

# Managing File Transfers with webMethods ActiveTransfer

Version 10.15

October 2022

This document applies to webMethods ActiveTransfer Server 10.15 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2012-2024 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <https://softwareag.com/licenses/>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <https://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <https://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

**Document ID: AT-AG-1015-20240404**

# Table of Contents

<b>About this Guide</b> .....	7
Document Conventions.....	8
Online Information and Support.....	9
Data Protection.....	10
<b>1 Understanding ActiveTransfer</b> .....	<b>11</b>
Overview of webMethods ActiveTransfer.....	12
What is webMethods ActiveTransfer?.....	12
Windows Deployment.....	13
Linux Deployment.....	18
ActiveTransfer Features.....	27
ActiveTransfer Capabilities.....	27
Typical Usage Scenarios.....	29
Protocols supported by ActiveTransfer.....	29
<b>2 Configuring ActiveTransfer</b> .....	<b>31</b>
Accessing ActiveTransfer New User Interface.....	32
Configuring Single Sign-On for ActiveTransfer User Interface.....	34
<b>3 Managing Listeners</b> .....	<b>37</b>
Overview.....	38
Features in Listeners.....	38
Adding a Listener.....	40
Configuring Additional Settings for a Listener.....	40
Activating or Deactivating a Listener.....	48
Modifying a Listener.....	49
Including Listener Information in User Emails.....	50
<b>4 API Support for HTTP file operations</b> .....	<b>51</b>
Introduction.....	52
Creating a folder.....	53
Deleting a file or a folder.....	53
Renaming a file or folder.....	54
Uploading a file.....	54
Listing of files.....	55
Verifying the input.....	55
Downloading a file.....	56
<b>5 Managing Gateways</b> .....	<b>57</b>
Overview.....	58
Features in Gateways.....	58
Adding a Gateway.....	59

---

Configuring Additional Settings for a Gateway.....	60
Modifying a Gateway.....	61
<b>6 Managing Virtual Folders.....</b>	<b>63</b>
Overview.....	64
Features in Virtual Folders.....	64
Adding a Virtual Folder.....	66
Configuring Additional Settings for a Virtual Folder.....	66
Modifying a Virtual Folder.....	75
Searching for Virtual Folders.....	75
<b>7 Managing Actions.....</b>	<b>77</b>
Overview.....	78
Adding a Post-Processing Action.....	78
Adding a Scheduled Action.....	81
Adding a Monitor folder Action.....	84
Task Configuration Definitions.....	88
Operating Actions.....	125
Modifying a Post-Processing, Scheduled, or Monitor folder Action.....	126
Searching for a Post-Processing, Scheduled, or Monitor folder Action.....	127
Parameterizing Scheduled Action Tasks.....	127
<b>8 Managing Users and Templates.....</b>	<b>131</b>
Overview.....	132
Templates.....	144
<b>9 Viewing and Downloading Logs.....</b>	<b>151</b>
Overview.....	152
Viewing the Transaction Log.....	152
Viewing the Action Log.....	155
Rerun a Post-Processing Action.....	156
Viewing the Audit Log.....	159
Viewing the Analytical Details.....	160
Viewing the Agent Action Log.....	161
Viewing the Agent Activity Log.....	162
Downloading Log Data.....	164
<b>10 Managing Proxy Servers.....</b>	<b>167</b>
Overview.....	168
Proxy Server Alias Usage Scenarios.....	168
Adding Proxy Servers.....	170
<b>11 Managing Certificates.....</b>	<b>173</b>
Overview.....	174
Adding Certificates.....	174

<b>12 Managing ActiveTransfer Settings.....</b>	<b>177</b>
Overview.....	178
Features in ActiveTransfer Global Settings.....	178
Configuring Listener Preferences.....	180
Acceleration.....	185
Configuring Audit Settings.....	188
Configuring File Share Settings.....	188
Configuring Server Properties.....	190
Configuring ActiveTransfer to Send Emails.....	191
Configuring Password Complexity for Users.....	194
<b>13 Managing User Interface Permissions for Users, Roles, and Groups.....</b>	<b>197</b>
Overview.....	198
Configuring UI Permissions to Users, Roles, or Groups.....	198
Searching UI Permissions for Users, Roles, or Groups.....	199
<b>14 Archiving Data.....</b>	<b>201</b>
Overview.....	202
Configuring the Schema/Database for Data Archive.....	202
Configuring the ActiveTransferArchive Database Pool.....	204
Configuring the ActiveTransfer User Interface for Data Archive.....	204
Archiving Data from the ActiveTransfer User Interface.....	205
Scheduling Data Archive.....	205
Searching for Archived Data.....	205
Executing the Stored Procedure for Data Archive.....	206
<b>15 Managing ActiveTransfer Account Settings.....</b>	<b>207</b>
Configuring ActiveTransfer Account Settings.....	208
<b>16 Removing User Data from ActiveTransfer.....</b>	<b>211</b>
Overview.....	212
Removing PII from the ActiveTransfer Log Files.....	212
Removing PII from the ActiveTransfer Database.....	213
<b>17 Migrating Assets.....</b>	<b>215</b>
Overview.....	216
ActiveTransfer Assets You Can Migrate.....	216
Migration Methods.....	217
ActiveTransfer Asset Dependencies.....	217
How ActiveTransfer Server Detects Assets on the Target System Before Importing Them.....	219
Importing Assets.....	219
Exporting Assets.....	219
<b>A Server Configuration Parameters and Variables.....</b>	<b>221</b>
Server Configuration Parameters.....	222

Security Configuration Parameters.....	232
Server Variables.....	233
<b>B Calendar and Processing Options for Scheduled Events.....</b>	<b>241</b>
Scheduled Event Options.....	242
<b>C Working with Jump Conditions.....</b>	<b>245</b>
Overview.....	246
Jump Condition Elements.....	246
Defining a Jump Condition.....	248
<b>D Limitations.....</b>	<b>251</b>
Limitations.....	252

# About this Guide

■ Document Conventions .....	8
■ Online Information and Support .....	9
■ Data Protection .....	10

---

*Managing File Transfers with webMethods ActiveTransfer* explains how to configure webMethods ActiveTransfer, manage file transfers, and view analytical information about file transfer activity within an environment. The guide explains common administrative tasks, such as managing servers and ports, defining post-processing and scheduled actions, managing folders, granting user access to folders and server instances, and viewing and maintaining log information.

*Managing File Transfers with webMethods ActiveTransfer* assumes you are familiar with webMethods Integration Server.

A new user interface is now available for webMethods ActiveTransfer. You can work with functionalities such as Listeners, Gateways, Users, Roles, Groups, Templates, Folders, and Actions in the new user interface.

## Document Conventions

---

Convention	Description
<b>Bold</b>	Identifies elements on a screen.
Narrowfont	Identifies service names and locations in the format <i>folder.subfolder.service</i> , APIs, Java classes, methods, properties.
<i>Italic</i>	Identifies:  Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
Monospace font	Identifies:  Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the   symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

---

## Online Information and Support

---

### Product Documentation

You can find the product documentation on our documentation website at <https://documentation.softwareag.com>.

In addition, you can also access the cloud product documentation via <https://www.softwareag.cloud>. Navigate to the desired product and then, depending on your solution, go to “Developer Center”, “User Center” or “Documentation”.

### Product Training

You can find helpful product training material on our Learning Portal at <https://learn.softwareag.com>.

### Tech Community

You can collaborate with Software AG experts on our Tech Community website at <https://techcommunity.softwareag.com>. From here you can, for example:

- Browse through our vast knowledge base.
- Ask questions and find answers in our discussion forums.
- Get the latest Software AG news and announcements.
- Explore our communities.
- Go to our public GitHub and Docker repositories at <https://github.com/softwareag> and <https://containers.softwareag.com/products> and discover additional Software AG resources.

### Product Support

Support for Software AG products is provided to licensed customers via our Empower Portal at <https://empower.softwareag.com>. Many services on this portal require that you have an account. If you do not yet have one, you can request it at <https://empower.softwareag.com/register>. Once you have an account, you can, for example:

- Download products, updates and fixes.
- Search the Knowledge Center for technical information and tips.
- Subscribe to early warnings and critical alerts.
- Open and update support incidents.
- Add product feature requests.

---

## Data Protection

---

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

# 1 Understanding ActiveTransfer

■ Overview of webMethods ActiveTransfer .....	12
■ What is webMethods ActiveTransfer? .....	12
■ Windows Deployment .....	13
■ Linux Deployment .....	18
■ ActiveTransfer Features .....	27
■ ActiveTransfer Capabilities .....	27
■ Typical Usage Scenarios .....	29
■ Protocols supported by ActiveTransfer .....	29

## Overview of webMethods ActiveTransfer

---

webMethods ActiveTransfer is a Managed File Transfer (MFT) solution that ensures protected internal and external data transfers in a centralized system for Business-to-Business (B2B), Application-to-Application (A2A), cloud-based, or ad hoc environments. ActiveTransfer uses a combination of advanced software and secure communication protocols to provide:

- Reliable and secure data transfer.
- Automated data transfers based on specific policies, partners, and permissions.
- Management of large files.
- Insight and control at every stage of the transfer process, including real-time monitoring, error and receipt logging, auditing, and data tracking.

MFT solutions come in many implementations, including both software applications and services, with varying levels of control, integration, and transparency. Most MFT solutions are made up of at least the following four key components, available individually or bundled as an end-to-end solution:

- **ActiveTransfer servers** that do the primary work of data exchange behind a firewall, including support of all communications and security protocols.
- **Proxies/reverse proxies** that operate in the demilitarized zone and protect the actual IP addresses and ports of both transmitters and recipients.
- **Clients** that provide administration, reporting, scheduling, and scripting, used by both human users and applications (through application programming interfaces or APIs).
- **APIs** that enable third-party applications to interact and communicate with ActiveTransfer servers.

MFT offers a number of security, administration, and scalability advantages over non-secure file transfer protocols such as FTP. With MFT, there is no need to develop custom code for routine functions such as delivery confirmation, reporting, audit, security provisioning, and trading partner/community management.

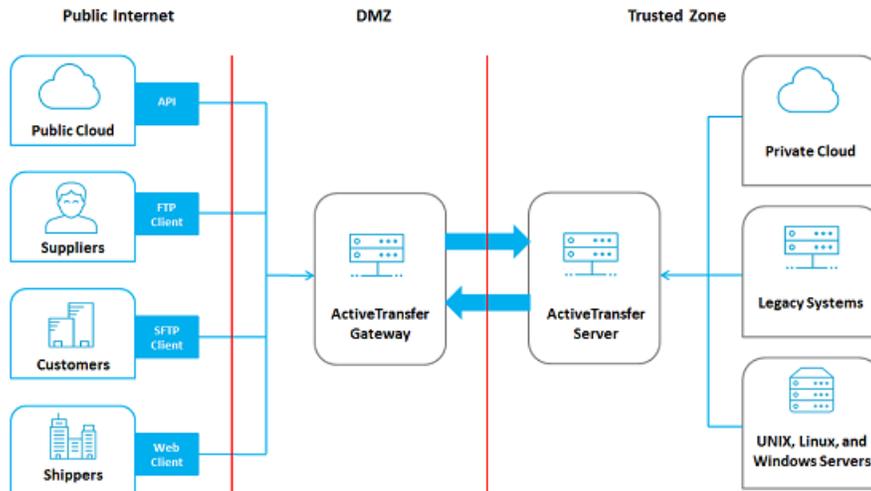
## What is webMethods ActiveTransfer?

---

webMethods ActiveTransfer is an integrated MFT solution that brings together B2B, application support, and MFT in a service-oriented platform.

webMethods ActiveTransfer provides you with a single point of control for all file transfer activities, both inside and outside the extended enterprise. ActiveTransfer enables organizations to exchange information securely over the Internet using a variety of communication protocols.

The following figure illustrates how ActiveTransfer components fit into an MFT scenario at a high level:



ActiveTransfer is fully integrated with the webMethods Product Suite, enabling companies to replace older, non-secure file transfer systems with a consolidated platform. ActiveTransfer supports collaboration, file sharing, integration, governance, and scalability.

