable by an Admin User with the Security Officer role. The Web User IP Filter is only configurable by an Admin User with the Web User Manager role.

Global IP Filter and Web User IP Filter Overview

A global IP filter list is typically set as a Blacklist. This type of IP filter will specifically block any service requests from specified IP addresses (IP addresses are specified on the "Manage IP Filters" on page 780 page) and permit the rest.

The IP filters at the Web User level are typically set as a Whitelist. A Whitelist will permit logins from specified IP ranges, but denies all others.

Manage IP Filters

The IP Filter page provides the options to create and configure the global IP filter list. This page is only available to Admin Users with the Security Officer role. The manage IP Filter page provides options to enable or disable the global IP filter, select Blacklist or Whitelist filtering, and IP filter list management options.

The IP filter entries are displayed on the page showing the filter name, the associated IP addresses, when the filter was last modified, and who made the last modification. Click a column heading to sort that column. An arrow in the heading indicates which column is sorted and if it is sorted in ascending or descending order.

To manage IP filters, log in as an Admin User with the Security Officer role.

From the main menu, select **System**, and then click the IP Filter link.

Page Toolbar

The following actions are available from the page toolbar:

- "Add IP Filter Entries" on page 781 IP addresses to the IP filter by clicking the **Add Filter Entries** link in the toolbar.
  - Test an IP address to see if it is currently blocked or permitted by clicking the Test IP Address link in the toolbar.
- "Search IP Filter Entries" on page 782 for IP filter entries by clicking the **Search** button.
  - Delete all the IP filters by clicking the Delete All link in the page toolbar.
  - Enable the IP Filter by clicking the **Edit** button. Enable the filter, choose a Filter Type and then click the **Save** button.

Manage IP Filter Actions

The following actions are available by selecting the Actions icon:

- "View IP Filter Entry" on page 783 the details of an IP filter entry by clicking the icon.
- "Edit IP Filter Entry" on page 783 an IP filter entry by clicking the icon.
  - Delete an IP filter by clicking the icon.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected filter entries.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Add IP Filter Entries

The Add IP Filter Entries page provides an easy to use text box to cut and paste IP addresses. IP addresses can be entered as either single addresses, ranges, or in *CIDR* notation. Entries can be separated by a comma or a line break.

Name

The IP filter name is for identification purposes. It is the name associated with the IP filter list. The list may only include specific ranges and will make finding the entry easier in the IP filter list.

IP Addresses

This text box is used to type or paste IP addresses that will be added to the global IP filter. The IP Addresses field accepts IP address in either a single IP, IP ranges, or *CIDR* notation format. Type each IP address entry on a new line. Do not leave spaces between hyphens or slashes when specifying ranges or using CIDR notation (for example, 10.1.4.1/24 or 10.1.4.1-10.1.255.255).

Note: A single IPv4 address is comprised of four sets of three numbers from 0 to 255, separated by periods. A single IPv6 address is comprised of eight sets of four hexidecimal numbers, separated by colons. An IP range includes all the addresses between two specified addresses. The addresses are separated by a hyphen. An IP address in CIDR notation is an IP address followed by a "prefix." The prefix notates a range of IP addresses without the need to type all the sets.The entries in this area are validated when you click the **Save** button and any errors will be indicated.

Search IP Filter Entries

The Search IP Filter Entries page allows you to search for IP addresses that have been entered into the IP Filter. The search query will find one or more matches within existing IP Filter entries. The resulting entries can be deleted or modified to prevent an address from being blocked. For example, if a Web User is unable to connect to Managed File Transfer, an Admin User could search for their IP address to see if it is being blocked.

To search for IP filters, log in as an Admin User with the Product Administrator or Security Officer role.

From the main menu, select **System**, and then click the IP Filter link. Click the **Search** button from the IP Filter page.

Page Toolbar

The following actions are available from the page toolbar:

- Return to the previous screen by clicking the **Done** button.
- Search for IP filter entries by entering a complete IP address in the IP Address field, and then click **Search**.

Search IP Filter Actions

The following actions are available by selecting the Actions icon:

- "View IP Filter Entry" on page 783 the details of an IP filter entry by clicking the icon.
- "Edit IP Filter Entry" on page 783 an IP filter entry by clicking the icon.

  - Delete an IP filter by clicking the icon.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete one or more selected filter entries.

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Edit IP Filter Entry

On the Edit IP Filter Entry page you can modify the Filter Name and the associated IP addresses. When complete, click the **Save** button.

Name

The IP Filter name is for identification purposes. It is the name associated with the IP Filter list. The list may only include specific ranges and will make finding the entry easier in the IP Filter list.

IP Addresses

This text box is used to type or paste IP addresses that will be added to the Global IP filter.

View IP Filter Entry

The View IP Filter Entry page displays detailed information related to the selected IP filter. The page additionally displays when the IP filter was created and who created it. The page also displays the *CIDR* notation for the entry. When finished, click **Done** to return to the IP Filter list.

Automatic IP Blacklist

The Automatic IP Blacklist feature in Managed File Transfer monitors the active services for repeated unsuccessful access attempts. The automatic IP blacklist can detect both brute-force and denial of service (DoS) attacks. IP addresses can be added to the Exemptions list to prevent them from becoming blocklisted.

To manage Automatic IP Blacklists, log in as an Admin User with the Security Officer role.

From the main menu, select **System**, and then click the Automatic IP Blacklist link.

Configure the settings by clicking the **Edit** button. Blocklisted IP addresses are listed in the lower portion of the page along with the reason for the blacklisting and the duration. After making changes to the automatic IP blacklist settings, click the **Save** button.

Exemptions

Add an "Automatic IP Blacklist Exemptions" on page 785 to prevent specific IP addresses from being blacklisted by clicking the **Exemptions** button.

Search

Click the **Search** button to locate a specific blacklisted IP address. Enter an IP address and then click Search. You can delete the IP entry from the results screen, search for another IP address, or close the Search window.

Automatic Blacklist Enabled

The automatic IP blacklist can be turned on or off.

Brute-force Attack Monitor Enabled

If enabled, the brute-force attack monitor keeps track of the repeated failed logins for each IP address. Based on the sensitivity setting, the monitor will blacklist the IP when the failed login threshold is met.

Sensitivity

The attack threshold level that must be exceeded to blacklist the IP.

Option Name	Description
Very Low	25 invalid logins received over 1 minute. If the Ban Type is set to temporary, then the IP address will be blacklisted for 1 hour.
Low	20 invalid logins received over 2 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 2 hours.
Medium	15 invalid logins received over 3 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 3 hours.
High	10 invalid logins received over 4 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 4 hours.
Very High	5 invalid logins received over 5 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 6 hours.

Ban Type

Attackers that have exceeded the sensitivity setting will be either blocked temporarily or permanently.

DoS Attack Monitor Enable

To accomplish a denial of service (DoS) attack, an attacker will attempt to open all available connections for a service and then send random commands through that connection. The DoS monitor keeps track of repeated connection attempts per service and the commands sent to the server. Based on the sensitivity setting, the monitor will perform the selected ban type when the threshold is satisfied.

Sensitivity

The attack threshold level that must be exceeded to trigger the ban type.

Option Name	Description
Very Low	100 invalid connections received over 1 minute. If the Ban Type is set to temporary, then the IP address will be blacklisted for 1 hour.
Low	90 invalid connections received over 2 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 2 hours.
Medium	80 invalid connections received over 3 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 3 hours.
High	70 invalid connections received over 4 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 4 hours.
Very High	60 invalid connections received over 5 minutes. If the Ban Type is set to temporary, then the IP address will be blacklisted for 6 hours.

Ban Type

Attackers that have exceeded the sensitivity setting will be either blocked temporarily or permanently.

Table Actions

- Click the button to move back to the previous page of results.
- Click the button to move forward to the next page of results.

Automatic IP Blacklist Exemptions

The Automatic IP Blacklist Exemptions feature in Managed File Transfer excludes specified IP addresses from being blacklisted after repeated unsuccessful access attempts.

To manage Automatic IP Blacklists Exemptions, log in as an Admin User with the Security Officer role.

From the main menu, select **System**, and then click the Automatic IP Blacklist link. Click the  **Exemptions** button on the Automatic IP Blacklist page.

Page Toolbar

The following actions are available from the page toolbar:

- "Add or Edit a Blacklist Exemption" on page 786 a new Blacklist Exemption by clicking the  **Add Exemption** button.
- Delete all the Blacklist Exemptions by clicking the  **Delete All** button.
- Return to the Automatic IP Blacklist page by clicking the  **Back** button.

Automatic IP Blacklist Exemption Actions

The following actions are available by selecting the Actions icon:

- "View Exemption" on page 786 the details for a Blacklist Exemption by clicking the **View** button to the entry.
- "Add or Edit a Blacklist Exemption" on page 786 the Blacklist Exemption by clicking the **Edit** button.

  - Delete the Blacklist Exemption by clicking the **Delete** button.

Footer Actions

The following actions are available when one or more items are selected from the table:

- Delete the selected Blacklist Exemption(s).

Table Navigation Tools

The following table navigation tools are available:

- Click the **Previous** button to move back to the previous page of results.
- Click the **Next** button to move forward to the next page of results.
- Select the number of Rows to display on each page.

Add or Edit a Blacklist Exemption

Follow the instructions below to add or edit an IP Blacklist Exemption:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu, select **System**, and then click the Automatic IP Blacklist link.
3. Click the **Exemptions** button on the Automatic IP Blacklist page.
4. To add an exemption, click the **Add Exemption** button in the sub menu bar. To edit an exemption, select it from the table.
5. Specify an optional Label and an IP Address, a range of IP addresses, or a range of IP addresses in CIDR notation.
6. Click the **Save** button when finished.

View Exemption

Follow the instructions below to view the Exemption details:

1. Log in as an Admin User with the Security Officer role.
2. From the main menu, select **System**, and then click the Automatic IP Blacklist link.
3. Click the **Exemptions** button on the Automatic IP Blacklist page.
4. On the list of Exemptions, click the Action icon and then click the **View** button.
5. Click the **Done** button when finished viewing Exemption details.

Active Transfers

The Active Transfers page displays the current file transfers being performed by Web Users and transfers invoked from a Project using FTP, FTPS, SCP, and SFTP. For each file transfer, the name of the file, its size, total bytes transferred and current rate is shown.

The overall transfer speeds can be limited using the settings on the Bandwidth tab in the "Global Settings" on page 752.

To view the Active Transfers page, log in as an Admin User with the **Job Manager** or Product Administrator role and click the **System > Active Transfers** link from the main menu.

Page Toolbar

The following actions are available from the page toolbar:

- Click the **Refresh** button to refresh the transfer details.
- Auto Refresh enables a refresh of the transfer details every 1 second.

Workflows

The Workflows section displays Inbound and Outbound file transfers that were invoked from a Project Workflow using designated FTP, FTPS, SCP, and SFTP Resources. The following columns are displayed:

Start Time

Displays the date and time the file transfer started.

File Name

The name of the file that is being transferred.

Current Rate

The rate the data is being transferred.

Total Transferred

The amount of data that has been transferred for the file.

File Size

The total size of the file being transferred.

Throttled

Indicates if the Resource or Task that is used to transfer the file contains a bandwidth limit.

Job Number

The unique ID number for the Job that invoked the file transfer.

Project

The name of the Project that invoked the file transfer.

Protocol

The name of the file transfer protocol that is being used to transfer the file.

Server

The name of the Resource or host that is being used to transfer the file.

Services

The Services section displays Inbound and Outbound file transfers invoked from a Web User. The following columns are displayed:

Start Time

Displays the date and time the file transfer started.

File Name

The name of the file that is being transferred.

Current Rate

The rate the data is being transferred.

Total Transferred

The amount of data that has been transferred for the file.

File Size

The total size of the file being transferred.

Throttled

Indicates if the Web User account that is being used to transfer the file contains a bandwidth limit.

Web User

The Web User name that is being used to transfer the file.