## Windows Deployment

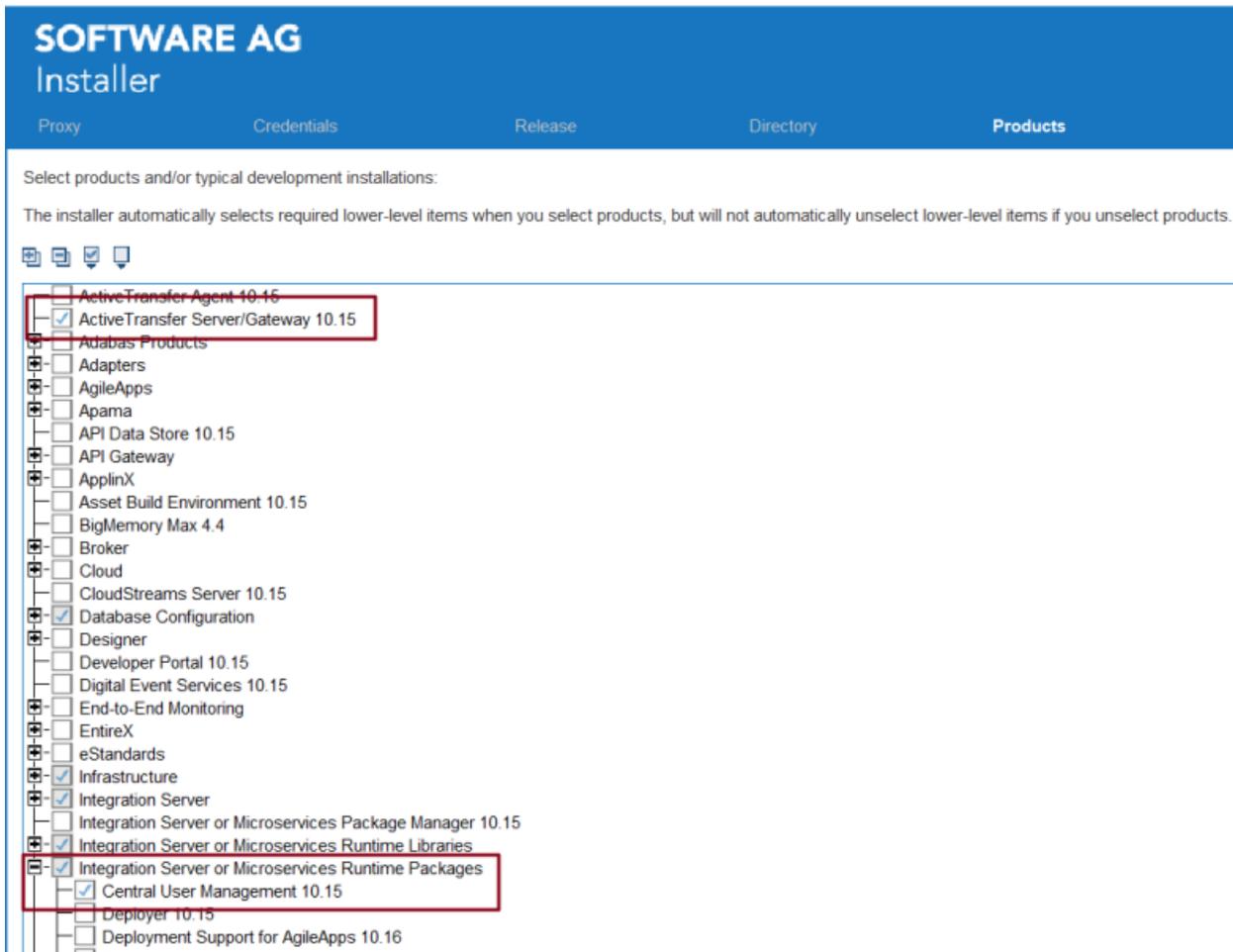
Ensure that you have the Software AG Installer and the license file copied to the system in which you want to install ActiveTransfer Server.

Use the following custom configuration when you run the Software AG Installer to install ActiveTransfer Server.

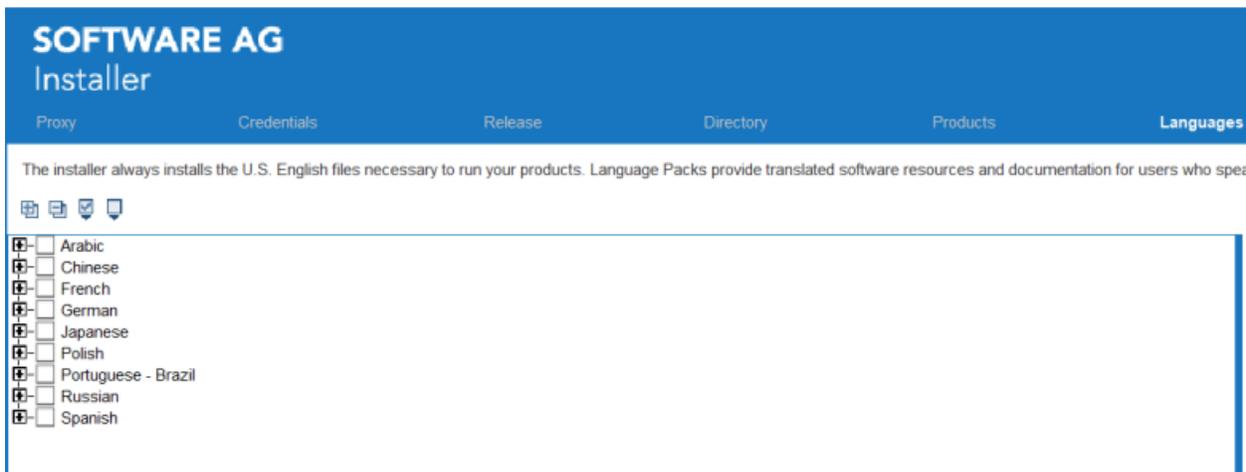
### ➤ To install ActiveTransfer Server using Software AG Installer

1. Run the Software AG Installer.
2. In the **Credentials** tab, provide your Empower credentials and click **Next**.
3. In the **Directory** tab, specify the installation directory if required, and click **Next**.
4. In the **Products** tab, select the following components:
  - a. **ActiveTransfer Server/Gateway**
  - b. **Integration Server or Microservices Runtime Packages > Central User Management**
 Click **Next**.

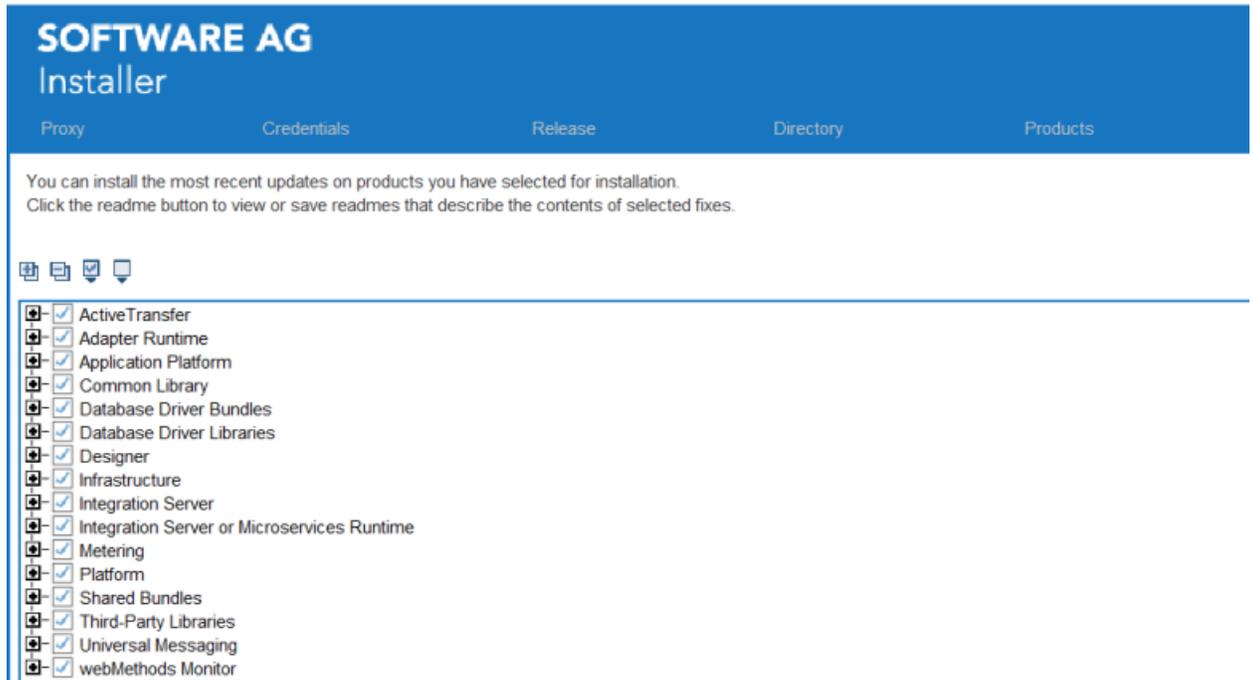
ActiveTransfer Server uses the Central User Management component for user management.



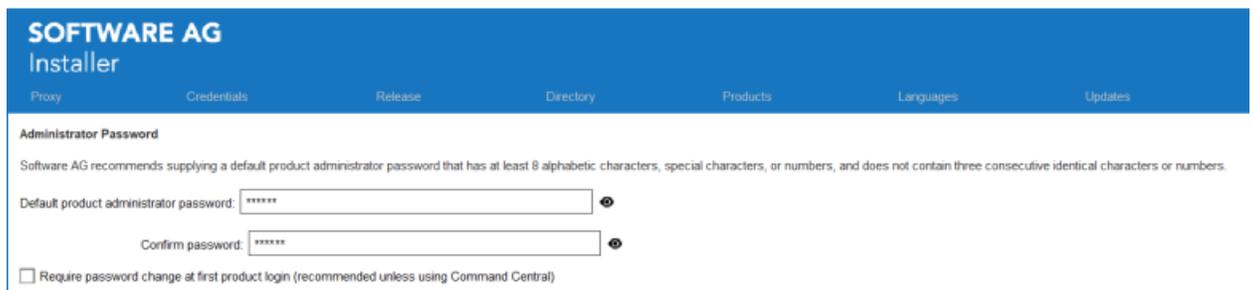
5. Read through the license agreement and select the checkbox below the agreement to provide your consent. Click **Next**.
6. Select your language packs. Click **Next**.



7. Select your most recent updates. Click **Next**.



8. Provide the **Administrator Password**. Select the checkbox **Require password change at first product login** to change the password at first login. Click **Next**.



9. In the **Configure** tab, click **Browse** to select the license file. **5555** and **9999** are the default primary ports for the Integration Server instance. Modify the ports, if required, and click **Next**.

**SOFTWARE AG**  
Installer

Proxy      Credentials      Release      Directory      Products      Languages

**Integration Server**

License file:

Server Instance

Instance name:       Secure port:

Primary port:       Diagnostic port:

Register Windows service/UNIX daemon for automatic startup

10. Provide the Integration Server database connection details. Click **Next**.

ActiveTransfer Server uses the scheduler from Integration Server to run scheduled actions.

**SOFTWARE AG**  
Installer

Proxy      Credentials      Release      Directory      Products      Languages

**Integration Server**

Database Connection

You can specify the database connection now or after installation. The product might not start or work properly until the database connection exists.

External RDBMS     Embedded database

RDBMS:

jdbc:wm:oracle://<server>:<port>;serviceName=<service>[;<option>=<value>]...

Connection name:

URL:

Database user:

Password:

11. Provide the **Platform manager** details. Click **Next**.

12. On the **ActiveTransfer Server/Gateway** page, select **Run as Server**. Provide a valid license file and database details for ActiveTransfer Server. Click **Next**.

Note that there are separate license files for ActiveTransfer Server and ActiveTransfer Gateway. At runtime, this license file decides whether the instance runs as ActiveTransfer Server or ActiveTransfer Gateway.

**Note:**

The license files are saved at `\IntegrationServer\instances\<instance_name>\packages\WmMFT\config\licenseKey.xml`. You must replace this file with a new file, if you need to

change the license file after the installation. Restart the Integration Server after changing the license file.

**SOFTWARE AG**  
Installer

Proxy      Credentials      Release      Directory      Products      Languages

**Active Transfer Server/Gateway**

Run as Server  
 Run as Gateway (reverse proxy)

Registration port:

License file:

The license file must match your choice of Server or Gateway.

**Database Connection**

You must specify the database connection or ActiveTransfer Server or Gateway will not start.

RDBMS:

jdbc:wm:oracle://<server>:<port>;serviceName=<service>[<option>=<value>...]

Connection name:

URL:

Database user:

Password:

- Provide the **Common Directory Service Support** details. This is required as you have selected the **Central User Management** component during initial setup. Click **Next**.

For more information about what database components to install, see the ActiveTransfer Server Database Components section in *Installing Software AG Products*. For more information about how to run the Database Configurator, see the Database Component Configurator Graphical User Interface section in *Installing Software AG Products*.