Module

The Web User file sharing module (HTTPS, FTP, FTPS, and SFTP) that is being used to transfer the file.

Tools

The Tools menu in Managed File Transfer provides access to the "SQL Wizard" on page 788, and "JDBC URL Wizard" on page 791.

SQL Wizard

The Managed File Transfer **SQL Wizard** allows users to quickly build SQL SELECT statements (for retrieving data from a database) without having knowledge of the SQL syntax. This intuitive interface allows a user to choose a database server, select a schema (library), tables, columns, order by, where and join criteria for the SQL statement.

The resulting SELECT statement can be tested and embedded within a Project for future execution.

Note: Data can be retrieved from a single table or from multiple tables through a join.

Using the SQL Wizard

There are two methods to access the SQL Wizard from within Managed File Transfer:

- If you want to build a SQL statement without embedding it into a Project, click the **System > Tools > SQL Wizard** link from the main menu bar. You will first be prompted to choose a "Database Servers Resource" on page 54 from a list, and then click the **Connect** button. After the connection is established, you can use the tabs to build the parameters of the SQL statement.
- Otherwise, if you want to build a SQL statement to embed within a Project, then click the  button next to SQL Statement field on the "SQL Task" on page 267 query element from within the Project. You will first be prompted to choose a "Database Servers Resource" on page 54 from a list, and then click the **Connect** button. After the connection is established, you can use the tabs to build the parameters of the SQL statement. Finally, click the **Select** button to apply the SQL Statement to the query.
  The SQL Wizard page (shown below) is made up of several panels where the schemas, tables, columns, etc. can be selected. You can navigate to a panel by clicking its corresponding tab.

  Follow the steps below to use the SQL Wizard.

Step 1: Choose the Schemas or Libraries

The **Schemas** tab allows you to choose the schemas or libraries (that contain the tables) you want to work with.

- To select schemas, click the checkboxes next to the schemas you want and click the → button. The selected schemas will move to the right side of the page.

Step 2: Choose the Tables (Physical Files)

Click the tab labeled Tables. From this page, you can choose one or more tables for the SELECT statement. There are two different approaches to choose a table (physical file):

- To select tables, click the checkboxes next to the tables you want and click the → button. The selected tables will move to the right side of the page.

Step 3: Choose the Columns (Fields)

Click the tab labeled Columns. A list of all columns (fields) in the selected table(s) will be shown on the left side of the page. From this page, you can choose the columns (fields) for the SELECT statement.

- To select columns, click the checkboxes next to the columns you want and click the → button. The selected columns will move to the right side of the page.

Step 4: Choose the Column Headings

Click the tab labeled Column Headings. By default, the SQL Wizard will use the column names (field names) as the headings within the SELECT statement. You can optionally choose to use the Column Descriptions as the headings OR you can specify your own Custom Headings. If you choose the Custom Heading option, you can enter the heading on the right side of each column in the list.

Step 5: Specify the Where criteria

Click the tab labeled Where. The Where criteria allows you specify which rows (records) to retrieve from the table(s). Multiple lines of criteria can be entered. Follow the steps below to add Where criteria:

1. Choose the column (field) for the compare.
2. Choose the operator (=, >, >=, <, <=, <>, etc.) for the compare.
3. Choose the Value Type and specify the Value.
   - Constant - For comparing the column against a constant value (for example, Country = 'USA'). For the Value, specify the constant (number or string) for the compare.
   - Column - For comparing the column against another column in the table (for example, ShipDate <> OrderDate). For the Value, choose the column for the compare.
   - Function - For comparing the column against a SQL Function (for example, BillDate = curdate()). For the Value, either enter the name of the function or choose the function from a list by clicking the **F** button.
   - Parameter - For comparing the column against a parameter (for example, City = ?). This should only be specified when a parameter subelement is defined in the Project's "SQL Task" on page 267.
4. If additional lines of Where criteria need to be entered, then choose the conjunction under the AND/OR column and click the **Add Where** link. Repeat steps 1-3 above for the new row of Where criteria.
5. Additional functions:
   - Delete a row of Where criteria by selecting its check box and clicking the **Delete Rows** button.
   - Move a row by selecting it and dragging it up or down.
   - Use parenthesis to change the order of the Where criteria by entering one or more left parenthesis under the (column and one or more right parenthesis under the) column.

Step 6: Specify the Join criteria

If multiple tables were selected, then click the tab labeled Join. The Join page allows you specify the criteria on how the tables should be joined together. Multiple lines of criteria can be entered. Follow the steps below to add Join criteria:

1. Choose the column (field) to compare on the left side of the join.
2. Choose the operator (=, >, >=, <, <=, <>) for the join condition.
3. Choose the type of join:
   - Inner Join - The results will contain any rows (records) from the two joined tables which match the join condition. All other rows will be excluded from the results.
   - Left Outer Join - The results will contain all rows from the "left" table, even if the join-condition does not find any matching rows in the "right" table.
   - Right Outer Join - The results will contain all rows from the "right" table, even if the join-condition does not find any matching rows in the "left" table.
4. Choose the column (field) to compare on the right side of the join.
5. If additional lines of Join criteria need to be entered, then specify the conjunction under the AND/OR column and click the **Add Join** link. Repeat steps 1-4 above for the new row of Join criteria.
6. Additional functions:
   - Delete a row of Join criteria by selecting its check box and clicking the **Delete Rows** button.
   - Move a row by selecting it and dragging it up or down.

- Use parenthesis to change the order of the Join criteria by entering one or more left parenthesis under the (column and one or more right parenthesis under the) column.

Step 7: Specify the Order By criteria

Click the tab labeled Order By. The Order By page allows you specify how the rows (records) should be sorted. Multiple lines of criteria can be entered. Follow the steps below to add Order By criteria:

1. Choose the column (field) to order by.
2. Choose how it should be ordered (ascending or descending).
3. If additional lines of Order By criteria need to be entered, then click the **Add Order By** link. Repeat steps 1-2 above for the new row of Order By criteria.
4. Additional functions:
   - Delete a row of Order By criteria by selecting its check box and clicking the **Delete Rows** button.
   - Move a row by selecting it and dragging it up or down.

Step 8: Additional tailoring of the SQL statement

You can optionally tailor the SELECT statement with the features below:

- Click the **Quote Identifiers** check box to place double quotes around any table or column names. This is only needed if any of the selected table or field names have spaces in them (for example, "Order Date").
- Click the **Qualify Field Names** check box to qualify any field (column) names with the corresponding schema and table names (for example, schemaname.tablename.fieldname). This is only needed if you selected multiple tables which have some of the same field names.

Step 9: Test and Generate the SQL statement

When you are done specifying the criteria for the SELECT statement, you can perform one of the following functions:

- Click the **Test** button to test the SELECT statement. This will run the statement against the database and will either return any errors (if the syntax is invalid) OR it will show the results of the SELECT statement (displaying the first few selected rows). This feature will help you verify that the SELECT statement is generating the results that you expected.
- If the SQL Wizard was launched from a Project, then click the **Done** button to embed the generated SELECT statement into the Project's SQL Task.

JDBC URL Wizard

The JDBC URL Wizard allows for the creation of a URL string for connecting to a database. The JDBC URL requires at least the host name (or IP address) of the database server. Depending on the type of database server, it may also be necessary to specify the database port number, database name and other properties in the URL.

The JDBC URL Wizard provides preconfigured drivers and settings for popular databases, or you can specify a custom URL to connect to other databases.

1. From the JDBC URL Wizard page, select a predefined or custom JDBC Driver type.
2. For a Predefined driver, specify the database Host name or IP. For a Custom driver, specify the Driver and URL.
3. Specify any other required settings for the JDBC URL in the lower section.

4. Click the **Advanced Properties** button for additional options based on the selected JDBC database type, if needed.
5. Click the Generate URL buton to display the JDBC URL.

Advanced Settings

The Advanced Settings page provides a number of additional settings for the selected database JDBC URL. The Current / Default settings for the selected database JDBC URL are displayed for quick reference. When configuration changes are complete, click the **Generate URL** button to generate the JDBC URL based on the configuration.

Generate URL

The Generate URL page displays the JDBC URL that was generated based on the selected database and the required settings.

When working with Projects or Resources, click the **Select** button to place this JDBC URL in the location the JDBC URL Wizard was started.

CHAPTER 11

Appendix

This chapter includes the following topics:

About Informatica Managed File Transfer

The About pages display version numbers, local computer (System) information and memory usage. This information is helpful if you ever need to contact Informatica Support.

About

The Managed File Transfer version number is displayed on the About tab. Click the **Done** button when finished.

System Info

The installation location and local computer operating system information is displayed on the System Info tab. Click the **Done** button when finished.

System Resources

Memory usage information is displayed on the System Resources tab. The information on this tab refreshes every five (5) seconds. Click the **Done** button when finished.

System Properties

The System Properties tab displays all the detailed installation and application version information. This information is useful if you need to contact Informatica Support. Click the **Done** button when finished.

Date and Time Patterns

Date and time formats are specified by date and time pattern strings. Within date and time pattern strings, unquoted letters from 'A' to 'Z' and from 'a' to 'z' are interpreted as pattern letters representing the components of a date or time string. Text can be quoted using single quotes (') to avoid interpretation. All other characters are not interpreted; they're simply copied into the output string during formatting or matched against the input string during parsing.

The following pattern letters are defined (all other characters from 'A' to 'Z' and from 'a' to 'z' are reserved):

Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
y	Year	Year	1996; 96
M	Month in year	Month	July; Jul; 07
w	Week in year	Number	27
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday; Tue
a	Am/pm marker	Text	PM
H	Hour in day (0-23)	Number	0
k	Hour in day (1-24)	Number	24
K	Hour in am/pm (0-11)	Number	0
h	Hour in am/pm (1-12)	Number	12
m	Minute in hour	Number	30

s	Second in minute	Number	55
S	Millisecond	Number	978
z	Time zone	General time zone	Pacific Standard Time; PST; GMT-08:00
Z	Time zone	RFC 822 time zone	-0800

Pattern letters are usually repeated, as their number determines the exact presentation:

- Text: For formatting, if the number of pattern letters is 4 or more, the full form is used; otherwise a short or abbreviated form is used if available. For parsing, both forms are accepted, independent of the number of pattern letters.
- Number: For formatting, the number of pattern letters is the minimum number of digits, and shorter numbers are zero-padded to this amount. For parsing, the number of pattern letters is ignored unless it's needed to separate two adjacent fields.
- Year: For formatting, if the number of pattern letters is 2, the year is truncated to 2 digits; otherwise it is interpreted as a number.
  For parsing, if the number of pattern letters is more than 2, the year is interpreted literally, regardless of the number of digits. So using the pattern "MM/dd/yyyy", "01/11/12" parses to Jan 11, 12 A.D.

  For parsing with the abbreviated year pattern ("y" or "yy"), the date must interpret the abbreviated year relative to some century. It does this by adjusting dates to be within 80 years before and 20 years after the time the date instance is created. For example, using a pattern of "MM/dd/yy" and a date instance created on Jan 1, 1997, the string "01/11/12" would be interpreted as Jan 11, 2012 while the string "05/04/64" would be interpreted as May 4, 1964. During parsing, only strings consisting of exactly two digits will be parsed into the default century. Any other numeric string, such as a one digit string, a three or more digit string, or a two digit string that isn't all digits (for example, "-1"), is interpreted literally. So "01/02/3" or "01/02/003" are parsed, using the same pattern, as Jan 2, 3 AD. Likewise, "01/02/-3" is parsed as Jan 2, 4 BC.
- Month: If the number of pattern letters is 3 or more, the month is interpreted as text; otherwise, it is interpreted as a number.
- General time zone: Time zones are interpreted as text if they have names. For time zones representing a GMT offset value, the following syntax is used:
  GMTOffset TimeZone:

  GMT Sign Hours : Minutes

  Sign: one of

  + -

  Hours:

  Digit

  Digit Digit

  Digit : one of

  0 1 2 3 4 5 6 7 8 9

- RFC 822 time zone: For formatting, the RFC 822 4-digit time zone format is used:
  RFC822TimeZone:

  Sign TwoDigitHours Minutes

  TwoDigitHours:

  Digit Digit

  TwoDigitHours must be between 00 and 23. Other definitions are as for general time zones.