**Note:**

The database that you configure here must have the MWS database component installed to have all CDS related schema available.

**SOFTWARE AG**  
Installer

Proxy    Credentials    Release    Directory    Products    Languages

**Common Directory Service Support**

Database Connection

You can specify the database connection now or after installation. The product might not start or work properly until the database connection exists.

RDBMS: Oracle

Connection name: AT

jdbc:wm:oracle://<server>:<port>;serviceName=<service>[<option>=<value>]...

URL:

Database user:

Password: \*\*\*\*\*

14. Verify your installation details. Click **Install**.

**SOFTWARE AG**  
Installer

Proxy    Credentials    Release    Directory    Products    Languages    Updates    Configure    Install    About

The items listed below are ready to be installed.

Products    Updates

ActiveTransfer Server/Gateway 10.15  
Database Configuration  
Integration Server and Microservices Runtime Embedded Database Scripts 10.15  
Infrastructure  
  Common C/C++ Runtime  
  Event Routing Event Type Store 10.15  
  Integration Server  
  Adapter Runtime 10.15  
  Flat File 10.7  
  Integration Core 10.15  
Java  
  Java Package Core 11.0  
Libraries  
  Shared Libraries 10.15  
  Broker Libraries 10.15  
  CentralSite Libraries 10.11  
  Common Libraries for OpenSSL 10.15  
  Composite Applications Runtime 10.15  
  Database Component Configurator Core 10.15  
  Database Driver Libraries 10.15  
  Designer Libraries 10.15  
  Digital Event Services 10.15  
  Glue Libraries 8.0  
  Installer Libraries 10.15  
  Migration Framework Libraries 10.15  
  My webMethods Server Libraries 10.15  
  Optimize Libraries 10.15  
  Third-Party Libraries  
  Application Server Libraries 10.15 for Glassfish  
  Base Security Libraries 10.15

< Back    Install    Cancel

## Linux Deployment

Ensure that you have the Software AG Installer and the license file copied to the system in which you want to install ActiveTransfer Server.

Use the following custom configuration when you run the Software AG Installer to install ActiveTransfer Server.

➤ **To install ActiveTransfer Server using Software AG Installer**

1. Change directory to the installer download folder.

```
cd ~/Downloads/SoftwareAG/
```

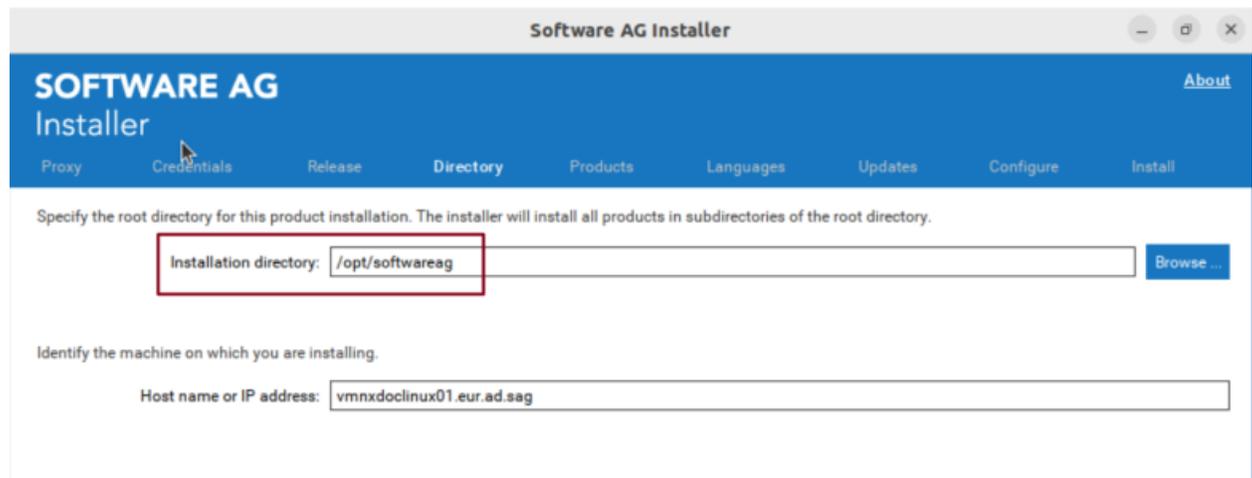
2. Make the installer executable.

```
chmod +x ~/Downloads/SoftwareAG/SoftwareAGInstaller20230725-Linux_x86_64.bin
```

3. Run the Software AG Installer.

```
./SoftwareAGInstaller20230725-Linux_x86_64.bin
```

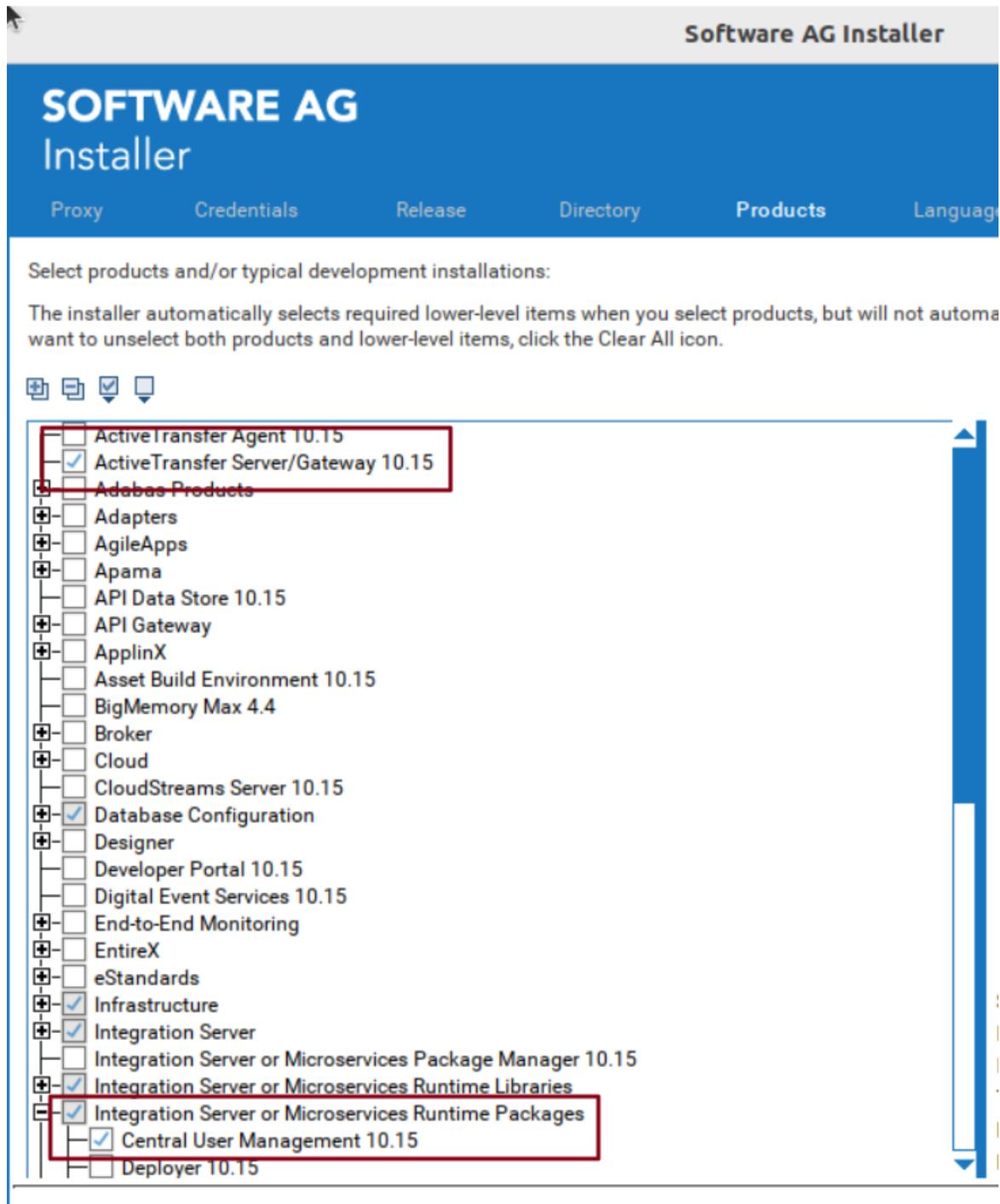
4. In the **Credentials** tab, provide your Empower credentials and click **Next**.
5. In the **Directory** tab, specify the installation directory if required, and click **Next**.



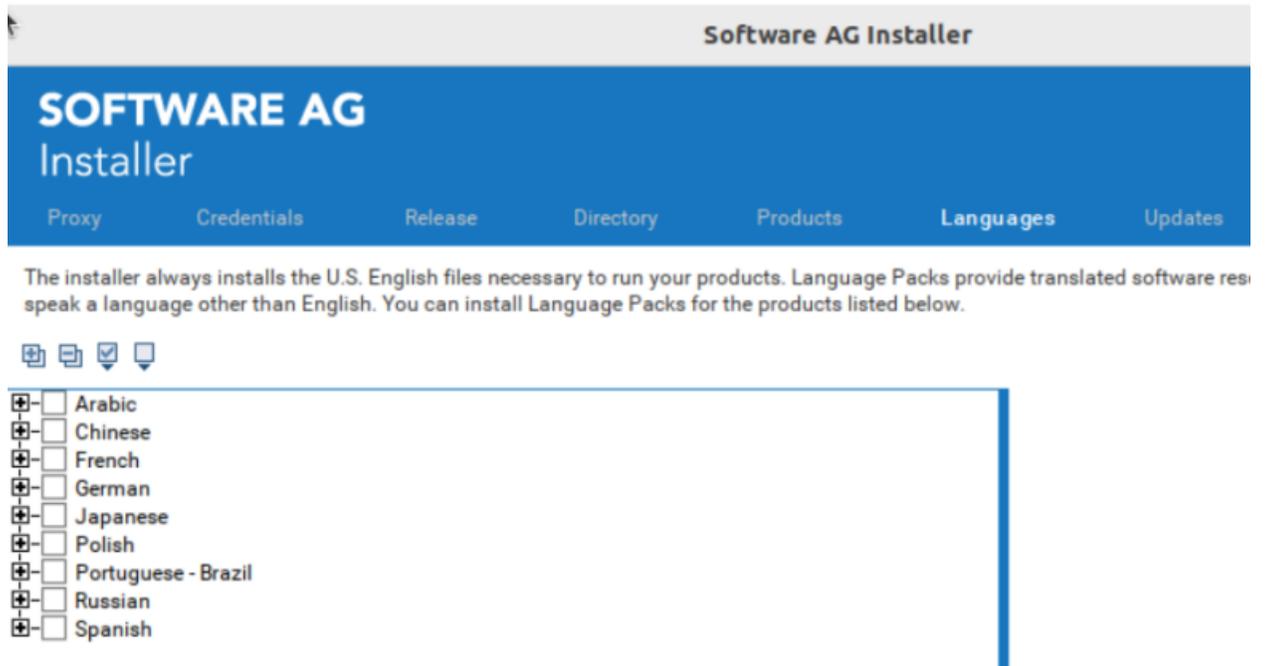
The screenshot shows the 'Software AG Installer' window with the 'Directory' tab selected. The window title is 'Software AG Installer'. The main header is 'SOFTWARE AG Installer' with an 'About' link. The navigation tabs are: Proxy, Credentials, Release, Directory, Products, Languages, Updates, Configure, and Install. The 'Directory' tab is active, showing the instruction: 'Specify the root directory for this product installation. The installer will install all products in subdirectories of the root directory.' Below this is a text input field for 'Installation directory:' containing '/opt/softwareag', with a 'Browse ...' button to its right. Below that is the instruction: 'Identify the machine on which you are installing.' followed by a text input field for 'Host name or IP address:' containing 'vmnxdoclinox01.eur.ad.sag'.

6. In the **Products** tab, select the following components:
  - a. **ActiveTransfer Server/Gateway**
  - b. **Integration Server or Microservices Runtime Packages > Central User Management**
 Click **Next**.