  For parsing, general time zones are also accepted.

Examples

The following examples show how date and time patterns are interpreted in the U.S. locale. The given date and time are 2001-07-04 12:08:56 local time in the U.S. Pacific Time time zone.

Date and Time Pattern	Result
"yyyy.MM.dd G 'at' HH:mm:ss z"	2001.07.04 AD at 12:08:56 PDT
"EEE, MMM d, ''yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02001.July.04 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 4 Jul 2001 12:08:56 -0700
"yyMMddHHmmssZ"	010704120856-0700

Date and Time Pattern	Result
"yyyy.MM.dd G 'at' HH:mm:ss z"	2001.07.04 AD at 12:08:56 PDT
"EEE, MMM d, ''yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02001.July.04 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 4 Jul 2001 12:08:56 -0700
"yyMMddHHmmssZ"	010704120856-0700

Number Patterns

Number patterns are used to format how numbers are displayed. The characters specified in the table below are interpreted as patterns representing the components of a number string. A number pattern can be prefixed or suffixed by text or other special characters using single quotes. Characters that are not interpreted are copied into the output string during formatting or matched against the input string during parsing.

The following pattern letters are defined:

Symbol	Description
0	Placeholder for a digit. If more placeholders are specified than the value returned, zeros are displayed in those positions.
#	Placeholder for a digit. If more placeholders are specified than the value returned, nothing is displayed in those positions.
'	Single quotes can be wrapped around text and symbols before or after a number pattern.
.	Placeholder for decimal separator
,	Placeholder for grouping separator
E	Separates the significant digits from the exponent in scientific notation
-	Default negative prefix
$	Currency sign
%	Percent sign

Examples

The following examples show how number patterns are interpreted in the U.S. locale.

Input	Number Pattern	Result	Description
25	0 000	25 025	When the value has more positions in the whole number than specified, the complete value is returned. If the value has fewer positions than indicated in the pattern, 0's are padded to the number.
25	# ###	25 25	When the value has more positions in the whole number than specified, the complete value is returned. If the value has fewer positions than indicated in the pattern, the extra placeholders in the pattern are ignored.
56874	$#,###.00	$56,874.00	The whole number is formatted with the currency and separator. No decimals were in the first parameter, so the specified formatting added them.
56874.879865	###,###.##	56,874.88	Six digits are to the right of the decimal, but only two places are requested, so the value is rounded.

Input	Number Pattern	Result	Description
56874.87	000.000	56874.870	Two digits are to the right of the decimal in the source, but the format expects three and adds a zero.
100	0.00	100.00	When the value has more positions in the whole number than specified, the complete value is returned. No decimals were in the first parameter, so the specified formatting added them.
100	$	$100	The currency sign prefix is placed before the value.
5.6874	E4	56874	The coefficient 4 specifies 10 to the 4th power. The value is multiplied by the exponent to produce the result.
25	'#'00	#25	The special character prefixed the number and is displayed ahead of the result.
56874	$###,###.00'R'	$56,874.00R	The text was added to the value as a suffix.
.25	"0%"	25%	The value is multiplied by 100 to produce the percentage.

Starting and Stopping Managed File Transfer

This section contains the procedures to start and stop Managed File Transfer.

Start Managed File Transfer in Windows

Start the Managed File Transfer by following these instructions:

1. Go to the Windows machine and logon with an administrator account.
2. Go to **Control Panel** > **Administrative tools** > **Services**.
3. In the Services window, right-click on Managed File Transfer and select **Start**. After starting Managed File Transfer, its status is updated to **Started**.

Stop Managed File Transfer in Windows

Perform the following steps to stop Managed File Transfer:

1. Login with an administrator account.
2. Go to **Control Panel** > **Administrative tools** > **Services**.
3. In the **Services** window, right-click on the Managed File Transfer and select **Stop**.

Start Managed File Transfer in UNIX

Start the Managed File Transfer by following these instructions:

1. Open a Terminal window.

2. Change the working directory to the tomcat directory where Managed File Transfer is installed, for example `<Managed File Transfer installation>/MFT/server/tomcat/bin`.
3. Start Managed File Transfer by running the following command:
   `mft-server.sh start`

Stop Managed File Transfer in UNIX

Perform the following steps to stop Managed File Transfer:

1. Open a Terminal window.
2. Change the working directory to the directory where Managed File Transfer is installed.
3. Stop the Managed File Transfer by executing the running the following command:
   `mft-server.sh stop`

Event Types

The following events are logged by Managed File Transfer and can be used to initiate other actions.

Note: Event types denoted with an * cannot be triggered using the "Trigger Manager" on page 206.

Event Name	Service	Executed When (Examples)
AS2 Message Receive Failed	AS2	- Decryption of the message failed - Message signature could not be verified - Message exceeded the maximum upload size
AS2 Message Receive Successful	AS2	- AS2 Message successfully received
Account Disabled	HTTPS, AS2, FTP, FTPS, SFTP	- Maximum number of failed logins exceeded
Before AS2 MDN Send*	AS2	- Web User attempts to send a file using AS2
Before Shared Drive Upload*	Shared Drive, HTTPS	- Web User attempts to upload a file to Shared Drive using the Shared Drive Sync Client or the File Transfer Portal
Before Secure Mail Send*	HTTPS	- Web User attempts to send a Secure Mail message using the Secure Mail Outlook plugin or the File Transfer Portal
Attachment Add Failed*	HTTPS	- File could not be copied to the Secure Mail package - File name exceeds 128 characters - Web User does not have Upload permission - File extension not permitted - File name contains invalid characters
Attachment Add Successful*	HTTPS	- File successfully copied to the Secure Mail package

Event Name	Service	Executed When (Examples)
Attachment Delete Failed*	HTTPS	- File not deleted from the Secure Mail package - Web User does not have Delete Files permission - File no longer exists
Attachment Delete Successful*	HTTPS	- File successfully deleted from the Secure Mail package
Attachment Download Failed*	HTTPS	- Secure Mail recipient did not successfully download the file - File no longer exists
Attachment Download Successful*	HTTPS	- Secure Mail recipient successfully downloaded the file
Change Password Failed	HTTPS	- New password is not successfully created - Password does not meet Web User Password Policy
Change Password Successful	HTTPS	- New password is successfully created and saved
Chmod*	HTTPS, FTP, FTPS, SFTP	- Permissions were changed on a file
Checksum Failed*	HTTPS, FTP, FTPS, SFTP	- Checksum creation failed - Checksum could not be verified
Checksum Successful*	HTTPS, FTP, FTPS, SFTP	- Checksum creation successful - Checksum compare successful
Connection Rejected	FTP, FTPS, SFTP	- Connection was rejected by Managed File Transfer
Connection Successful	FTP, FTPS, SFTP	- Connection was successful to Managed File Transfer
Create Folder Failed	HTTPS, FTP, FTPS, SFTP	- Web User does not have Create Directory permission - Folder name contains invalid characters
Create Folder Successful	HTTPS, FTP, FTPS, SFTP	- Folder creation was successful
Delete File Failed	HTTPS, FTP, FTPS, SFTP	- Files were not successfully deleted - Web User does not have Delete Files permissions - File no longer exists
Delete File Successful	HTTPS, FTP, FTPS, SFTP	- Files are successfully deleted
Delete Folder Failed	HTTPS, FTP, FTPS, SFTP	- Folder was not deleted successfully - Web User does not have Delete Directories permissions - Folder no longer exists
Delete Folder Successful	HTTPS, FTP, FTPS, SFTP	- Folder deletion was successful
Disconnect	FTP, FTPS, SFTP	- A Web User disconnects from Managed File Transfer

Event Name	Service	Executed When (Examples)
Download Failed	HTTPS, FTP, FTPS, SFTP	- A file fails to download (lost connection, file corrupt, etc.) - Web User does not have Download permissions
Download Successful	HTTPS, FTP, FTPS, SFTP	- A file downloads successfully
IP Address Blacklisted	HTTPS, FTP, FTPS, SFTP	- IP address is included in the Automatic IP Blacklist
Invitation Failed	HTTPS	- An invitation will fail when the email address is restricted due to policy restrictions. - Web User enters an invalid email address.
Invitation Successful	HTTPS	- An invitation email was sent to a recipient.
Login Failed	HTTPS, AS2, FTP, FTPS, SFTP	- Web User typed incorrect username - Web User typed incorrect password - Web User account is disabled or expired
Login Successful	HTTPS, AS2, FTP, FTPS, SFTP	- Successful authentication by a Web User
MLLP Commit Receive Failed	MLLP	- MLLP Message rejected by the backend system
MLLP Commit Receive Successful	MLLP	- MLLP Message successfully received by the backend system
MLLP Message Receive Failed	MLLP	- MLLP Message rejected
MLLP Message Receive Successful	MLLP	- MLLP Message successfully received
Not Logged In*	HTTPS, AS2, FTP, FTPS, SFTP	- A Web User tried to access a direct URL on the Managed File Transfer server before logging in - A Web User tried to use the Managed File Transfer interface after exceeding the Session Timeout period for inactivity
Package Create Failed*	HTTPS	- Secure Mail package creation failed
Package Create Successful*	HTTPS	- Secure Mail package creation was successful
Package Delete Failed*	HTTPS	- Secure Mail package could not be deleted - Package no longer exists
Package Delete Successful*	HTTPS	- Secure Mail package successfully deleted
Package Read Failed*	HTTPS	- Secure Mail package could not be read - Package no longer exists
Package Read Successful*	HTTPS	- Secure Mail package read successfully

Event Name	Service	Executed When (Examples)
Package Revoke Failed*	HTTPS	- Secure Mail package could not be revoked
Package Revoke Successful*	HTTPS	- Secure Mail package successfully revoked
Recipient Email Failed*	HTTPS	- The recipient's email address is invalid - Managed File Transfer was unable to send the Secure Mail notification
Recipient Email Successful*	HTTPS	- The Secure Mail notification was delivered successfully
Registration Failed	HTTPS	- Invalid email domain - Incorrect or expired validation code - Password does not meet password requirements
Registration Successful	HTTPS	- Self-registration process is successful
Rename File Failed	HTTPS, FTP, FTPS, SFTP	- Web User does not have Rename Files permission - New name contains invalid characters or extension
Rename File Successful	HTTPS, FTP, FTPS, SFTP	- Renaming a file is successful
Rename Folder Failed	HTTPS, FTP, FTPS, SFTP	- Web User does not have Rename Directories permission - New name contains invalid characters
Rename Folder Successful	HTTPS, FTP, FTPS, SFTP	- Renaming a folder is successful
Share Failed*	HTTPS	- Web User does not have permission to share file or folder with recipient email address - Web User does not have permission to share file or folder with unregistered users
Share Successful*	HTTPS	- Web User successfully shared file or folder
Upload Failed	HTTPS, FTP, FTPS, SFTP	- File name contains invalid characters - File name exceeds 128 characters - Web User does not have Upload permission - File exceeds maximum file size - File extension not permitted
Upload Successful	HTTPS, FTP, FTPS, SFTP	- File upload is successful

Trigger Event Variables

The following table lists the available Trigger Event Variables and their definitions. The variable values are populated when Triggers are run.

Note: The variables displayed in each drop-down list are dynamic to the selected Event Type. Not all variables are available for all events.

Variable Name	Variable Definition
event.ackType	The acknowledgement type associated with the message that caused the event.
event.messageID	The message ID associated with the message that caused the event.
event.systemName	The name of the system that processed the event.
event.userName	The user name of the Web User.
event.user.firstname	The first name of the Web User.
event.user.lastname	The last name of the Web User.
event.user.email	The email address of the Web User.
event.user.phone	The phone number of the Web User.
event.user.description	The description of the Web User.
event.user.organization	The organization of the Web User.
event.user.loginDirectory	The home directory of the Web User.
event.localAddress	The IP address of the service connected to.
event.localPort	The port number of the service connected to.
event.remoteAddress	The remote IP address of the Web User.
event.remotePort	The remote port address of the Web User.
event.physicalPath	The physical path of the file or folder (for example, C:\<installdirectory> \userdata\webdocs\<webuser>\file.txt).
event.physicalFolder	The physical folder name.
event.virtualPath	The virtual path of the file or folder (for example, ../pub/programs/mft/).
event.virtualFolder	The virtual folder name.
event.file	Contains the Shared Drive file
event.fileName	The file name.
event.fileSize	The file size.

Variable Name	Variable Definition
event.package	Contains the details of the Secure Mail package.
event.package.subject	The subject line of the Secure Mail package.
event.package.message	The message body of the Secure Mail package.
event.package.fromAddress	The email address of the sender.
event.package.toAddress	The email addresses for the recipients in a comma delimited list.
event.package.toAddressList	The email addresses for the recipients in a list.
event.package.attachmentCount	The number of attachments on a Secure Mail package.
event.package.attachmentList	All of the attachments on a Secure Mail package.
event.package.protectionLevel	The code for the protection level of the Secure Mail package. - UURL - PPassword - CCertified Delivery
event.package.passwordGeneration	If the protection level is Password, then this is the code for how the password was generated. - SSystem created - MManually created by the Web User
event.package.sendPassword	Indicates if the password is included in the email for password protected packages.
event.package.maxDownloads	The number of downloads allowed per attachment per recipient, -1 for unlimited downloads.
event.package.expiresAfterDays	The number of days from the day the Secure Mail package was sent before it expires, -1 for unlimited.
event.package.expiresOn	The date the Secure Mail package will expire in ISO format, or empty if there is no expiration date.
event.package.replyAllowed	Indicates if the recipient can reply anonymously (without having a Web User account).
event.package.id	The ID of the Secure Mail Package.
event.toPhysicalPath	The physical path of the file or folder being renamed to.
event.toPhysicalFolder	The physical directory being renamed to.
event.toVirtualPath	The virtual path of the file or folder being renamed to.
event.toVirtualFolder	The virtual directory being renamed to.
event.remarks	The remarks attribute of the command.
event.id	The ID of the Event.

Variable Name	Variable Definition
event.as2.messageId	The AS2 Message ID.
event.as2.fromId	The AS2 From ID.
event.as2.toId	The AS2 To ID.
event.as2.subject	The AS2 subject.
event.as2.encryptionAlgorithm	The AS2 encryption algorithm.
event.as2.signatureAlgorithm	The AS2 signature algorithm.
event.as2.compressed	Indicates if the AS2 message was compressed.
event.as2.fileList	The uploaded files in a File List.
event.as2.mdnType	Indicates if the AS2 *MDN* was synchronous or asynchronous.
event.as2.mdnSigned	Indicates if the AS2 MDN was signed.
event.as2.mdnSent	Indicates if the AS2 MDN was sent.
event.as2.mic	The AS2 MIC.
event.as2.micAlgorithm	The AS2 MIC algorithm.
event.as2.physicalFolder	The AS2 physical folder location.
event.as2.physicalFilePaths	The AS2 physical path(s) to the file(s) (for example, [installdirectory]\userdata \webdocs\[webuser]\file.txt). If more than one file is sent, each path is listed on a new line using a CRLF delimiter. This variable can be passed to Managed File Transfer to process the files.
event.as2.virtualFolder	The AS2 virtual folder location.
event.as2.virtualFilePaths	The AS2 virtual path(s) to the file(s) (for example, /[webuser]/file.txt). If more than one file is sent, each path is listed on a new line using a CRLF delimiter. This variable can be passed to Managed File Transfer to process the files.
event.mdn.originalMessageId	The Original Message ID attribute
event.mdn.fromId	The From ID
event.mdn.toId	The To ID
event.mdn.subject	The Subject
event.mdn.signatureAlgorithmName	The signature algorithm
event.mdn.type	Indicates if the MDN was synchronous or asynchronous
event.mdn.signed	Indicates if the MDN was signed
event.mdn.receivedMic	The MIC received attribute

Variable Name	Variable Definition
event.mdn.receivedMicAlgorithm	The MIC received algorithm attribute
event.systemName	The name of the system that the trigger is being executed on
event.mdn.receiptText	The message included in the MDN
system.environment	The value of this variable will be the name for this environment as specified in the "Global Settings" on page 752.
system.emptyString	The value of this variable will be an empty string. This is not an Event Variable.

Advanced Network Shares Configuration

Advanced settings and options are available for configuring some connections to a Network Share using the SMB/CIFS protocol. If the standard options available in the "Network Shares" on page 52 resource do not make the desired connection, the properties for the network shares connection can be defined using a configuration file. The jcifs.properties file for the custom configuration of a Network share is located in the [installdirectory]\config folder.

The jcifs.properties file uses a key=value format. If a specific value is required for a key/parameter, type one key and its value per line.

For example, jcifs.encoding=UTF-8

Common Properties	Definition
jcifs.smb.client.username	The username to use for the connection.
jcifs.smb.client.password	The password to use for the connection.
jcifs.smb.client.domain	The authentication domain to use for the connection.
jcifs.netbios.wins	The IP address of the WINS server. This is only required when accessing hosts on different subnets.
jcifs.netbios.baddr	The local network's broadcast address. It may be necessary to set this for certain network configurations.
jcifs.netbios.scope	NetBIOS provides for a "scope id" to be used in a attempt to conceal groups of machines on the same network.
jcifs.smb.client.laddr	The IP address of the local interface the client should bind to if it is different from the default.
jcifs.netbios.laddr	The IP address of the local interface the client should bind to for name queries if it is different from the default.

Common Properties	Definition
jcifs.netbios.lmhosts	The path to an lmhosts file containing a map of IP addresses to hostnames. The format of this file is identical to that of the Windows lmhosts file format.
jcifs.smb.client.disablePlainTextPasswords	Plain text passwords are not recommended and disabled by default. To enable plain text passwords, set this property to false.
jcifs.encoding	The default encoding is Cp850 (MS-DOS Latin 1).
jcifs.smb.client.useExtendedSecurity	Older versions of Samba do not support this property and in those cases the value should be set to false.

Enhanced Properties	Definition
jcifs.resolveOrder	The name resolution method identifiers, separated by commas, that specify which methods will be used to resolve hostnames. The possible identifiers in default order are LMHOSTS, WINS, BCAST, and DNS.
jcifs.util.loglevel	0 - No log messages are printed. 1 - Only critical messages are logged (default level). 2 - Critical and some Event messages are logged. 3 - Almost everything is logged. N - Debugging log level.
jcifs.smb.client.attrExpirationPeriod	The time in milliseconds that the attributes of a file are cached (default 5000). To turn off attribute expiration, set the value to 0.
jcifs.smb.client.responseTimeout	The time in milliseconds that the client will wait for a response to a request from the server (default 30000). Increase this value if network conditions are poor.
jcifs.smb.client.soTimeout	The time in milliseconds the server will keep a socket open for activity (default 35000). If the responseTimeout value was increased, adjust this value accordingly.
jcifs.netbios.cachePolicy	The time in seconds that a NetBIOS name is cached (default 30). Set the value to 0 to disable caching and set the value to -1 to retain the cache.
jcifs.netbios.hostname	This property will force port 139 rather than the default port 445.
jcifs.smb.client.listSize	The byte size of the data buffer (default 65535). High latency networks may perform better with a value below the MTU (1200).
jcifs.smb.client.listCount	The maximum number of directory and file entries returned with each request (default 200).
jcifs.smb.client.lport	Specify a local port, if needed, for socket communications. This has no effect on the remote port - 139.
jcifs.netbios.soTimeout	The time in milliseconds (default 5000), the datagram socket used for nameservice queries is left open.
jcifs.netbios.lport	Specify a local port, if needed, for socket communications.

Enhanced Properties	Definition
jcifs.netbios.retryCount	The number of times a name query is made if no answer is received (default 2). Consider increasing the jcifs.netbios.retryTimeout instead.
jcifs.netbios.retryTimeout	The time in milliseconds the client will wait for a response to a name query (default 3000).
jcifs.http.domainController	The DNS hostname or IP address of a server that should be used to authenticate HTTP clients with the NtlmSsp class.
jcifs.http.basicRelm	The realm for basic authentication (default 'jCIFS').
jcifs.http.enableBasic	To enable basic authentication over HTTPS, set this value to true.
jcifs.http.insecureBasic	To enable basic authentication over HTTP, set this property to true. This configuration passes user credentials in plain text over the network.
jcifs.smb.lmCompatibility	0,1 - Sends LM and NTLM responses. Use 0 for older Samba. 2 - Sends only the NTLM response. 3,4,5 -- Sends LMv2 and NTLMv2 data (default). These values mirror those used with the Windows registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
jcifs.smb.client.ssnLimit	The number of sessions open per transport (default 250). Setting the value too high may result in ERRSVR/90: Too many Uids active on this session.
jcifs.smb.client.signingPreferred	If SMB signing is required or supported, set this vale to true. Signing is required by default with Windows 2003 and later.
jcifs.http.loadBalance	If a jcifs.smb.client.domain value is specified (and domainController is not specified) the NtlmHttpFilter will query for domain controllers by name. The filter will rotate through the list of domain controllers when authenticating users (default value is true). The jcifs.netbios.lookupRespLimit property can also be used to limit the number of domain controllers used.
jcifs.netbios.lookupRespLimit	Limits the range of servers returned by the 0x1C NetBIOS name query (default 5).
jcifs.smb.client.logonShare	The shared name against which SmbSession.logon() authenticates users (default IPC$). Changing the value can be used to create simple group based access control for the NtlmHttpFilter or other applications that use SmbSession.logon().
jcifs.smb.client.dfs.disabled	When used in a non-domain environment set this value to true (default false).

Enhanced Properties	Definition
jcifs.smb.client.dfs.ttl	The time in seconds that DFS topology information should be cached (default 300).
jcifs.smb.client.dfs.strictView	A list of shares is returned even if DFS roots are not enumerated (default). If set to true, an error is logged if DFS information cannot be successfully retrieved.

Advanced Properties	Definition
jcifs.smb.client.nativeOs	The NativeOS field. The default is the os.name system property.
jcifs.smb.client.nativeLanMan	Specifies the NativeLanMan field in the SMB_COM_SESSION_SETUP_ANDX request.
jcifs.smb.client.maxMpxCount	The number of simultaneous outstanding transactions with a given server (default 10).
jcifs.smb.client.useNTSmbs	This value is rarely set.
jcifs.smb.client.useUnicode	The client uses Unicode strings, unless set to false and then will only use 8 bit strings (although Unicode will still be used to accommodate a few protocol bugs).
jcifs.netbios.client.writeSize	The buffer size in bytes used by the NetBIOS Socket layer to write data to the raw socket (default 1500).
jcifs.smb.client.flags2	The flags2 field of the SMB header.
jcifs.smb.client.capabilities	The capabilities field of the SMB_COM_SESSION_SETUP_ANDX command.
jcifs.smb.client.rcv_buf_size	The buffer size in bytes for decoding incoming packets (default 60416).
jcifs.smb.client.snd_buf_size	The buffer size in bytes for encoding outgoing packets (default 16644).
jcifs.smb.client.serviceType	Service types can be A:, LPT1:, IPC, and COMM.
jcifs.smb.client.<smb_ident>.<smb_ident>	Batching (chaining) requires an integer batch level for a pair of SMB messages.
jcifs.smb.client.useBatching	Batching is turned off by setting this value to false (default true).
jcifs.smb.client.tcpNoDelay	SMB transport sockets will call setTcpNoDelay if the value is set to true. The default value is false (Nagle's algorithm is enabled).
jcifs.smb.client.transaction_buf_size	The maximum SMB transaction buffer size. The default is 0xFFFF - 512.
jcifs.smb.maxBuffers	The maximum number of of jcifs.smb.client.transaction_buf_size buffers that the buffer cache will create (default 16).