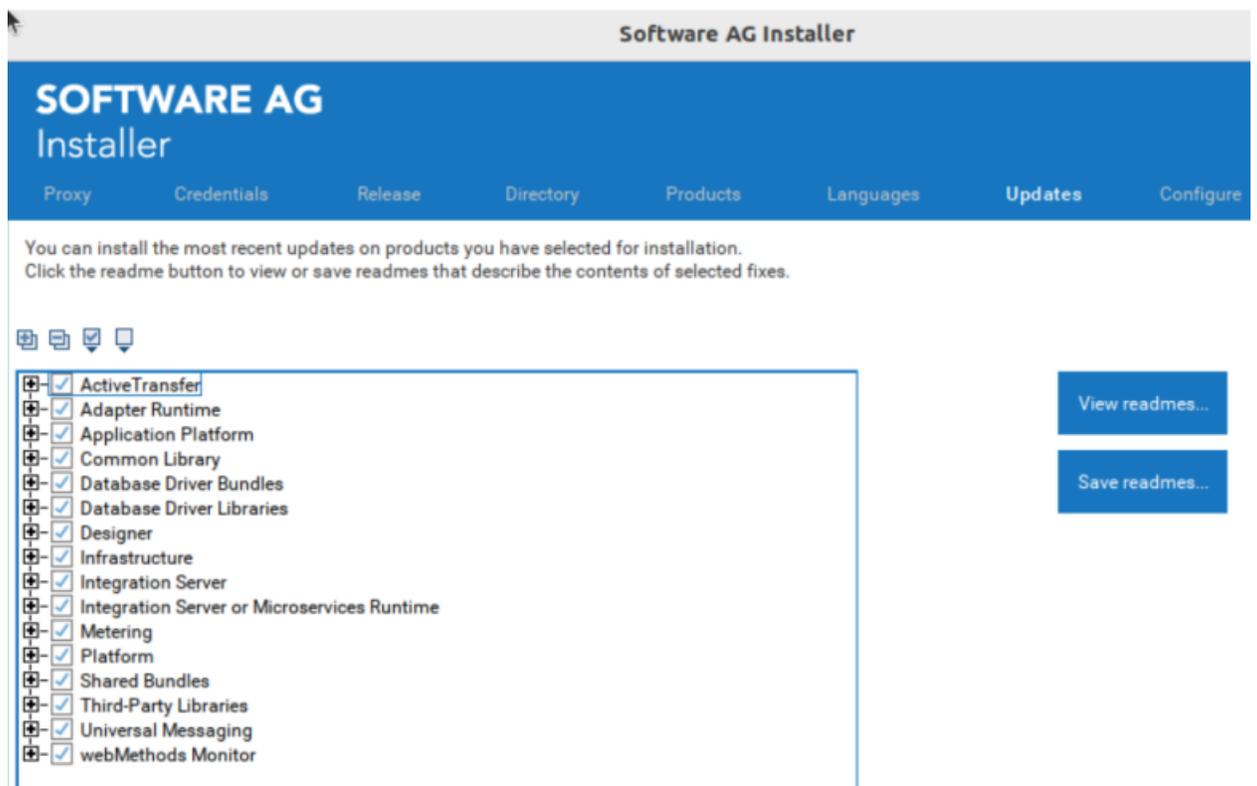
ActiveTransfer Server uses the Central User Management component for user management.



7. Read through the license agreement and select the checkbox below the agreement to provide your consent. Click **Next**.
8. Select your language packs. Click **Next**.



9. Select your most recent updates. Click **Next**.



10. Provide the **Administrator Password**. Select the checkbox **Require password change at first product login** to change the password at first login. Click **Next**.

**SOFTWARE AG**  
Installer

Proxy Credentials Release Directory Products Languages Updates **Configure**

**Administrator Password**

Software AG recommends supplying a default product administrator password that has at least 8 alphabetic characters, special characters, or number contain three consecutive identical characters or numbers.

Default product administrator password:

Confirm password:

Require password change at first product login (recommended unless using Command Central)

11. Provide the **sudo** password for the Linux user running the installation.

**SOFTWARE AG**  
Installer

Proxy Credentials Release Directory Products Languages Updates **Configure**

**Sudo**

Sudo is required to register daemons, and in some cases to set file permissions, for one or more products you are installing.

Use sudo, with password

The user under which you are running the installer must be in the sudoers configuration.

Do not use sudo or sudo is not available

You will have to manually run the afterinstallAsRoot.sh script with root user privileges after installation. The script is located in the /opt/softwareag/bin directory after installation. See your installation guide for details.

12. In the **Configure** tab, click **Browse** to select the license file. **5555** and **9999** are the default primary ports for the Integration Server instance. Modify the ports, if required. Select the register service checkbox if you want Integration Server to start automatically on startup. Click **Next**.

Software AG Installer

**SOFTWARE AG**  
Installer

Proxy Credentials Release Directory Products Languages Updates **Configure** Install

Integration Server

License file:  [Browse...](#)

Server Instance

Instance name:  Secure port:

Primary port:  Diagnostic port:

Register Windows service/UNIX daemon for automatic startup

13. Provide the Integration Server database connection details. Click **Next**.

ActiveTransfer Server uses the scheduler from Integration Server to run scheduled actions.

Software AG Installer

**SOFTWARE AG**  
Installer

Proxy Credentials Release Directory Products Languages Updates **Configure** Install

Integration Server

Database Connection

You can specify the database connection now or after installation. The product might not start or work properly until the database connection exists.

External RDBMS  Embedded database

RDBMS:

`jdbc:wm:oracle://<server>:<port>;serviceName=<service>[<option>=<value>]...`

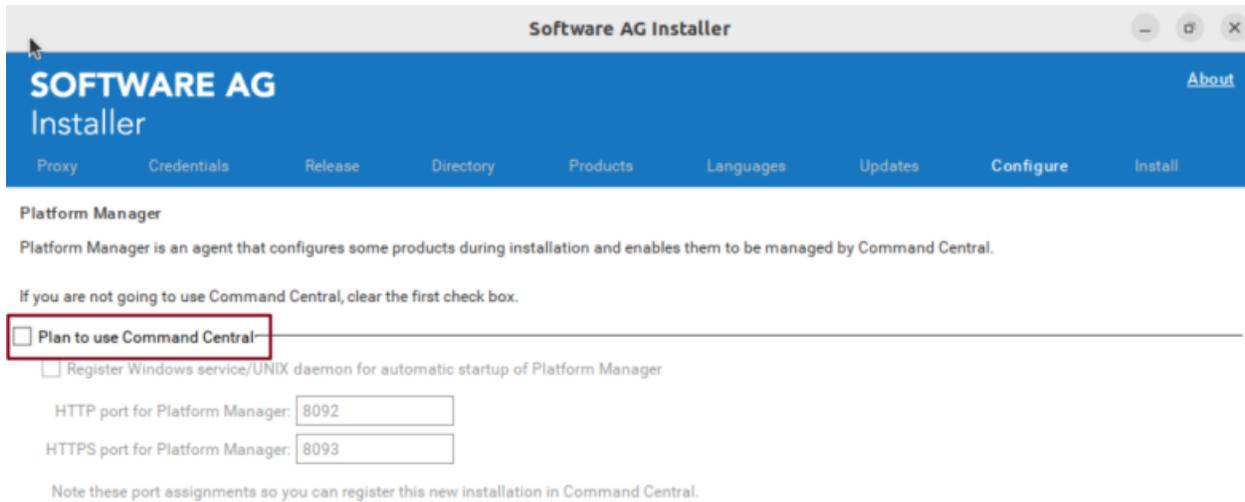
Connection name:

URL:

Database user:

Password:

14. Provide the **Platform manager** details. Clear the **Plan to use Command Central** checkbox if you are not using Command Central. Click **Next**.



15. On the **ActiveTransfer Server/Gateway** page, select **Run as Server**. Provide a valid license file and database details for ActiveTransfer Server. Click **Next**.

Note that there are separate license files for ActiveTransfer Server and ActiveTransfer Gateway. At runtime, this license file decides whether the instance runs as ActiveTransfer Server or ActiveTransfer Gateway.

**Note:**

The license files are saved at `\IntegrationServer\instances\<instance_name>\packages\WmMFT\config\licenseKey.xml`. You must replace this file with a new file, if you need to change the license file after the installation. Restart the Integration Server after changing the license file.

**Software AG Installer**

**SOFTWARE AG**  
Installer

Proxy Credentials Release Directory Products Languages Updates **Configure** Install

ActiveTransfer Server/Gateway

Run as Server  
 Run as Gateway (reverse proxy)

Registration port: 8500

License file: /home/EUR/tech-doc-autodeploy/Downloads/ActiveTransferServer/0000763142\_ActiveTransfer\_Server100.xml Browse...

The license file must match your choice of Server or Gateway.

Database Connection

You must specify the database connection or ActiveTransfer Server or Gateway will not start.

RDBMS: Oracle

jdbc:wm:oracle://<server>:<port>;serviceName=<service>[<option>=<value>...]

Connection name: AT

URL: [Redacted]

Database user: [Redacted]

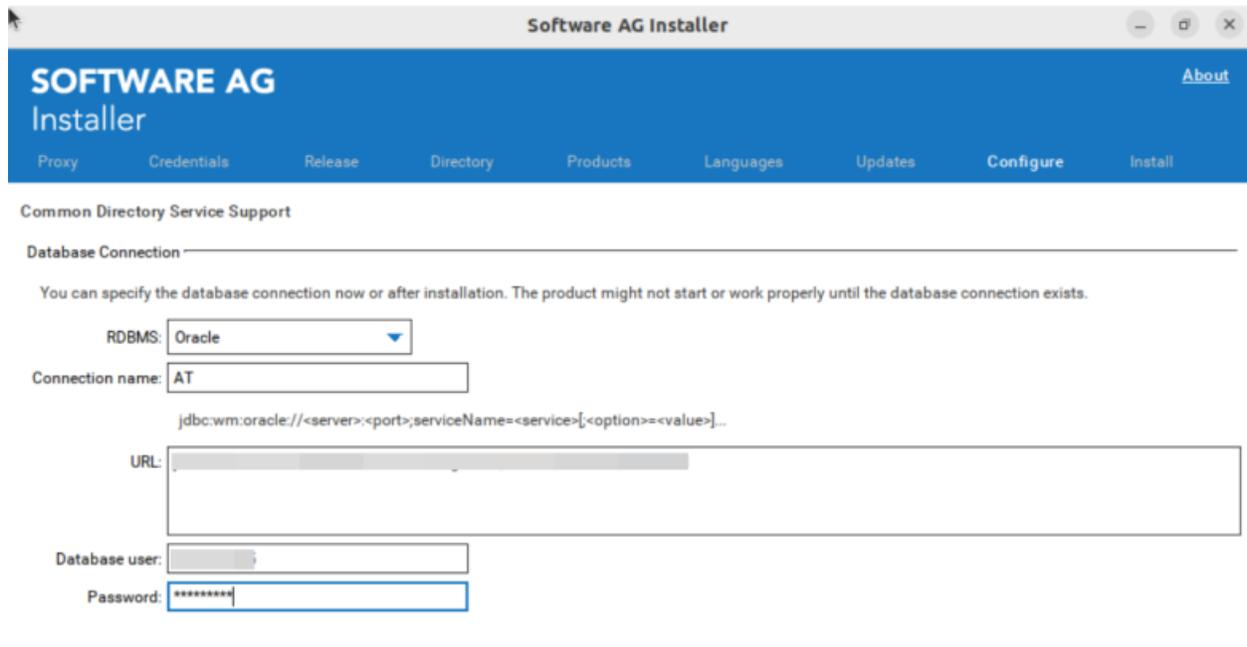
Password: [Redacted]

16. Provide the **Common Directory Service Support** details. This is required as you have selected the **Central User Management** component during initial setup. Click **Next**.