NT Retry Status Codes

Informatica Managed File Transfer can retry failed "Network Shares" on page 52 connections based on predefined NT status codes (below). The predefined status codes can be overwritten by using the Retry Status Code property.

Retry Status Code Property	Definition
jcifs.ext.smb.retryNtStatusCodes	Specify the NT status value(s) or hex code(s) that will be used to retry failed connections. When values are specified, the default retry status codes are ignored. Separate each value with a comma. Example: jcifs.ext.smb.retryNtStatusCodes=0xC00000AB,0xC00000AC

The following table contains the default NT Retry Status codes:

Value	Code	Definition
NT_STATUS_PIPE_BUSY	0xC00000ae	All pipe instances are busy.
NT_STATUS_PIPE_BROKEN	0xC000014b	The pipe has been ended.
NT_STATUS_PIPE_CLOSING	0xC00000b1	The pipe is being closed.
NT_STATUS_PIPE_DISCONNECTED	0xC00000b0	No process is on the other end of the pipe.
NT_STATUS_PIPE_NOT_AVAILABLE	0xC00000ac	All pipe instances are busy.
NT_STATUS_PIPE_LISTENING	0xC00000b3	Waiting for a process to open the other end of the pipe.
NT_STATUS_PATH_NOT_COVERED	0xC0000257	The remote system is not reachable by the transport.
NT_STATUS_REQUEST_NOT_ACCEPTED	0xC00000d0	No more connections can be made to this remote computer at this time because there are already as many connections as the computer can accept.
NT_STATUS_BAD_NETWORK_NAME	0xC00000cc	The network name cannot be found.
NT_STATUS_NETWORK_NAME_DELETED	0xC00000c9	The specified network name is no longer available.
NT_STATUS_UNSUCCESSFUL	0xC0000001	A device attached to the system is not functioning.
NT_STATUS_INVALID_HANDLE	0xC0000008	The handle is invalid.

Email Templates

Managed File Transfer sends emails for various administrator and Web User functions. The notifications are based on email templates that communicate the relevant information to the recipient. The templates are defined in XML files and stored in a repository located at [installdirectory]/proddata/emailtemplates.

The templates can be modified to meet your specifications using an XML or a plain text editor. Email templates can use "Functions" on page 131 to perform various operations on variables, strings and data. If

you would like to make changes to an email template, copy the template file from [installdirectory]/proddata/emailtemplates/[templatetype] and save it to [installdirectory]/userdata/emailtemplates/[templatetype]. Only make changes to the templates in the /userdata folder. The email templates located in /proddata will be overwritten during upgrades. When using an email template, Managed File Transfer first looks for an email template in the /userdata folder before using the email template from the /proddata folder.

Note: Emails are sent using the settings on the SMTP tab of the "Global Settings" on page 752 page.

Template Structure

Each template follows the same basic structure. The template contains a title, a brief summary of the email, any relevant information attachments, or links, and then a disclaimer/footer. The variables used in each template are populated with their corresponding values when the messages are generated and sent.

Email Template (XML Schema)

The email templates must conform to the following XML schema. A validation error occurs if a template does not conform to the schema below:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:complexType name="EmailAddress">
<xs:attribute name="name" />
<xs:attribute name="address" use="required" />
</xs:complexType>
<xs:complexType name="Attachment">
<xs:attribute name="name" />
<xs:attribute name="file" use="required" />
</xs:complexType>
<xs:complexType name="EmailTemplate">
<xs:sequence>
<xs:element name="from" type="EmailAddress" minOccurs="0" />
<xs:element name="to" type="EmailAddress" minOccurs="1" maxOccurs="unbounded" />
<xs:element name="cc" type="EmailAddress" minOccurs="0" maxOccurs="unbounded" />
<xs:element name="bcc" type="EmailAddress" minOccurs="0" maxOccurs="unbounded" />
<xs:element name="subject" />
<xs:element name="contentType" minOccurs="0" default="text/plain" />
<xs:element name="message" />
<xs:element name="attachment" type="Attachment" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
<xs:element name="emailTemplate" type="EmailTemplate" />
</xs:schema>
```

Template XML Schema Defined

The email template schema ensures the following:

1. The "root" element must be emailTemplate.
2. The "from" element is optional, but if it is specified, it must be the first element. If not specified, the email engine uses the From Name and Address from the Managed File Transfer Global Settings.
3. Must have at least one "to" element. Multiple "to" elements are permitted and will send the email to more than one recipient.
4. The "to" element may be followed by one or more "cc" or "bcc" elements. The "cc" element must be defined before the "bcc" element.
5. There must be one "subject" element.
6. If required, a "contentType" may be specified. The default is "text/plain."

7. There must be one "message" element that contains the body text for the email.
8. Optionally, there could be one or more "attachment" elements.
   The schema also defines two data types for EmailAddress and Attachment. The EmailAddress data type is used by the "from," "to," "cc" and "bcc" elements. Each of these elements must contain the address attribute. These elements may also define a name attribute which is the person's name.

   The Attachment data type, must define the file attribute and an optional name attribute. If a "name" attribute is not specified, it defaults to the name of the file defined using the file attribute. The file attribute may contain an absolute path or a relative path. Relative paths are resolved relative to the installation directory of the product.

Web User Email Templates

Managed File Transfer sends emails for Secure Mail, Self-Registration and other various functions related to the management of Web User accounts. The templates are defined in XML files and stored in a repository located at [installdirectory]/proddata/emailtemplates.

If you would like to make changes to an email template, copy the template file from [installdirectory]/proddata/emailtemplates and save it to [installdirectory]/userdata/emailtemplates.

The available variables for each Web User Email template are detailed below:

CertifiedDelivery.xml

The notification message sent to a Package recipient when the Package was sent Certified Delivery.

Variable	Description
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:files	This variable lists the files attached to the Package when an email is only sent in plain text.
package:filesHTML	The list of files in the Package.
package:invite	If the package contains an invitation to register, this variable displays true. Otherwise the variable displays false.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:recipient:address	The recipient of the Package.
package:sender:address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject line of the Package message.

Variable	Description
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

ForgotPassword.xml

The verify password reset request message sent to a user after clicking the Forgot Password? link on the File Transfer Portal login page.

Variable	Description
site:url	The URL of the Managed File Transfer server.
webuser:email	The Web User's email address.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

InvitationRequest.xml

The email sent to a new user inviting them to register to use the Managed File Transfer secure file server.

Variable	Description
invitation:expiresAfter	The link sent to the new user is valid for the number of hours specified by the Email Verification Grace Period setting on the "Web User Self-Registration" on page 645 page.
invitation:recipient	The address of the person being invited.
invitation:siteName	This is the site name for the Managed File Transfer instance. It is the same name as the Page Title in the "HTTPS Configuration" on page 521.
invitation:url	Each recipient receives a unique URL with which to register.
invitation:webUser:emailAddress	The email address of the Web User who made the invitation.
invitation:webUser:firstName	The first name of the Web User who made the invitation.
invitation:webUser:fullName	The full name (first name and last name) of the Web User who made the invitation.
invitation:webUser:lastName	The last name of the Web User who made the invitation.
invitation:webUser:organization	The organization of the Web User who made the invitation.
invitation:webUser:phone	The Web User's phone number.

Variable	Description
invitation:webUser:userName	The account name of the Web User who invited the user.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

NewWebUserAccount.xml

The new account message sent to a new Web User.

Variable	Description
webuser:email	The Web User's email address.
webuser:name	The Web User's account/login name.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

NewWebUserPassword.xml

The new password message sent to a new Web User.

Variable	Description
webuser:email	The Web User's email address.
webuser:password	The Web User's password.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

PackagePassword.xml

The notification message sent to a Package recipient when the Package is password protected, and the password is included in a separate email.

Variable	Description
package:password	The password that will open the package.
package:recipient:address	The recipient of the Package.
package:sender:address	The email address of the Web User who sent the Package.

Variable	Description
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject line of the Package message.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

PackageReadNotification.xml

The notification message sent to a Package sender when the recipient reads the Package.

Variable	Description
readNotification:recipient	The email of the notification recipient.
readNotification:sender	The email address of notification sender.
readNotification:siteUrl	The URL of the Managed File Transfer server.
readNotification:subject	The subject line of the message.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

PasswordPackageWithoutPasswordWithFiles.xml

The notification message sent to a Package recipient when the Package is password protected, the password is not included in the email and files are included in the Package.

Variable	Description
package:downloadLimit	The number of times the package is allowed to be downloaded.
package:downloadLimitSet	If a package download limit is set, this variable displays true. Otherwise the variable displays false.
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:files	This variable lists the files attached to the Package when an email is only sent in plain text.
package:filesHTML	The list of files in the Secure Mail Package.

Variable	Description
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:recipient:address	The recipient of the Package.
package:sender.address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject line of the Package message.
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

PasswordPackageWithoutPasswordWithoutFiles.xml

The notification message sent to a Package recipient when the Package is password protected, the password is not included in the email and the Package only contains a secure message.

Variable	Description
package:downloadLimit	The number of times the package is allowed to be downloaded.
package:downloadLimitSet	If a package download limit is set, this variable displays true. Otherwise the variable displays false.
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:recipient:address	The recipient of the Package.
package:sender.address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject line of the Package message.

Variable	Description
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

PasswordPackageWithPasswordWithFiles.xml

The notification message sent to a Package recipient when the Package is password protected, the password is included in the email and files are included in the Package.

Variable	Description
package:downloadLimit	The number of times the package is allowed to be downloaded.
package:downloadLimitSet	If a package download limit is set, this variable displays true. Otherwise the variable displays false.
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:files	This variable lists the files attached to the Package when an email is only sent in plain text.
package:filesHTML	The list of files in the Secure Mail Package.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:password	The password that will open the Package.
package:recipient:address	The recipient of the Package.
package:sender:address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject of the message.
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

PasswordPackageWithPasswordWithoutFiles.xml

The notification message sent to a Package recipient when the Package is password protected, the password is included in the email and the Package only contains a secure message.

Variable	Description
package:downloadLimit	The number of times the package is allowed to be downloaded.
package:downloadLimitSet	If a package download limit is set, this variable displays true. Otherwise the variable displays false.
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:password	The password that will open the Package.
package:recipient:address	The recipient of the Package.
package:sender:address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject of the message.
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

ResetWebUserPassword.xml

The message sent to a Web User after their password was reset.

Variable	Description
webuser:email	The Web User's email address.
webuser:password	The Web User's password.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

SendPackageReceipt.xml

The message placed in the Outlook Sent Items folder after a Secure Mail Package is sent using the Outlook plugin.

Variable	Description
package:files	The list of files included in the Secure mail Package, displayed in plain text format.
package:filesHTML	The list of files included in the Secure Mail Package, displayed in HTML format.
package:packageId	The Package's 36-character ID number.
package:recipients	The email address to whom the Secure Mail message was sent, displayed in plain text format.
package:recipientsHTML	The email address to whom the Secure Mail message was sent, displayed in HTML format.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:sentOn	The date and time the Secure Mail message was submitted.
package:subject	The subject line of the Secure Mail message.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

ShareVirtualFile.xml

The notification message sent to a recipient when a virtual file or folder is shared.

Variable	Description
fileType	They type of item shared, either file or folder.
message	The message that was supplied by the sender.
invite	If an invitation was sent, this variable displays true. Otherwise, the recipient already has an account and the variable displays false.
recipientAddress	The recipient of the virtual file or folder invite.
senderAddress	The email address of the sender.
subject	The subject line of the message.
url	The URL a recipient will click to access the file or folder.

Variable	Description
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

URLPackageNotificationWithFiles.xml

The notification message sent to a Package recipient when the Package is URL protected and files are included in the Package.

Variable	Description
package:downloadLimit	The number of times the package is allowed to be downloaded.
package:downloadLimitSet	If a package download limit is set, this variable displays true. Otherwise the variable displays false.
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:files	This variable lists the files attached to the Package when an email is only sent in plain text.
package:filesHTML	The list of files in the Secure Mail Package.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:recipient:address	The recipient of the Package.
package:sender:address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject of the message.
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

URLPackageNotificationWithoutFiles.xml

The notification message sent to a Package recipient when the Package is URL protected and the Package only contains a message.

Variable	Description
package:downloadLimit	The number of times the package is allowed to be downloaded.
package:downloadLimitSet	If a package download limit is set, this variable displays true. Otherwise the variable displays false.
package:expirationDateInMillis	The number of milliseconds before the package expires after it has been sent.
package:expirationInDays	The number of days before the package expires after it has been sent.
package:expirationLimitSet	If a package expiration is set, this variable displays true. Otherwise the variable displays false.
package:message	This variable displays the Package message in plain text.
package:messageHTML	This variable displays the Package message formatted for HTML.
package:recipient:address	The recipient of the Package.
package:sender:address	The email address of the Web User who sent the Package.
package:sender:name	The username of the Web User who sent the package.
package:subject	The subject of the message.
package:url	The URL a recipient will click to receive the Package contents.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

WebUserApproved.xml

The notification message sent to a new Web User when their account is approved.

Variable	Description
site:url	The URL of the Managed File Transfer server.
webuser:email	The Web User's email address.
webuser:firstName	The first name of the Web User.
webuser:lastName	The last name of the Web User.
webuser:name	The Web User's account/login name.

Variable	Description
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

WebUserPasswordExpirationEmail.xml

The notification message sent to a Web User when their account password is about to expire.

Variable	Description
expiration:date	The expiration date of the Web User account .
site:url	The URL of the Managed File Transfer server.
webuser:email	The Web User's email address.
webuser:firstName	The first name of the Web User.
webuser:lastName	The last name of the Web User.
webuser:name	The Web User's account/login name.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

WebUserPendingRegistrationNotification.xml

The message sent to users with the Web User Manager role when a new Web User account needs approval.

Variable	Description
registration:invitedBy	If the new user was invited, this is the Web User account name that made the invitation.
registration:invitedOn	If the new user was invited, this the timestamp of when the invitation was sent.
users:webUserManagerEmails	The list of email addresses for all members of the Web User Manager role.
webuser:email	The Web User's email address.
webuser:firstName	The first name of the Web User.
webuser:lastName	The last name of the Web User.
webuser:name	The Web User's account/login name.
webuser:organization	The company of the Web User.

Variable	Description
webuser:phone	The phone number of the Web User.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

WebUserRegistrationNotification.xml

The message sent to users with the Web User Manager role when a new Web User account is created via the self-registration process.

Variable	Description
registration:invitedBy	If the new user was invited, this is the Web User account name that made the invitation.
registration:invitedOn	If the new user was invited, this the timestamp of when the invitation was sent.
users:webUserManagerEmails	The list of email addresses for all members of the Web User Manager role.
webuser:email	The Web User's email address.
webuser:firstName	The first name of the Web User.
webuser:lastName	The last name of the Web User.
webuser:name	The Web User's account/login name.
webuser:organization	The company of the Web User.
webuser:phone	The phone number of the Web User.
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

WebUserRegistrationVerifyEmail.xml

The message sent to Web Users to verify their email during the self-registration process.

Variable	Description
registration:email	The email address used by the Web User when self-registering.
registration:token	The unique code that is sent to verify the email account.
registration:url	The URL of the Managed File Transfer server.

Variable	Description
system:name	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
system:environmentName	The environment name defined on the "Global Settings" on page 752 page.

Shared Drive Email Templates

Shared Drive sends emails to Web Users when certain activities occur with the service. The templates are defined in XML files and stored in a repository located at [installdirectory]/proddata/emailtemplates/shareddrive.

If you would like to make changes to an email template, copy the template file from [installdirectory]/proddata/emailtemplates/shareddrive and save it to [installdirectory]/userdata/emailtemplates/shareddrive.

The available variables for each Shared Drive Email template are detailed below:

CommentNotification.xml

The notification message sent to the file owner when another user comments on a file the owner has shared.

Variable	Description
event:recipientProfile:email	The email address for the recipient of the notification.
event:subscribedItemName	The name of the item that was shared.
event:senderProfile:displayName	The name of the user who made the comment on the shared item.
event:file:fileName	The name of the file that had been commented on.
event:isSharedItem	Determines if the item was shared to another user.
event:comment	The comment that was made to the shared item.
site:url	The File Transfer Portal Site URL defined on the HTTPS Settings page.

DeleteNotification.xml

The notification message sent to the file owner when another user deletes a file the owner has shared.

Variable	Description
event:recipientProfile:email	The email address for the recipient of the notification.
event:subscribedItemName	The name of the item that was shared.
event:senderProfile:displayName	The name of the user who deleted the shared item.