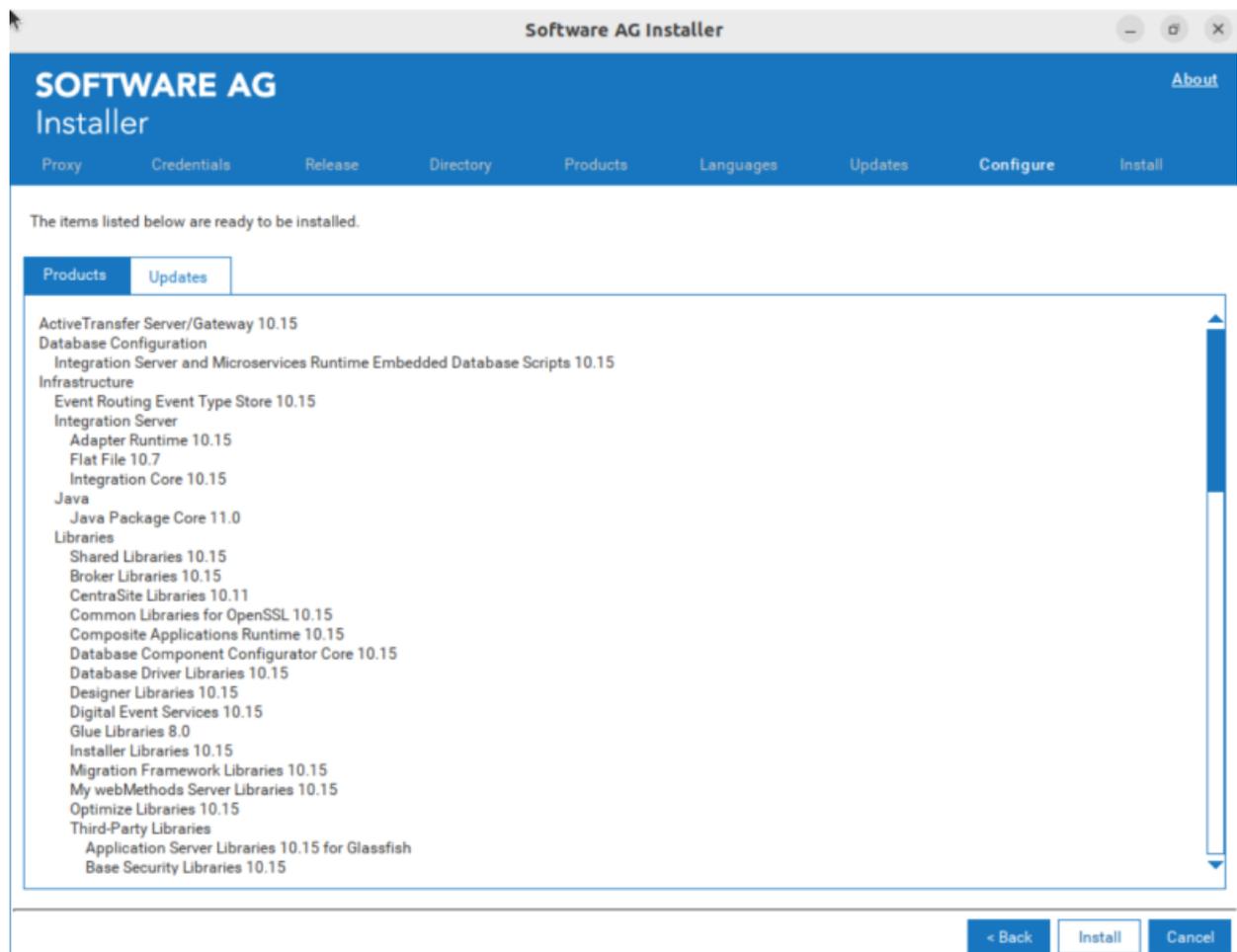
For more information about what database components to install, see the ActiveTransfer Server Database Components section in *Installing Software AG Products*. For more information about how to run the Database Configurator, see the Database Component Configurator Graphical User Interface section in *Installing Software AG Products*.

**Note:**

The database that you configure here must have the MWS database component installed to have all CDS related schema available.



17. Verify your installation details. Click **Install**.



## ActiveTransfer Features

ActiveTransfer offers the following features:

- Listeners: Configure listeners to connect to ActiveTransfer Servers.
- Gateways: Configure Gateway instances to connect to ActiveTransfer Servers that reside behind a firewall.
- Virtual folders: Associate virtual folders with physical locations.
- Actions: Define post-processing or scheduled actions to perform specific tasks.
- Users: Associate existing or new users, groups, or roles with ActiveTransfer.
- Logs: Monitor file transactions, executions of post-processing or scheduled actions, and asset updates in the file transactions, action, and audit logs respectively.

## ActiveTransfer Capabilities

ActiveTransfer offers the following capabilities:

- **Multi-protocol support:** Provides complete support for HTTP, HTTPS, FTP, FTPS (SSL), SFTP (SSH), SCP (server only), SMB (client only), WebDAV, and WebDAVs protocols.

**Note:**

The HTTP(S) port defined in ActiveTransfer can also be used as WebDAV and WebDAVs server respectively.

- **Centralized management:** Provides a centralized interface to manage file transfers, servers, and users. You can set up transfer definitions to facilitate the transfer of entire directories or individual files. You can also control access to file transfers on a per-user basis.
- **Transaction monitoring and analytics:** Provides a centralized interface to browse and search audit logs of all file transfers. A variety of embedded analytics provide insight into all the file transfers happening within your environment by displaying metrics, making comparisons, and summarizing key activities.
- **Business action triggers:** Provides the ability to trigger scheduled or post-processing actions based on file transfer criteria that you specify. For example, you can configure an action to have webMethods Integration Server automatically activate an internal business process, such as order entry or invoicing, if a file transfer is successful. Other actions include executing a file operation (for example, finding, copying, renaming, deleting, encrypting, or zipping the file), executing a script or a Trading Networks service, sending an Universal Messaging or Broker notification, sending an email, or writing a file to the database.
- **Proxy server support:** Provides complete support for file transactions to HTTP, HTTPS, and SOCKS proxy servers for protocols that support these proxy server types.
- **Built-in encryption and security:** Offers complete data security and support for the world's most stringent encryption standards, including SSL and integrated PGP. You can apply global and per-user IP address restrictions. You can also apply policies that can restrict activity during a specific time of the day or days of the week.
- **Client support:** Provides a variety of client interfaces that end users can use to send files to ActiveTransfer Server. End users can upload or download files using a standard web browser.
- **Direct integration:** Integrates files directly into your infrastructure. The tight integration of ActiveTransfer with Integration Server, webMethods Broker, Universal Messaging, and webMethods Trading Networks provides a single platform for interactions based on services, actions, and files.
- **Acceleration:** Accelerated file transfers use a server's complete bandwidth regardless of network latency or distance. Acceleration is performed over HTTPS and does not require opening of other ports in the firewall. File transfers through FTP can also be accelerated by tunneling them through HTTPS. Bandwidth can be controlled either globally or at an individual user level, which ensures that file transfers only occupy a certain percentage of the bandwidth available without affecting other resources on the network.
- **Gateway support:** ActiveTransfer Gateway functions as a reverse proxy server, which acts as an intermediary between the Internet and the internal ActiveTransfer Server for secure file transfers.

- **Failover support for file transfer operations:** Multiple ActiveTransfer Servers can be connected to an ActiveTransfer Gateway. If one server node connected to an ActiveTransfer Gateway fails, another node connected to the ActiveTransfer Gateway automatically takes over the operation of the failed node provided the nodes point to the same ActiveTransfer database. Note that failover is not supported for post-processing actions that fail when an ActiveTransfer Server goes down or for post-processing actions that have not started after a file transfer is complete because ActiveTransfer Server went down.
- **Session replication:** A group of ActiveTransfer Servers can be configured to replicate an ActiveTransfer client session that is in progress on one node, across all other ActiveTransfer Server nodes in the group. So, if one ActiveTransfer Server goes down, the client is directed to another ActiveTransfer Server node in the group and the client session continues without the need for a client re-login.
- **Parallel processing of multiple threads for actions:** Provides you the option of selecting parallel processing of files in multiple threads instead of a single-thread, sequential processing of files for an action. Parallel processing results in quicker and more efficient file processing.
- **Integration with webMethods Trading Networks:** Provides you the option of using a single solution, webMethods Trading Networks, to manage partners for ActiveTransfer actions. In addition, Trading Networks users can use ActiveTransfer as a delivery method to deliver and receive documents. For details on Trading Networks, see the Trading Networks documentation.
- **Integration with Software AG Command Central:** Provides you the option of using Command Central to manage all ActiveTransfer Server instances from a single user interface. With Command Central, you can start, stop, or restart the WmMFT package and ActiveTransfer Server instances; manage listeners, manage licenses, access and download ActiveTransfer Server logs.

## Typical Usage Scenarios

---

Typical business uses of ActiveTransfer include the following:

- Business-to-Business (B2B)
  - Transfers between a manufacturer and a wholesaler
  - Transfers between a wholesaler and a retailer
- Application-to-Application (A2A)
  - Transfers between a bank branch and the central headquarters
  - Transfers between different systems and a mainframe/ERP

## Protocols supported by ActiveTransfer

---

ActiveTransfer supports a specific set of protocols for each asset as follows:

<b>ActiveTransfer asset</b>	<b>Supported protocols</b>
Listeners	FTP, SFTP, HTTP, and HTTPS.
Virtual folders	FTP, FTPES, FTPS, HTTP, HTTPS, SFTP, SMB (1.0, 2.0, and 3.0 versions), WebDAV, and WebDAVs.
Actions	FTP, FTPES, FTPS, HTTP, HTTPS, SFTP, SMB (1.0, 2.0, and 3.0 versions), WebDAV, and WebDAVs.
Proxy servers	HTTP and HTTPS.

# 2 Configuring ActiveTransfer

- Accessing ActiveTransfer New User Interface ..... 32
- Configuring Single Sign-On for ActiveTransfer User Interface ..... 34

## Accessing ActiveTransfer New User Interface

---

After you install ActiveTransfer, ensure that you adhere to the following criteria to access the webMethods ActiveTransfer new user interface.

- Type `http://host:9100` or `https://<host>:9102` (where, *host* is the host name or IP address on which ActiveTransfer Server is running and 9100 and 9102 are the default ports) on a web browser to access the webMethods ActiveTransfer new user interface.

If you want to change the default port, do the following:

1. Navigate to the following installation directory location: *Integration Server\_directory* \ profiles\IS\_default\configuration\com.softwareag.platform.config.propsloader
2. Open the following files:

- `com.softwareag.catalina.connector.http.pid-ActiveTransfer.properties`
- `com.softwareag.catalina.connector.https.pid-ActiveTransfer.properties`

**Note:**

The **keystoreFile** property is used to define the required file path for the keystore, while the **@secure.keystorePass** property is used to set the corresponding password for the key.

3. Update the port number in the port property.
  4. For HTTPS protocol, if you want to use a different version of Transport Layer Security (TLS), do the necessary changes in the `com.softwareag.catalina.connector.http.pid-ActiveTransfer.properties` file. Additionally, if you want to support different ciphers other than the existing list of ciphers, then make the corresponding changes in the same file. ActiveTransfer supports TLSv1.2 by default.
  5. Restart Integration Server.
- Provide users with access to ActiveTransfer screens and functional actions to enable users, Common Directory Service roles, or Integration Server groups to log into ActiveTransfer. For more information, see [“Overview” on page 198](#).
  - webMethods ActiveTransfer new user interface connects to the Integration Server that hosts ActiveTransfer Server for exchanging data. ActiveTransfer Server user interface automatically detects the Integration Server host and port that it needs to connect to. In case you want to specify a different host and port, you can configure the following parameters and restart Integration Server:
    1. Open `properties.cnf` file located in the *Integration Server\_directory* \ instances\*instance\_name*\packages\WmMFT\config directory.
    2. Update the following parameters:

- `mft.isserver.host`: Defines the Integration Server host. Specify the IP address or host name of the machine where ActiveTransfer Server is running. If you do not specify a host name, then 'localhost' is used.
- `mft.isserver.port`: Defines the Integration Server port. Specify the port in the following format: *Protocol@Port*. For example, *Protocol* is either HTTP or HTTPS and *Port* is 5555. The default protocol is HTTP. If you do not specify a port number, then the primary Integration Server port is used.

### 3. Restart Integration Server.

For more information about the properties supported by Integration Server, see *webMethods Integration Server Administrator's Guide*.

## Configuring Single Sign-On for ActiveTransfer Web Client

ActiveTransfer supports Single Sign-On (SSO) through Security Assertion Markup Language (SAML) 2.0, an XML-based framework for the exchange of security information. You can use SAML to access ActiveTransfer web client through SSO. SSO is supported only for HTTPS protocol.

ActiveTransfer serves as the service provider (SP) and communicates between a third-party identity provider (IDP) such as, ADFS, Okta, and so on, to access the target application, ActiveTransfer web client. You can configure ActiveTransfer for exchanging authentication data between the third-party identity provider and ActiveTransfer service provider. The third-party identity provider is the SAML authority and ActiveTransfer is the SAML consumer.

### Who are involved?

- ActiveTransfer administrator, who performs SSO configurations in ActiveTransfer.
- Identity provider administrator, who creates an identity provider account and manages the SSO configurations for ActiveTransfer.
- ActiveTransfer web client users, who use the ActiveTransfer web client to perform file transfers.

### Visual Model



### Preconditions

- Keys for generating signed and encrypted SAML requests

- IP Metadata XML
- User with SSO credentials
- User associated with ActiveTransfer web client through VFS
- Redirection URI, which is the URL generated or shared by the identity provider to access the ActiveTransfer web client
- Third party SAML provider such as ADFS, Keycloak, OKTA and so on

### Basic Flow

To enable SSO for ActiveTransfer Web Client, see [“Configuring Additional Settings for a Listener” on page 40](#).