event:filesHTML	The list of files that had been deleted.

Variable	Description
event:isSharedItem	Determines if the item was shared to another user.
site:url	The File Transfer Portal Site URL defined on the HTTPS Settings page.

DownloadVerification.xml

The notification message sent to the file owner when another user downloads a file the owner has shared.

Variable	Description
event:recipientProfile:email	The email address for the recipient of the notification.
event:subscribedItemName	The name of the item that was shared.
event:senderProfile:displayName	The name of the user who downloaded the file.
event:filesHTML	The list of files that were downloaded by the other user.
event:isSharedItem	Determines if the item was shared to another user.
site:url	The File Transfer Portal Site URL defined on the HTTPS Settings page.

ShareFile.xml

The notification message sent to a user when an item has been shared with them.

Variable	Description
recipientAddress	The email address for the recipient of the notification.
subject	The subject the Web User entered on the Share File or Folder page in the File Transfer Portal.
fileType	Determines the type of item shared, either File, file, or folder.
senderAddress	The email address of the user who shared the item.
invite	Determines if the recipient is a registered user.
message	The message the Web User entered on the Share File or Folder page in the File Transfer Portal.
url	The URL to access the shared item.
acceptURL	The URL a Web Users selects to accept the shared item. The shared item willl appear in the Web User's root Shared Drive directory.
denyURL	The URL a Web User selects to deny the shared item.

Upload Notification.xml

The notification message sent to the file owner when another user uploads a new version of the shared file(s).

Variable	Description
event:recipientProfile:email	The email address for the recipient of the notification.
event:subscribedItemName	The name of the item that was shared.
event:senderProfile:displayName	The name of the user who uploaded a new version of the shared item.
event:isSharedItem	Determines if the item was shared to another user.
event:filesHTML	The list of files that were uploaded by the other user.
site:url	The File Transfer Portal Site URL defined on the HTTPS Settings page.

Project Email Templates

Managed File Transfer can send notification emails to specified recipients based on the success or failure of a Scheduled Job or Monitor. The templates are defined in XML files under the [installdirectory]/proddata/emailtemplates folder where [installdirectory] is the installation directory of the Managed File Transfer product.

The FailedMonitor.xml and MonitorNoFilesFound.xml variables reference the Monitor module and are prefixed with monitor (for example, ${monitor:formattedStartTime}). The variables at the Job level reference the Job module and are prefixed with job (for example, ${job:projectLocation}).

Detailed below are the variables available for each Project Email template:

Monitor Related Variables

FailedMonitor.xml

Variable	Description
monitor:onFailureEmails	The list of email addresses that receive notice when a Monitor fails.
monitor:name	The name of the Monitor.
monitor:exception:message	The error message generated by the exception that caused the error.
monitor:formattedStartTime	The time the monitor started. The time is formatted based on the Time Pattern defined in Global Settings.
monitor:formattedEndTime	The time the monitor ended. The time is formatted based on the Time Pattern defined in Global Settings.

MonitorNoFilesFound.xml

Variable	Description
monitor:noFilesFoundEmails	The list of email addresses that receive notice when a Monitor fails.
monitor:name	The name of the Monitor.
monitor:exception:message	The error message generated by the exception that caused the error.
monitor:formattedStartTime	The time the monitor started. The time is formatted based on the Time Pattern defined in Global Settings.
monitor:formattedEndTime	The time the monitor ended. The time is formatted based on the Time Pattern defined in Global Settings.

Job Related Variables

FailedMonitorJob.xml

Variable	Description
job:onFailureEmails	The list of email addresses that receive notice when a job fails.
job:jobName	The name of the monitor that started the job.
job:jobNumber	The number of the job.
job:projectLocation	The full Project path and file name.
job:runUser	The user that started the job.
job:formattedStartTime	The time the job started. The time is formatted based on the Time Pattern defined in Global Settings.
job:formattedEndTime	The time the job ended. The time is formatted based on the Time Pattern defined in Global Settings.

FailedScheduledJob.xml

Variable	Description
job:onFailureEmails	The list of email addresses that receive notice when a job fails.
job:jobName	The name of the scheduled job that started this job.
job:jobNumber	The number of the job.
job:projectLocation	The full Project path and file name.

Variable	Description
job:runUser	The user that started the job.
job:formattedStartTime	The time the job started. The time is formatted based on the Time Pattern defined in Global Settings.
job:formattedEndTime	The time the job ended. The time is formatted based on the Time Pattern defined in Global Settings.

SuccessfulMonitorJob.xml

Variable	Description
job:onSuccessEmails	The list of email addresses that receive notice when a job completes successfully.
job:jobName	The name of the monitor that started the job.
job:jobNumber	The number of the job.
job:projectLocation	The full Project path and file name.
job:runUser	The user that started the job.
job:formattedStartTime	The time the job started. The time is formatted based on the Time Pattern defined in Global Settings.
job:formattedEndTime	The time the job ended. The time is formatted based on the Time Pattern defined in Global Settings.

SuccessfulScheduledJob.xml

Variable	Description
job:onSuccessEmails	The list of email addresses that receive notice when a job completes successfully.
job:jobName	The name of the scheduled job that started this job.
job:jobNumber	The number of the job.
job:projectLocation	The full Project path and file name.
job:runUser	The user that started the job.
job:formattedStartTime	The time the job started. The time is formatted based on the Time Pattern defined in Global Settings.
job:formattedEndTime	The time the job ended. The time is formatted based on the Time Pattern defined in Global Settings.

System Alert Email Templates

The notifications sent from "System Alerts" on page 776 are based on email templates that communicate the relevant information to the recipient. The templates are defined in XML files and stored in a repository located at [installdirectory]/proddata/emailtemplates/alerts.

If you would like to make changes to an email template, copy the template file from [installdirectory]/proddata/emailtemplates/alerts and save it to [installdirectory]/userdata/emailtemplates/alerts.

The variables available in each System Alert Email template are detailed below:

ClusterMembershipChanges.xml

The notification message sent to Product Administrators and other email recipients when changes occur in an Managed File Transfer Cluster.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
subject	The subject contains a brief description of the cluster change.
message	The message contains a detailed description of the cluster change.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
date	The date and time the cluster change took place.
coordinator	The name of the system that is acting as the cluster Coordinator.
participants	The name of the systems that are cluster Participants.
siteURL	The Admin Site URL defined on the Global Settings page.

GatewayConnected.xml

The notification message sent to Product Administrators and other email recipients when Managed File Transfer™ is connected to Managed File Transfer Gateway™.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
controllerAddress	The IP address and port of the Gateway controller.

Variable	Description
connectedOn	The system time when Managed File Transfer was connected to Gateway.
siteURL	The Admin Site URL defined on the Global Settings page.

GatewayDisconnected.xml

The notification message sent to Product Administrators and other email recipients when Managed File Transfer is disconnected from Managed File Transfer Gateway.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
controllerAddress	The IP address and port of the Gateway controller.
disconnectedOn	The system time when Managed File Transfer was disconnected from Gateway.
siteURL	The Admin Site URL defined on the Global Settings page.

MFTServerShutdown.xml

The notification message sent to Product Administrators and other email recipients when Managed File Transfer is shut down.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the <installdirectory>/config/cluster.xml file.
shutdownOn	The system time when Managed File Transfer was shut down.
siteURL	The Admin Site URL defined on the Global Settings page.

MFTServerStarted.xml

The notification message sent to Product Administrators and other email recipients when Managed File Transfer is started.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the <installdirectory>/config/cluster.xml file.
startedOn	The system time when Managed File Transfer was started.
siteURL	The Admin Site URL defined on the Global Settings page.

JVMMemory.xml

The notification message sent to Product Administrators and other email recipients when Managed File Transfer reaches the minimum JVM memory threshold.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
availableMemoryThreshold	The minimum memory the JVM must reach before an email alert is sent.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
maxMemory	The total amount of JVM memory allocated for Managed File Transfer.
usedMemory	The total amount of JVM memory used for Managed File Transfer.
freeMemory	The total amount of free JVM memory available for Managed File Transfer.
siteURL	The Admin Site URL defined on the Global Settings page.

LicenseExpiring.xml

The notification message sent to Product Administrators and other email recipients when the Managed File Transfer product license is nearing the expiration date.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
expiresOn	The day the Managed File Transfer license expires.
siteURL	The Admin Site URL defined on the Global Settings page.

OpenPGPKeyExpiring.xml

The notification message sent to Key Managers and other email recipients when an Open PGP key is set to expire.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
keyID	The unique hexadecimal identifier for the key.
keyUser	The name and email address of the key's owner.
keyExpiresOn	The date the OpenPGP key will expire.
siteURL	The Admin Site URL defined on the Global Settings page.

SSLCertificateExpiring.xml

The notification message sent to Key Managers and other email recipients when an SSL certificate is set to expire.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.

Variable	Description
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
keyStoreName	The name of the key store that contains the expiring certificates.
keyAlias	The alias of the certificate that is reaching its expiration date.
keyExpiresOn	The certificate expiration date.
siteURL	The Admin Site URL defined on the Global Settings page.

TriggerFailed.xml

The notification message sent to Trigger Managers and other email recipients when a Trigger fails.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
triggerName	The name of the failed trigger.
triggerError	The summary message of the error.
triggerException	The detailed error message recorded for the failure.
siteURL	The Admin Site URL defined on the Global Settings page.

WebUserDeactivated.xml

The notification message sent to Web User Managers and other email recipients when a Web User is deactivated.

Variable	Description
recipients	The recipient(s) of the email alert.
subjectPrefix	The subject line prefix set on the "System Alerts" on page 776 page.
enviornmentName	The environment name defined on the "Global Settings" on page 752 page.
systemName	The system name of the local server as defined in the [installdirectory]/config/cluster.xml file.
userName	The name of the Web User that was deactivated.

Variable	Description
reason	The reason the Web User was deactivated.
deactivatedOn	The date and time the Web User was deactivated.
siteURL	The Admin Site URL defined on the Global Settings page.

MQ Connection URL

When connecting to a Messaging Queue (MQ) server using the MQ Provider Specific option for the connection type, the following properties and keys can be used in the URL string to configure the connection. When using the JNDI (JMS Standard) connection type, the URL is provided by the MQ server administrator.

providerCode:[transportProtocol:]//host[:port][?key1=value1&key2=value2]

Example: wmq:tcp://hostname:1414?queueManager=QM_Test

Provider Code

The provider code indicates the MQ server to which the connection is made.

Provider Name	Provider Code
WebSphere MQ	wmq
SonicMQ	sonicmq
ActiveMQ	activemq

Transport Protocol

The transport protocol is optional. If one is not specified, the MQ server's default is used. Most MQ servers use TCP, but if supported HTTP and HTTPS are valid options.

Host and Port

The host is the name or the IP address of the server. The port number is optional and if not specified will use the MQ server default based on the provider.

Provider Name	Default Port Number
WebSphere MQ	1414
SonicMQ	2506
ActiveMQ	61616

Additional Properties

The following properties can be used to configure the connection parameters to the MQ server. Each set of key-value pairs, as shown in the example above, are case-sensitive and must be separated by an ampersand (&). If a property value contains characters other than letters or numbers, use HTTP URL encoding to represent the character (for example, "%20" is a space and "%7C" is a pipe). A property value can include an ampersand (&) or an equals sign, but within the value they must use their URL encoded value ("%26" is an ampersand and "%3D" is an equals sign).

Websphere MQ Connection Properties

Property Name	Description
queueManager	The name of the Queue Manager.
clientID	The ID assigned to Managed File Transfer (client). This is used as part of the topic's subscription ID.
hostName	Name or IP address of the host MQ server. If specified, this value overrides the value in the host portion of the URL.
port	The port number of the MQ server. If specified, this value overrides the value in the port portion of the URL.
transportType	The type of transport (default 1).
channel	Sets the name of the channel - applies to client transport mode only.
localAddress	The local address to be used. The format of a local address is [IP address or Host Name][(low-port[,high-port])]. Most MQ servers use 4-5 ports, but if an application is having difficulty making connections, increase the number of ports in the range. A host name can be specified instead of an IP address. Local address examples: 9.20.4.98 - The channel binds to 9.20.4.98 locally. 9.20.4.98(1000) - The channel binds to 9.20.4.98 locally and uses port 1000. 9.20.4.98(1000,2000) - The channel binds to 9.20.4.98 locally and uses a port in the range 1000 to 2000. (1000) - The channel binds to port 1000 locally. (1000,2000) - The channel binds to a port in the range 1000 to 2000 locally. Considerations: - Specify a range of ports to allow for connections that are required internally as well as those explicitly used by an application. The number of ports required depends on the application and the facilities it uses. Typically, this is the number of sessions the application uses plus three or four additional ports. If an application is having difficulty making connections, increase the number of ports in the range. - Connection pooling has an effect on how quickly a port can be reused. In JMS, connection pooling is switched on by default and it might be several minutes before a port can be reused. Connection errors might occur in the meantime. - For real-time connections, the local address determines which of the local network interfaces is used for multicast connections. When specifying a local address for a real-time connection, do not include a port number. A port number is not valid for multicast and, if specified, causes a failure at connect time.
maxBufferSize	The maximum number of received messages stored in an internal message buffer (default 1000).

Property Name	Description
proxyHostName	The host name of the proxy server when establishing a real-time connection.
proxyPort	The port number of the proxy server when establishing a real-time connection.

SonicMQ Connection Properties

Property Name	Description
clientID	The ID assigned to Managed File Transfer (client). This is used as part of the topic's subscription ID.
brokerURL	The connection URL of the MQ broker or server. If specified, this value overrides the URL specified in the main portion of the URL.
connectionURLs	Secondary URLs to try if the primary URL cannot be accessed.

ActiveMQ Connection Properties

Property Name	Description
clientID	The ID assigned to Managed File Transfer (client). This is used as part of the topic's subscription ID.
brokerURL	The connection URL of the MQ broker or server. If specified, this value overrides the URL specified in the main portion of the URL.

MQ Message Filters

Message Filters provide an SQL-like syntax to only retrieve MQ messages meeting specific filter criteria in its message header or properties. The remaining messages are left on the MQ server and can be accessed by other applications or additional MQ Retrieve Message Tasks that process a different sub-set of messages.

Multiple message filter strings can be grouped in parenthesis and concatenated with NOT, AND, OR. The message filters are constructed using the following structure:

[Selector Property or Identifier] [Operator] [Literal]

Example: The message filter JMSPriority >=8 AND system = 'production' would only retrieve messages who's priority was greater than or equal to 8 and had a property named system with a value of production.

Selector Property or Identifier

The selector property or identifier (Property Name field value), are the basis for each message filter argument. Identifiers are case-sensitive and the message header field references are limited to: JMSDeliveryMode, JMSPriority, JMSMessageID, JMSTimestamp, JMSCorrelationID, and JMSType.

The JMSMessageID and the JMSCorrelationID identifiers expect an ID number as the literal value. As literal values must start with a letter, prefix the ID numbers for these identifiers with ID:.

Example: JMSMessageID = 'ID:414d5120514d5f736c75656262655f50421e274d20003f02'

Operators

The following operators can be used in the filter argument:

AND	NOT	OR	BETWEEN
LIKE	IN	IS	ESCAPE
IS NULL	IS NOT NULL	+	-
*	/	=	>
>=	<	<=	<>

Literals

Literals can be any sequence of letters or numbers, starting with a letter. All literals that are not numerical (string literal) must be enclosed in single quotes. Use a double single quote to reference a single quote within a string (for example, 'literal''s' = literal's).