### How Does SSO Work When The User Accesses ActiveTransfer Web Client?

1. For the first-time login, the user types the ActiveTransfer web client URL (for example, `https://localhost:234`) in a web browser.

The first-time logins are preauthenticated by the browser and redirected to the identity provider for login. The SAML identity window appears.

2. The user types the user name and password.
3. An SSO token is sent through the HTTPS port to the identity provider and results in one of the following:

- The SAML configuration is authenticated successfully.

ActiveTransfer web client is displayed. The user can switch between the applications without having to log in again.

- The SAML configuration is not authenticated successfully and the user authentication fails. In the next login, the user can do one of the following:
  - Bypass SSO login to the HTTPS port by appending `nosso` at the end of the URL. For example, `https://servername:port/nosso`.
  - Login using the user name and password.

## Configuring Single Sign-On for ActiveTransfer User Interface

---

ActiveTransfer supports Single Sign-On (SSO) through Security Assertion Markup Language (SAML) 2.0, an XML-based framework for exchanging security information. You can use SAML to access ActiveTransfer web client through SSO. SSO is supported only for HTTPS protocol.

ActiveTransfer serves as the service provider (SP) and communicates between a third-party identity provider (IDP) such as, ADFS, Okta, and so on, to access the target application, ActiveTransfer web client. You can configure ActiveTransfer for exchanging authentication data between the

third-party identity provider and ActiveTransfer service provider. The third-party identity provider is the SAML authority and ActiveTransfer is the SAML consumer.

### ➤ To enable SSO for ActiveTransfer user interface (UI)

1. Create a WebSSO configuration file at Integration Server\*instances*\default\packages\WmMFT\config\sso

**Note:**

You can also provide the configuration filename that represents the port number. For example, *websso\_9102.properties*.

The WebSSO configuration file requires the below key value pairs:

Key	Key value
SSO_KEYSTORE	C:/softwares/keycloak/keys/keycloak.jks
SSO_SP_MAPPED_PORT	9102
SSO_SP_ENDPOINT_URL	https://localhost:9102/mft/sso
SSO_IDP_METADATA_URL	https://localhost:8443/auth/realms/ TestSAML/protocol/saml/descriptor/  Or  file:///C:/SoftwareAG_105/IDPMetadata.xml
SSO_KEYSTORE_PASSWORD	password in plain text
SSO_KEYSTORE_TYPE	JKS
SSO_SIGN_ALIAS	keycloakssl
SSO_SIGN_ALIAS_PASSWORD	password in plain text
SSO_ENCRYPT_ALIAS	keycloakssl
SSO_ENCRYPT_ALIAS_PASSWORD	password in plain text
SSO_DEFAULT_ALIAS	keycloakssl

**Important:**

- If you want to configure SSO for IDP initiated login, then add the property, SSO\_IDP\_INITIATED\_REDIRECT\_URI in the file (*websso\_9102.properties*) with the IDP initiated URL. For example,  
SSO\_IDP\_INITIATED\_REDIRECT\_URI=https://idp.machine/adfs/ls/idpinitiatedsignon.aspx
- When you configure the WebSSO property file, the system generates the SPMetadata.xml file and downloads the IDPMetadata.xml file in the /sso and /gen directories. However, if you cannot download the IDPMetadata.xml file from the IDP server or file path, copy the content of the hosted IDPMetadata XML file to the generated IDPMetadata.xml file.

- You can restart the server or trigger `wm.mft.sso:initializeSSO` from Designer or Package Management from Integration Server Administrator console to regenerate the property file.
- The SP metadata file needs to be used by the IDP Provider to add the Service Provider.
- You can map multiple values of SSO in your system by creating multiple *sso* configuration files.

# 3 Managing Listeners

- Overview ..... 38
- Features in Listeners ..... 38
- Adding a Listener ..... 40
- Configuring Additional Settings for a Listener ..... 40
- Activating or Deactivating a Listener ..... 48
- Modifying a Listener ..... 49
- Including Listener Information in User Emails ..... 50

## Overview

---

You can configure listeners for ActiveTransfer Server. Each listener is associated with a host, port, and protocol. Clients can connect to ActiveTransfer Server through the configured listeners to transfer files and execute other commands, such as obtaining a directory listing. For example, if you create a listener with port 21 and FTP protocol, clients can connect to ActiveTransfer Server through port 21 by using any standard FTP client, and then transfer files or execute FTP commands.

**Important:**

The references to *Ports* in ActiveTransfer 10.2 and earlier versions are now changed to *Listeners* in the new ActiveTransfer user interface.

You can create and manage any number of listeners on the Listeners page. Ensure that you select ActiveTransfer Server or an ActiveTransfer Gateway instance before you start creating listeners. Each listener in ActiveTransfer Server awaits for a client connection to initiate file transfers.

**Note:**

ActiveTransfer Server does not share listeners with ActiveTransfer Gateway.

You can add listeners to ActiveTransfer Server or an ActiveTransfer Gateway instance that enables you to perform file transfers by configuring basic settings, such as name, port, and protocol using the quick add feature. To configure additional settings for listeners, see [“Configuring Additional Settings for a Listener” on page 40](#).

## Features in Listeners

---

This topic provides information about specific features you can use to configure listeners in ActiveTransfer:

### Access

You can configure access settings for a listener that uses FTP protocol for ActiveTransfer Server or an ActiveTransfer Gateway instance. The ActiveTransfer Server or an ActiveTransfer Gateway instance can work in the following FTP modes:

- In passive FTP mode, the client initiates a connection to the server specified from the range of port numbers for such a data connection. This is the default mode. This mode is used when it is not possible to create an outgoing connection to a client machine. For example, when a firewall imposes restrictions on connections.
- In active FTP mode, the server creates an outgoing connection through the specified listener to the client machine for data transfer as specified in the FTP commands issued by the client.

**Note:**

Ensure that you provide access for the listener in your firewall settings. Otherwise, connections between the client machine and ActiveTransfer Server might be blocked.

## Encryption

You can configure encryption methods for ActiveTransfer Server or ActiveTransfer Gateway listeners that use FTP protocol.

ActiveTransfer supports Transport Layer Security (TLSv1) and Secure Sockets Layer (SSLv3) cryptographic protocols that provide internet communication security. FTP protocol uses two types of client security methods:

- **Explicit:** Connections between an FTPS-aware server and the clients remain secure even if the clients are not FTPS-aware.
- **Implicit:** SSL authentication is used for all clients that connect with the FTPS server for each session. This method is not compatible with clients that are not FTPS-aware.

## SSH Server Host Keys

ActiveTransfer supports both RSA and DSA encryptions.

### Note:

When you create a default SFTP listener in ActiveTransfer Server or ActiveTransfer Gateway instance, the default RSA and DSA keys are used for login. The default RSA and DSA keys are adequate for demo or testing purposes. However, in production environments, we recommend that you replace these default keys with your own RSA and DSA keys.

## SSH Supported Ciphers

Ciphers are algorithms that are used to encrypt or decrypt data. In ActiveTransfer, you can configure the ciphers supported for SSH. The aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr, and arcfour256 ciphers require strong Java security policy certificates. You need to set the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for your JDK/JRE in order to use these ciphers. Java comes with a default maximum key strength of 128 bytes.

## SSH Connection Settings

You can configure the following SSH connection settings:

- Default character encoding that controls how ASCII characters are encoded when sent to a client.
- Use of asynchronous threading to enable tasks to run in parallel. Asynchronous threading is useful to transfer a file to multiple external locations concurrently instead of sequentially.
- Number of seconds to wait before disconnecting an idle connection.
- Handshake options to use when establishing a secure connection with a partner.

## Adding a Listener

---

You can add a listener to ActiveTransfer Server or an ActiveTransfer Gateway instance using the quick add feature. To configure additional settings for the listener, see [“Configuring Additional Settings for a Listener”](#) on page 40.

### > To add a listener

1. On the navigation pane, select **Listeners**.
2. On the Listeners page, from the **Instance** list, select the ActiveTransfer Server or an ActiveTransfer Gateway instance.
3. Click .
4. In the Add listener dialog box, specify the following details:

Field	Description
<b>Name</b>	Type a unique name for the listener.
<b>Protocol</b>	Select the required protocol from the list.
<b>Port</b>	Type a unique port number for the ActiveTransfer Server or ActiveTransfer Gateway instance.  <b>Note:</b> Ensure that the specified port is not used by any application, including the default ports used for ActiveTransfer Server and ActiveTransfer Gateway (2080 and 8500, respectively).
<b>Activate listener</b>	Select this option to activate and run the listener in all the ActiveTransfer instances.

5. Click **Add**.

The new listener appears in the listeners list.

## Configuring Additional Settings for a Listener

---

You can configure additional settings for a listener based on the protocol (FTP, SFTP, HTTP, or HTTPS) used by the listener.

### > To configure additional settings

1. On the navigation pane, select **Listeners**.
2. On the Listeners page, from the **Instance** list, select the ActiveTransfer Server or an ActiveTransfer Gateway instance.
3. Click on the listener for which you want to configure additional settings and specify the required details:
  - For a listener using *FTP* or *FTPS* protocol:

Field	Description
<b>Activate listener</b>	Select this option to activate and run the listener in all the ActiveTransfer instances.
<b>Bindings</b>	
<b>Name</b>	Type a unique name for the listener.
<b>Host</b>	Type a host name or IP address. <code>localhost</code> is the default. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;"> <p><b>Note:</b> A listener created with <code>localhost</code> as the host will be accessible through all the IPs assigned to the host machine.</p> </div>
<b>Port</b>	Type a unique port number. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;"> <p><b>Note:</b> Make sure that the port you specify is not used by any application, including the default ports used for ActiveTransfer Server and ActiveTransfer Gateway (2080 and 8500, respectively).</p> </div>
<b>Share this information with the user through email</b>	Select this option if you want to mention that this port number is used along with the other listener information such as, listener name, host, port, protocol, creation of a new user account, modification to the credentials or server connection details for a user, or permissions granted to folders in the email shared with the user.
<b>Support single sign-on</b>	Select this option if you want to enable SSO for this listener.  For more information about configuring SSO, see <a href="#">“Configuring Single Sign-On for ActiveTransfer Web Client” on page 33</a> . Also, to understand how client certificate authentication affects this field, see the description of <b>Require valid client certificate and password</b> .
<b>Access</b>	
<b>Passive port range</b>	Type the <b>From</b> and <b>To</b> range of port numbers that can be used for passive port connections.
<b>Passive IP address</b>	Do one of the following:

Field	Description
	<ul style="list-style-type: none"> <li>■ If you want ActiveTransfer Server to automatically assign the IP address or host name of the server based on the listener configuration, type <code>Auto</code>.</li> <li>■ If you want to provide a specific IP address manually, type the IP address to use for the passive IP address.</li> </ul>
<b>Welcome message</b>	Type a welcome message for display in the client console (example, ActiveTransfer web client, FileZilla client, and so on) when a user logs in.
<b>Router/Firewall aware</b>	<p>Select this option if the incoming client connections are routed through a router or firewall, that is FTP-aware. FTP-aware routers and firewalls inspect the FTP command and response, and might modify the response.</p> <p>It is possible that a client cannot connect to ActiveTransfer Server or transfer files even when a listener is active. This happens when either a firewall exists between the client and the server or the virtual private network the client uses has altered the IP address given to ActiveTransfer Server.</p> <p><b>Note:</b> Check your firewall configuration before selecting this option.</p>
<b>SSL options</b>	
<b>Activate</b>	Select this option to activate SSL encryption.
<b>Keystore alias</b>	Type the certificate alias for the keystore password.
	<p><b>Note:</b> This keystore file overrides any global SSL encryption settings that apply to all listeners on the server.</p>
<b>Truststore alias</b>	Type the certificate alias for the private key password.
<b>Require valid client certificate</b>	<p>Select this option if you want to allow connections for clients with a valid client certificate.</p> <p>When this option is selected, ActiveTransfer Server expects the clients requesting a server connection to present a valid certificate. The certificate should match one of the certificates stored in the truststore.</p> <p>For details on how to map client certificates to users, see "User Certificate Mapping" section in the document.</p> <p>When establishing a connection with the server, ActiveTransfer validates only the client certificate but not the password.</p>

Field	Description
	<p><b>Tip:</b> To store valid certificates:</p> <ol style="list-style-type: none"> <li>1. Create a truststore file in the same location as the keystore file named <i>keystoreName_trust</i>. For example, if the keystore file name is <i>server_ks.jks</i>, the truststore file name should be <i>server_ks.jks_trust</i>.</li> <li>2. Add the valid client certificates to this truststore.</li> </ol>
<b>Require valid client certificate and password</b>	Select this option if you want ActiveTransfer to validate both the client certificate and the password when establishing a connection with the server.
<b>Encryption</b>	
<b>Explicit SSL</b>	<p>Select this option to enable support for explicit SSL for use in encryption mode (FTPES).</p> <p>Select the <b>Require encryption</b> option to force the client to use the data transfer encryption mode while connecting to an FTP server. In this mode, the client cannot switch off the channel encryption.</p>
<b>Implicit SSL</b>	Select this option to enable support for implicit SSL for use in encryption mode (FTPES). SSL is used on all the clients in each session.
<b>Protocols</b>	<p>Select one or more of the following supported protocols for explicit SSL or implicit SSL encryption modes:</p> <ul style="list-style-type: none"> <li>■ <b>TLSv1.2</b></li> <li>■ <b>TLSv1.1</b></li> <li>■ <b>TLSv1.0</b></li> <li>■ <b>SSLv3</b></li> </ul> <p><b>Note:</b> In JDK 8u31, JDK 7u75, JDK 6u91, and later version, SSLv3 is disabled by default. To use SSLv3, you must manually enable SSLv3 in JVM.</p>
<b>Priority options</b>	
<b>Command delay interval (in ms)</b>	Type the command delay interval in milliseconds to add a pause between each command in order to slow down clients that continually access the server.