Wildcards and Regular Expressions

Both wildcard and regular expression patterns operate by matching and grouping sections of a given string.

Wildcards

Wildcard patterns support two special matching characters, * and ?.

Characters

* - Zero or more characters

? - single character

Wildcard patterns may be used to search and replace characters. Each matched wildcard character will create a regular expression group that can be accessed in the replacement pattern by using the same wildcard character.

String	Search Pattern	Replace Pattern	New Value
abc.txt	*.txt	*.csv	abc.csv
abc.txt	???.*	??b.*	abb.txt
abc.txt	*.*	*20100101.*	abc20100101.txt
abc20080523.txt	*????????.*	*.*	abc.txt

Regular Expressions

Regular expressions, commonly referred to as regex patterns, can be used to search for and replace sets of characters in a given string a files.

Summary of regular-expression constructs

Construct	Matches
Characters	
x	The character x
\\	The backslash character
\0n	The character with octal value 0n (0 <= n <= 7)
\0nn	The character with octal value 0nn (0 <= n <= 7)
\0mnn	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh	The character with hexadecimal value 0xhh
\uhhhh	The character with Unicode value hhhh
\t	The tab character ('\u0009')
\n	The newline (line feed) character ('\u000A')
\r	The carriage-return character ('\u000D')
\f	The form-feed character ('\u000C')
\a	The alert (bell) character ('\u0007')
\e	The escape character ('\u001B')
\cx	The control character corresponding to x
Character Classes	

Construct	Matches
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](subtraction)
Predefined Character Classes	
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
Boundary Catchers	
^	The beginning of a line
$	The end of a line
/b	A word boundary
/B	A non-word boundary
/A	The beginning of the input
/G	The end of the previous match
/Z	The end of the input but for the final terminator, if any
/z	The end of the input
Back References	
$n	Where n is the nth captured group
Quotation	

Construct	Matches
\	Nothing, but quotes the following character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends quoting started by \Q

Example

String	Search Pattern	Replace Pattern	New Value
abc.txt	(.*)\.txt	$1.csv	abc.csv
abc.txt	(.*)(.)\.(.*)	$1x.$3	abx.txt
abc.txt	(.*)\.(.*) $120150101.$2	$120150101.$2	abc20150101.txt
abc20150101.txt	(.*)\d{8}\.(.*)	$1.$2	abc.txt

Backslashes, Escapes, and Quoting

The backslash character ('\') serves to introduce escaped constructs, as defined in the table above, as well as to quote characters that otherwise would be interpreted as unescaped constructs. Thus the expression \\ matches a single backslash and \{ matches a left brace.

It is an error to use a backslash prior to any alphabetic character that does not denote an escaped construct; these are reserved for future extensions to the regular-expression language. A backslash may be used prior to a non-alphabetic character regardless of whether that character is part of an unescaped construct.

Character Classes

Character classes may appear within other character classes, and may be composed by the union operator (implicit) and the intersection operator (&&). The union operator denotes a class that contains every character that is in at least one of its operand classes. The intersection operator denotes a class that contains every character that is in both of its operand classes.

The precedence of character-class operators is as follows, from highest to lowest:

1. Literal escape \x
2. Grouping [...]
3. Range a-z
4. Union [a-e][i-u]

5. Intersection [a-z&&[aeiou]]

   Note: A different set of metacharacters are in effect inside a character class than outside a character class. For instance, the regular expression . loses its special meaning inside a character class, while the expression - becomes a range forming metacharacter.

Line terminators

A line terminator is a one or two-character sequence that marks the end of a line of the input character sequence. The following are recognized as line terminators:

- A newline (line feed) character ('\n'),
- A carriage-return character followed immediately by a newline character ("\r\n"),
- A standalone carriage-return character ('\r'),
- A next-line character ('\u0085'),
- A line-separator character ('\u2028'), or
- A paragraph-separator character ('\u2029)
  The regular expression . matches any character except a line terminator.

  The regular expressions ^ and $ ignore line terminators and only match at the beginning and the end, respectively, of the entire input sequence.

Groups and capturing

Capturing groups are numbered by counting their opening parentheses from left to right. In the expression ((A)(B(C))), for example, there are four such groups:

- ((A)(B(C)))
- (A)
- (B(C))
- (C)
  Group zero always stands for the entire expression.

  Capturing groups are so named because, during a match, each subsequence of the input sequence that matches such a group is saved. The captured subsequence may be used later in the expression, via a back reference, and may also be retrieved from the matcher once the match operation is complete.

  The captured input associated with a group is always the subsequence that the group most recently matched. If a group is evaluated a second time because of quantification then its previously-captured value, if any, will be retained if the second evaluation fails. Matching the string "aba" against the expression (a(b)?)+, for example, leaves group two set to "b". All captured input is discarded at the beginning of each match.

  Groups beginning with (? are pure, non-capturing groups that do not capture text and do not count towards the group total.

Unicode support

This class is in conformance with Level 1 of Unicode Technical Standard #18 and RL2.1 Canonical Equivalents.

Unicode escape sequences such as \u2014 in Java source code are processed as described in §3.3 of the Java Language Specification. Such escape sequences are also implemented directly by the regular-expression parser so that Unicode escapes can be used in expressions that are read from files or from the

keyboard. Thus the strings "\u2014" and "\\u2014", while not equal, compile into the same pattern, which matches the character with hexadecimal value 0x2014.

Unicode blocks and categories are written with the \p and \P constructs as in Perl. \p{prop} matches if the input has the property prop, while \P{ prop} does not match if the input has that property. Blocks are specified with the prefix In, as in InMongolian. Categories may be specified with the optional prefix Is: Both \p{L} and \p{IsL} denote the category of Unicode letters. Blocks and categories can be used both inside and outside of a character class

For a more precise description of the behavior of regular expression constructs, please see Mastering Regular Expressions, 2nd Edition, Jeffrey E. F. Friedl, O'Reilly and Associates, 2002.

FTP FAQs

In this section, we have listed answers to common questions for Managed File Transfer.

FTP - Connection fails

There are two modes in FTP communications: Active and Passive.

In Active mode, the FTP server will attempt to connect back to a port on the Managed File Transfer FTP client in order perform the data transfer. The challenge with Active mode is that your firewall may block the FTP server from trying to open a port back into your network.

In Passive mode, the FTP server does not need to connect back to a port on the Managed File Transfer FTP client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the FTP server, you may want to change the mode on the "FTP Servers Resource" on page 55 to Passive.

FTP - Connection times out

A FTP server may not respond on the first connection attempt. This may be due to a slow network or perhaps the FTP server is overloaded with other requests at the time. In order to solve this challenge, you can use a combination of the **Timeout, Connection Retry Attempts** and **Connection Retry Interval** settings for the "FTP Servers Resource" on page 55.

For instance, if you want Managed File Transfer to wait up to 180 seconds for a FTP server to respond, then specify 180 for the **Timeout** setting on the FTP server resource. The **Connections Retry Attempts** and **Connection Retry Interval** settings can additionally be specified to have Managed File Transfer continue to retry the FTP connection up to a certain limit.

FTP - Cannot retrieve (get) files

When a FTP directory listing (DIR) command is sent to a FTP server, most FTP servers will return the listing in a UNIX-style format. However, some Windows-based FTP servers may return the listing in a Windows-style format. If you experience problems with retrieving files from a Windows-based FTP server, you may want to change the **List Parser** to "Windows" on the "FTP Servers Resource" on page 55.

CHAPTER 12

Glossary Terms

AES

AES is the abbreviation for Advanced Encryption Standard. AES utilizes symmetric key cryptology. It provides strong encryption and is approved by the U.S. Government for protecting sensitive information. See http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf for more information on the AES encryption standard.

Asymmetric

A key system that utilizes two keys. One to encrypt and another to decrypt.

Asymmetric Cryptology

A form of cryptology that implements Key Pairs, in which the Public key portion of the Key Pair is used to encrypt information and the Private key portion is used to decrypt information. Otherwise known as Public Key Cryptology. SSH and SSL implement Asymmetric Cryptology.

Authentication

A mechanism to positively identify users by requesting credentials, such as a password or digital signature.

Certificate

Certificates are digital identification documents that allow both servers and clients to authenticate each other. A certificate contains information about a company and the organization that signed the certificate (such as Verisign). Certificates are used within SSL connections. See definition of SSL.

Certificate Authority

A trusted organization that issues signed certificates. Examples of Certificate Authorities are Verisign, Entrust and Equifax.

CIDR

Classless Inter-Domain Routing (CIDR) is a methodology of allocating IP addresses and routing Internet Protocol packets.

Cipher

A mathematical process (algorithm) used to scramble (encrypt) data.

Cryptology

The art and science of keeping data secret.

CSV

A Comma separated values (CSV) file is a computer data file used for storage of data structured in a table form. Each line in the CSV file corresponds to a row in the table. Within a line, fields are separated by commas, each field belonging to one table column.

Decryption
The process of converting encrypted code into understandable information.

Diffie-Hellman/DSS
A standard algorithm used for encrypting information and encoding digital signatures. DSS is an abbreviation for Digital Signature Standard.

Digital Signature
An electronic signature which is encoded into a document using the sender's Private key. This signature can be authenticated by the recipient using the sender's Public key. An authenticated signature will ensure the original content of the document has not been altered by an unauthorized party.

DSA
Abbreviation for Digital Signature Algorithm. DSA is one of the allowable algorithms for creating SSH keys.

Element
Elements are used to define the Email Server.

Encryption
The process of converting information into unintelligible code.

Fingerprint
The fingerprint is a unique hash value generated by the software for the key. You can verify the authentication of a key by reading the fingerprint (generally over the phone) back to the owner of the key.

FTP
A communications protocol governing the transfer of files from one computer to another over a network.

FTPS
FTPS utilizes the SSL security protocol standard for encrypting data over FTP connections. See the definition for SSL.

Hash Function
An algorithm for calculating a value based on a block of data. If the data changes in any way, then the hash values will not match when it is recalculated. A hash will protect the integrity of data.

HTTP
Hypertext Transfer Protocol. The communications protocol on which the Web is based. HTTP sets rules for how information is passed between the server and the browser software.

HTTPS
Hypertext Transfer Protocol Secure. HTTPS users a SSL/TLS layer to add encryption to the data transport over standard HTTP.

ICAP
Internet Content Adaptation Protocol

Icon
A picture or symbol that represents an object, task, command, or choice users can select by pointing and clicking with a mouse.

ISO format

The ISO format for a date is yyyy-MM-dd. The ISO format for a time is HH:mm:ss. The ISO format for a timestamp is yyyy-MM-dd HH:mm:ss.

JCE Service Provider

A vendor that provides JCE (Java Cryptology Extensions). Example providers of JCEs are IBM and Sun. A JCE is a framework and implementation for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms.

JDBC drivers

A JDBC driver is a software component that enables a Java application to interact with a database.

JKS

JKS (Java Key Store) is Java's standard file format for storing certificates and keys.

Key

The information needed to encrypt or decrypt data.

Key Alias/Key ID

A unique name assigned to a key in a Keyring or Key Store.

Key Pair

A combination of a Private key and its corresponding Public key. Key Pairs are used within Asymmetric Cryptology systems, such as SSH and SSL.

Key Store

A binary file which holds one or more keys. A Key Store is useful for keeping keys organized into one location. Also known as Keyring.

MDN

Message Disposition Notification - A return receipt format for electronic messages.

MMS

Multimedia Messaging Service

Non-Repudiation

Creating a proof of the origin or delivery of data, thus preventing the recipient from falsely denying that data has been received and preventing the sender from falsely asserting that data has been sent.

Passphrase

Similar to a password, a passphrase is a string of characters or words (entered by the User or program) that is used to authenticate or encrypt/decrypt information. A passphrase can generally be longer than a traditional password.

PKCS12

An internet standard file format commonly used to store private keys with accompanying public key certificates.

Private Key

The portion of a Key Pair which is used by the owner to decrypt information and to encode digital signatures. The Private key, typically protected by a password, should be kept secret by the owner and NOT shared with trading partners. Also known as a Secret Key.

Project

Projects are used to describe the work for Managed File Transfer to perform. For instance, a Project definition can indicate from where to retrieve data, what processes to perform on the data (e.g. convert to Excel, Zip, encrypt) and where to distribute the output. A Project can be made up of one or more Modules, Tasks and Elements.

Public Key

The portion of the Key Pair which is used to encrypt information bound for its owner and to verify signatures made by its owner. The owner's Public key should be shared with its trading partners.

Public Key Cryptology

The alternative name for Asymmetric Cryptology.

Public Keyring

A type of Keyring which contains Public keys.

RSA

An algorithm used for encrypting information, which was authored by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames.

Run Priority

The Run Priority indicates how much attention (CPU) the Job will receive from Managed File Transfer when it executes. The run priority is a value from 1 to 10, in which jobs with a higher run priority will receive more attention than jobs with a lower run priority. For instance a job with a run priority of 6 will receive more attention than a job with a run priority of 5.

SAML

Security Assertion Markup Language is an XML-based open standard data format for exchanging authentication and authorization between parties.

Secret Key

The alternative name for Private key.

Secret Keyring

A type of Keyring that contains Private keys. This type of Keyring should be kept private and NOT be shared with trading partners.

Self-Signed Certificate

A certificate that is signed by its own creator. That is, the person that created the certificate also signed off on its legitimacy.

SFTP

SFTP utilizes the SSH program for encrypting data over FTP connections. See the definition for SSH.

Signing
The process of encoding an electronic signature into a document using the sender's Private key. This signature can be authenticated by the recipient using the sender's Public key. An authenticated signature will ensure the original content of the document has not been altered by an unauthorized party.

SMS
Short Message Service

SMTP
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SSH
SSH is an abbreviation for Secure Shell. SSH is both a computer program and an associated network protocol designed for encrypting communications between two untrusted hosts over a network. It utilizes Public keys to provide asymmetric cryptology.

SSL
SSL is an abbreviation for Secure Sockets Layer. SSL is a security protocol for encrypting communications between two hosts over a network. SSL utilizes certificates to establish trust between the two hosts. SSL can be used over several network protocols, including FTP, HTTP and Email.

SSO
Single Sign On

Symmetric
A key system that utilizes a single key to encrypt and decrypt.

Symmetric Cryptology
A form of cryptology in which a single key can be used to encrypt and decrypt data. The key must be kept secret or the security is compromised. Also known as Secret key cryptology. ZIP password protection and AES encryption are both forms of Symmetric Cryptology.

URL
Uniform Resource Locator. An Internet address, as well as a standard method of naming files on the Web. A URL begins with a protocol name (such as http), followed by a colon and two forward slashes(//). Next comes the name of the internet server on which the file is stored, followed by directories that hold the file, separated by forward slashes(/). The filename comes last, as shown in the following example: http://www.mycompany.com/whatsnew.htm

Variable
A variable is an element that acts as a reference to a particular value (used within a Project).

Verification
The process of authenticating a digital signature that is embedded in a message or file. Verification is performed with the sender's Public key. An authenticated (verified) signature will ensure the original content of the document has not been altered by an unauthorized party.

XML
Extensible Markup Language (XML) is a general-purpose specification for creating custom markup languages. It is classified as an extensible language, because it allows the User to define the mark-up

elements. XML's purpose is to aid information systems in sharing structured data, especially via the Internet, to encode documents, and to serialize data.

INDEX

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W