- For a listener using *SFTP* protocol:

Field	Description
<b>Activate listener</b>	Select this option to activate and run the listener in all the ActiveTransfer instances.
<b>Bindings</b>	
<b>Name</b>	Type a unique name for the listener.
<b>Host</b>	Type a host name or IP address. <code>localhost</code> is the default.  <b>Note:</b> A listener created with <code>localhost</code> as the host will be accessible through all the IPs assigned to the host machine.
<b>Port</b>	Type a unique port number.  <b>Note:</b> Make sure that the port you specify is not used by any application, including the default ports used for ActiveTransfer Server and ActiveTransfer Gateway (2080 and 8500, respectively).
<b>Share this information with the user through email</b>	Select this option if you want to mention that this port number is used along with the other listener information such as, listener name, host, port, protocol, creation of a new user account, modification to the credentials or server connection details for a user, or permissions granted to folders in the email shared with the user.
<b>SSH: Server host keys</b>	
<b>Note:</b> When RSA/DSA host keys are configured and not found in the file system, ActiveTransfer generates the RSA/DSA host keys (private keys) in the specified location. If only the file name is mentioned, then ActiveTransfer generates the private keys in the default location, <code>Installation_directory\IntegrationServer\instances\default</code> .	
<b>RSA alias</b>	Select <b>Active</b> to enable RSA encryption, and type the certificate alias for the RSA algorithm.
<b>DSA alias</b>	Select <b>Active</b> to enable DSA encryption, and type the certificate alias for the DSA algorithm.
<b>SSH: Authentication</b>	
<b>Require password authentication</b>	Select this option if you want to make password authentication mandatory for a user.
<b>Require public key authentication</b>	Select this option if you want to make public key authentication mandatory for a user.
<b>SSH: Supported ciphers</b>	Select the required ciphers from the list.

Field	Description
<b>SSH: Supported MAC</b>	Select the supported keyed-hash message authentication codes (HMACs) for verification of data integrity from the list.
<b>SSH: Connection settings</b>	
<b>Use asynchronous threading</b>	Select this option if you want to use asynchronous threading to enable multiple file transfers to run concurrently.
<b>Idle timeout (sec)</b>	Type a timeout value in seconds for disconnecting an idle connection.
<b>Priority options</b>	
<b>Command delay interval (ms)</b>	Type a command delay interval in milliseconds to add a pause between each command in order to slow down clients that continually access the server.

- For a listener using *HTTP* or *HTTPS* protocol:

Field	Description
<b>Activate listener</b>	Select this option to activate and run the listener in all the ActiveTransfer instances.
<b>Bindings</b>	
<b>Name</b>	Type a unique name for the listener.
<b>Host</b>	Type a host name or IP address. <code>localhost</code> is the default.
	<b>Note:</b> A listener created with <i>localhost</i> as the host will be accessible through all the IPs assigned to the host machine.
<b>Port</b>	Type a unique port number.
	<b>Note:</b> Make sure that the port you specify is not used by any application, including the default ports used for ActiveTransfer Server and ActiveTransfer Gateway (2080 and 8500, respectively).
<b>Share this information with the user through email</b>	Select this option if you want to mention that this port number is used along with the other listener information such as, listener name, host, port, protocol, creation of a new user account, modification to the credentials or server connection details for a user, or permissions granted to folders in the email shared with the user.
<b>Support single sign-on</b>	Select this option if you want to enable SSO for this listener.  For more information about configuring SSO, see <a href="#">“Configuring Single Sign-On for ActiveTransfer Web Client”</a> on page 33. Also, to

Field	Description
	understand how client certificate authentication affects this field, see the description of <b>Require valid client certificate and password</b> .
<b>SSL options</b>	
<b>Keystore alias</b>	Type or browse to the path to the keystore file. ActiveTransfer Server loads the truststore file from the keystore file path, <Keystore-File-Path>_trust. For example, C://keystore/key for Windows and /usr/keystore/key for UNIX. <p><b>Note:</b> This keystore file overrides any global SSL encryption settings that apply to all listeners on the server.</p>
<b>Truststore alias</b>	Type the certificate alias for the private key password.
<b>Require valid client certificate</b>	Select this option if you want to allow connections for clients with a valid client certificate. <p>When this option is selected, ActiveTransfer Server expects the clients requesting a server connection to present a valid certificate. The certificate should match one of the certificates stored in the truststore.</p> <p>For details on how to map client certificates to users, see "User Certificate Mapping" section in the document.</p> <p>When establishing a connection with the server, ActiveTransfer validates only the client certificate but not the password.</p> <p><b>Tip:</b> To store valid certificates:</p> <ol style="list-style-type: none"> <li>1. Create a truststore file in the same location as the keystore file named <i>keystoreName_trust</i>. For example, if the keystore file name is <i>server_ks.jks</i>, the truststore file name should be <i>server_ks.jks_trust</i>.</li> <li>2. Add the valid client certificates to this truststore.</li> </ol>
<b>Require valid client certificate and password</b>	Select this option if you want ActiveTransfer to validate both the client certificate and the password when establishing a connection with the server.
<b>Protocols</b>	Select one or more of the following supported protocols for explicit SSL or implicit SSL encryption modes: <ul style="list-style-type: none"> <li>■ <b>TLSv1.2</b></li> <li>■ <b>TLSv1.1</b></li> <li>■ <b>TLSv1.0</b></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>SSLv3</b></li> </ul> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> In JDK 8u31, JDK 7u75, JDK 6u91, and later version, SSLv3 is disabled by default. To use SSLv3, you must manually enable SSLv3 in JVM.</p> </div>
<b>Priority options</b>	
<b>Command delay interval (ms)</b>	Type a command delay interval in milliseconds to add a pause between each command in order to slow down clients that continually access the server.

4. Click **Save** or **Save & Close**.

The ActiveTransfer Server or ActiveTransfer Gateway instance is updated with the additional settings.

## Configuring Single Sign-On for ActiveTransfer

ActiveTransfer supports Single Sign-On (SSO) through Security Assertion Markup Language (SAML) 2.0, an XML-based framework for the exchange of security information. You can use SAML to access ActiveTransfer web client through SSO. SSO is supported only for HTTPS protocol.

ActiveTransfer serves as the service provider (SP) and communicates between a third-party identity provider (IDP) such as, ADFS, Okta, and so on, to access the target application, ActiveTransfer web client. You can configure ActiveTransfer for exchanging authentication data between the third-party identity provider and ActiveTransfer service provider. The third-party identity provider is the SAML authority and ActiveTransfer is the SAML consumer.

### Configuring Single Sign-On in Listeners User Interface

#### ➤ To enable SSO for ActiveTransfer Web Client in Listeners user interface (UI)

1. Enable the system property, `mft.server.https.auth.saml` to `true` in the `Integration Server_directory \instances\ instance_name \packages\WmMFT\config\properties.cnf` file.
2. Enable the **Support Single Sign-On (SSO)** checkbox in the Server Management page for the port.
3. Specify the details for the following fields:

Field	Details
<b>ActiveTransfer certificate alias</b>	Configure the keystore in certificate management for the certificate alias to generate the SAML tokens.
<b>Service provider endpoint URL</b>	https://localhost:2343
<b>IDP metadata URL</b>	https://localhost:8443/auth/realms/ TestSAML/protocol/saml/descriptor/  Or  file:///C:/SoftwareAG_105/IDPMetadata.xml
<b>Sign alias</b>	keycloakssl
<b>Encrypt alias</b>	keycloakssl
<b>Default alias</b>	keycloakssl

**Important:**

- If you want to configure Single Sign-On for IDP initiated login through URI, then enable the **IDP Initiated SSO** option and specify the IDP initiated redirect URI.
- When you configure WebSSO in listeners UI, the system generates the `SPMetadata.xml` file and downloads the `IDPMetadata.xml` file in the `/sso` and `/gen` directories. However, if you cannot download the `IDPMetadata.xml` file from the IDP server or file path, then copy the content of the hosted IDPMetadata XML to the generated `IDPMetadata.xml` file. You can download the `SPMetadata.xml` file by clicking on the **Download SP Metadata** option.
- You can trigger the **Initialize** option in the listeners UI to regenerate the property file.
- The SP metadata file needs to be used by the IDP Provider to add the Service Provider.
- You can map multiple values of SSO for multiple ports by selecting the respective port number in listeners UI.

**IDP initiated Single Sign-On in Properties.cnf**

To enable IDP initiated Single Sign-on in `properties.cnf`, use the property `mft.server.https.auth.saml.redirecturi` and enable the **IDP initiated SSO** option.

**Activating or Deactivating a Listener**

When you activate a listener, ActiveTransfer starts the listener in all the instances. When you deactivate a listener, ActiveTransfer stops the listener in all the instances.

**Note:**

- When you start or stop a listener, the listener is started or stopped only on that ActiveTransfer Server or ActiveTransfer Gateway instance. However, when you activate or deactivate a listener, the listener is started or stopped on all ActiveTransfer Server instances or that specific ActiveTransfer Gateway instance.
- Ensure to activate a listener before you start it.

- Disabled listeners will not start when Integration Server is restarted or WmMFT package is reloaded.

#### ➤ To activate and start a listener

1. On the navigation pane, select **Listeners**.
2. On the Listeners page, from the **Instance** list, select the ActiveTransfer Server or an ActiveTransfer Gateway instance.
3. Click on an inactive listener.
4. Under **Bindings**, select **Activate listener** and click **Save**.

The listener is activated and ActiveTransfer starts the listener in all the ActiveTransfer Server instances and or this specific ActiveTransfer Gateway instance.

5. Click the toggle button  or  to start or stop the listener respectively.

#### ➤ To deactivate and stop a listener

1. On the navigation pane, select **Listeners**.
2. On the Listeners page, from the **Instance** list, select the ActiveTransfer Server or an ActiveTransfer Gateway instance.
3. Click on an active listener.
4. Under **Bindings**, deselect **Activate listener** and click **Save**.

The listener is deactivated and ActiveTransfer stops the listener in all the ActiveTransfer Server instances and or this specific ActiveTransfer Gateway instance.

## Modifying a Listener

---

You can edit the configuration settings of an existing listener created for the ActiveTransfer Server or ActiveTransfer Gateway instance.

#### ➤ To modify a listener

1. On the navigation pane, select **Listeners**.
2. On the Listeners page, from the **Instance** list, select the ActiveTransfer Server or an ActiveTransfer Gateway instance.
3. Click on a listener that you want to edit.
4. Modify the required configuration settings for the listener.
5. Click **Save** or **Save & Close**.

The ActiveTransfer Server or ActiveTransfer Gateway instance is updated with the modified settings.

## Including Listener Information in User Emails

---

When you create a new user account or edit the credentials or server connection details for a user, you can alert the user of the changes by way of email. You can specify the listener name, host, port, and protocol information in these alert emails.

### ➤ To include listener information in user emails

1. On the navigation pane, select **Listeners**.
2. In the Listeners page, select ActiveTransfer Server or ActiveTransfer Gateway instance.
3. Click on a listener.
4. Select **Include this information in the user credential email**.
5. Click **Save**.

The listener is enabled to include listener information in emails and appear under the **Default in emails** column.

# 4 API Support for HTTP file operations

- Introduction ..... 52
- Creating a folder ..... 53
- Deleting a file or a folder ..... 53
- Renaming a file or folder ..... 54
- Uploading a file ..... 54
- Listing of files ..... 55
- Verifying the input ..... 55
- Downloading a file ..... 56

## Introduction

ActiveTransfer supports file operations on HTTP listeners using the webClient. You can now perform file operations in ActiveTransfer using Application Programming Interfaces (APIs) without any dependency on the webClient. To use this API feature, you must create a listener in ActiveTransfer and then log in to that listener port using the same user previously used in the webClient.

### Pre-requisites:

- Create an HTTP listener in ActiveTransfer.
- Log in to the listener port using your webClient user credentials. Use the same user with basic authentication when using the APIs.
- Remove any unnecessary headers apart from the headers in the tables below.
- Use only single value inputs in the API requests.
- Check your user access permissions in the VFS configuration. APIs work based on these permissions.
- Check for validations for the API URL, payload parameters, payload and list of supported commands.

The supported APIs are listed below:

- Supported formats: Form-data, JSON
- HTTP Method: POST

### Note:

The API for uploading a file only supports the Form-data format.

Supported APIs	URL End-point
Creating a folder	http://<serverhost>:<port number>/api/createFolder
Deleting a file or a folder	http://<serverhost>:<port number>/api/delete
Renaming a file or a folder	http://<serverhost>:<port number>/api/rename
Uploading a file	http://<serverhost>:<port number>/api/upload
Listing of files in a specified path	http://<serverhost>:<port number>/api/list
Verifying if a given input is a file or a folder	http://<server host>:<port number>/api/isFile
Downloading a file	http://<server host>:<port number>/api/download

## Creating a folder

Use this API to create a folder with the given path.

Payload type	Body	Headers
form-data (key-value)	filepath: <vfs path for which the user is accessible to>	Authorization Content-Type: multipart/form-data; boundary=<calculated when the request is sent>
JSON	{ "path":"/vfspath/" }	Authorization Content-Type: application/json

### Response

```
{
  "success": "true" <If API request is success and false in case of failure>,
  "responseMessage": " < message associated with the operation.> "
}
```

## Deleting a file or a folder

Use this API to delete a file or folder.

Payload type	Body	Headers
form-data (key-value)	filepath: <vfs path for which the user is accessible to>	Authorization Content-Type: multipart/form-data; boundary=<calculated when the request is sent>
JSON	{ "path":"/vfspath/" }	Authorization Content-Type: application/json

### Response

```
{
  "success": "true" <If API request is success and false in case of failure>,
  "responseMessage": " < message associated with the operation.> "
}
```

## Renaming a file or folder

Use this API to rename a file or folder.

Payload type	Body	Headers
form-data (key-value)	renameFrom: <source filename>	Authorization
	renameTo: <target filename>	Content-Type: multipart/form-data; boundary=<calculated when the request is sent>
JSON	<pre>{   "path":"/local1/",   "renameFrom":"test1/",   "renameTo":"test1111" }</pre>	Authorization
		Content-Type: application/json

### Response

```
{
  "success": "true" <If API request is success and false in case of failure>,
  "responseMessage": " < message associated with the operation.> "
}
```

## Uploading a file

Use this API to upload a file.

Payload type	Body	Headers
form-data (key-value)	uploadPath: <vfs path for which the user is accessible to>	Authorization
	file: <file to be uploaded>	Content-Type: multipart/form-data; boundary=<calculated when the request is sent>

### Response

```
{
  "success": "true" <If API request is success and false in case of failure>,
  "responseMessage": " < message associated with the operation.> "
}
```

## Listing of files

Use this API to list all the files for a given path.

Payload type	Body	Headers
form-data (key-value)	filepath: <vfs path for which the user is accessible to>	Authorization Content-Type: multipart/form-data; boundary=<calculated when the request is sent>
JSON	{ "path":"/vfspath/" }	Authorization Content-Type: application/json

### Response

```
{
  "success": "true" <If API request is success and false in case of failure>,
  "responseMessage": " < message associated with the operation.> "
}
```

## Verifying the input

Use this API to verify if the input is a file or a folder.

Payload type	Body	Headers
form-data (key-value)	filepath: <vfs path for which the user is accessible to>	Authorization Content-Type: multipart/form-data; boundary=<calculated when the request is sent>
JSON	{ "path":"/vfspath/" }	Authorization Content-Type: application/json

### Response

```
{
  "success": "true" <If API request is success and false in case of failure>,
  "responseMessage": " true: in case of a file and false: in case of a folder."
  "file": true in case of a file and false in case of folder or directory.
}
```

## Downloading a file

Use this API to download a file.

Payload type	Body	Headers
form-data (key-value)	path: <filename>  isFile: true	Authorization
		Content-Type: multipart/form-data; boundary=<calculated when the request is sent>
JSON	<pre>{   "path":"/httpapi/ActiveTransfer.log",   "isFile":"true" }</pre>	Authorization
		Content-Type: application/json

### Response

```
{
  "success": "true (in case of api request is success and false in case of failure)",
  "responseMessage": "message associated to the operation."
}
```

# 5 Managing Gateways

■ Overview .....	58
■ Features in Gateways .....	58
■ Adding a Gateway .....	59
■ Configuring Additional Settings for a Gateway .....	60
■ Modifying a Gateway .....	61

## Overview

---

If your ActiveTransfer Server resides behind a firewall and does not accept communications from external clients through a DMZ, you can configure a dedicated ActiveTransfer Gateway that permits the internal ActiveTransfer Server to process requests for external clients. With an ActiveTransfer Gateway placed in the DMZ, users can establish a connection with a server inside a firewall using any of the protocols that ActiveTransfer supports.

If the client connections to ActiveTransfer Server are routed using an ActiveTransfer Gateway, the internal firewall is required to open only the connections required from ActiveTransfer Server to ActiveTransfer Gateway (that is, outbound connections from the internal network to the DMZ). There is no need to open inbound connections in the firewall from the DMZ to the internal network. By limiting the connections to only those established by the internal server, the Gateway architecture makes it extremely difficult for an attacker to directly penetrate the internal network, even if the attacker manages to subvert a system within the DMZ.

You can add Gateways in ActiveTransfer that enables you to perform file transfers by configuring basic settings, such as name, host, and port using the quick add feature. To configure additional settings for Gateways, see [“Configuring Additional Settings for a Gateway”](#) on page 60.

## Features in Gateways

---

This topic provides information about specific features you can use to configure Gateways in ActiveTransfer:

### Antivirus Scanning

You can configure an ActiveTransfer Gateway instance to connect to an Internet Content Adaptation Protocol (ICAP) server, which is, configured for antivirus filters that suit your organization's requirements. Each ActiveTransfer Gateway instance can have only one ICAP server configured. If you have multiple ActiveTransfer Gateway instances, you must configure the antivirus scan settings on each instance.

The pre-requisites to configure the antivirus scan settings on each instance are:

- Configuration of the JVM memory in ActiveTransfer Gateway.
- ICAP server must be accessible from ActiveTransfer Gateway.

### Service Configuration for ICAP Server

You can specify the virus scan service name of the ICAP server and the run-time parameter values to send to the ICAP server in the following format: *service name?parameter1 value&parameter2 value&parameter3...*

Here, ... indicates any additional parameters that you might want to include.

For example, the c-icap server's virus service expects the following parameters `virus_scan?allow204=onforce=on sizelimit=off mode=simple`

Where:

- `allow_204=on` enables 204 (no content) responses outside previews for virus scan if the ICAP client does not support it. If the 204 response to the virus scan request is `No modification needed` indicates that no virus was found in the file.
- `force=on` enables the scan of the file even if its file type is not included in the `srv_clamav.ScanFileTypes` directive in `c-icap.conf` file.
- `sizeLimit=off` enables the virus scan service to ignore the `srv_clamav.MaxObjectSize` directive in `c-icap.conf` file.
- `mode=simple` enables the 204 response only when no virus is found and an error message if a virus found.

For more details on the parameters you can use, see the ICAP server documentation.

## Adding a Gateway

You can add a Gateway instance that would serve as a proxy for an ActiveTransfer Server instance using the quick add feature. To configure additional settings for the Gateway, see [“Configuring Additional Settings for a Gateway” on page 60](#).

### ➤ To add a Gateway

1. On the navigation pane, select **Gateways**.
2. On the Gateways page, click .
3. In the Add gateway dialog box, specify the following details:

Field	Description
<b>Name</b>	Type a unique name for the Gateway.
<b>Host</b>	Type the host or IP address for the ActiveTransfer Gateway instance.
<b>Port</b>	Type the registration port number through which ActiveTransfer Server will connect to the ActiveTransfer Gateway. Specify the same port that you specified in the <code>mft.gatewayServer.port</code> parameter for ActiveTransfer Gateway. The default port is 8500. To view the property <code>mft.gatewayServer.port</code> go to the file path <code>installation_directory\IntegrationServer\instances&lt;InstanceName&gt;\packages\WmMFT\config\properties.cnf</code> in ActiveTransfer Gateway and refer the file <code>property.cnf</code> .

4. Click **Add**.

The new Gateway appears in the Gateways list. The Gateway instances that you add here are also listed in the server selection list on the Listeners and Listener preferences pages.

## Configuring Additional Settings for a Gateway

You can configure additional settings for an ActiveTransfer Gateway instance.

### > To configure additional settings

1. On the navigation pane, select **Gateways**.
2. On the Gateways page, click on the Gateway instance for which you want to configure additional settings, and specify the required details:

Field	Description
<b>Status</b>	
<b>Connect to ActiveTransfer Gateway</b>	<p>Select this option to establish a connection between the Gateway and the specified ActiveTransfer Server, if not already connected.</p> <p><b>Note:</b> If the ActiveTransfer Server is connected to another ActiveTransfer Gateway instance, then clear this option to disconnect ActiveTransfer Gateway from ActiveTransfer Server the next time the server restarts.</p> <p><b>Tip:</b> Click  to refresh the status.</p>
<b>Settings</b>	
<b>Name</b>	Type a unique name for the Gateway.
<b>Host</b>	Type the host or IP address where the Gateway is running. For example, 10.20.30.40.
<b>Port</b>	Type the port number through which ActiveTransfer Server will connect to the ActiveTransfer Gateway. For example, 8500.
<b>Antivirus</b>	
<b>Activate antivirus scan</b>	<p>Select this option to perform a virus scan check on all the files that are uploaded.</p> <p><b>Note:</b></p>

Field	Description
	You can deactivate virus scanning at any time by clearing the <b>Activate antivirus scan</b> selection.
<b>ICAP server name</b>	Type a suitable name for the ICAP server.
<b>Host</b>	Type the host name or IP address of the server that hosts the ICAP server. For example, localhost or 10.20.30.40.
<b>Port</b>	Type the port number assigned to the ICAP server host that is running. For example, 80.
<b>Service configuration</b>	Specify the virus scan service name of the ICAP server and the run-time parameter values to send to the ICAP server in the following format:  <i>servicename?parameter1value&amp;parameter2value&amp;parameter3value&amp;..</i>  For more information about the parameter and values, see the <a href="#">“Features in Gateways” on page 58</a> section.
<b>Scan buffer size per upload (MB)</b>	Type the maximum data buffer size in megabytes that ActiveTransfer Gateway must store in-memory for an individual upload before streaming the file data to the ICAP server for scanning.
<b>Total scan buffer size (MB)</b>	Type the maximum data buffer size in megabytes that ActiveTransfer Gateway must store in-memory for all uploads across all user sessions. When ActiveTransfer Gateway reaches this limit, it refuses to accept any additional uploads and the file transactions fail.

3. Click **Test Connection** to check the ActiveTransfer Gateway connection to the ICAP server.

ActiveTransfer Gateway starts forwarding all inbound files to the ICAP server for virus scanning.

4. Click **Save** or **Save & Close**.

The Gateway instance is updated with the additional settings.

## Modifying a Gateway

You can edit the configuration settings of an existing ActiveTransfer Gateway instance.

### > To modify a Gateway

1. On the navigation pane, select **Gateways**.

2. On the Gateways page, click on a Gateway that you want to edit.
3. Modify the required configuration settings for the Gateway.
4. Click **Save** or **Save & Close**.

The Gateway instance is updated with the modified settings.

# 6 Managing Virtual Folders

■ Overview .....	64
■ Features in Virtual Folders .....	64
■ Adding a Virtual Folder .....	66
■ Configuring Additional Settings for a Virtual Folder .....	66
■ Modifying a Virtual Folder .....	75
■ Searching for Virtual Folders .....	75

## Overview

---

ActiveTransfer enables you to create a Virtual File System (VFS) to provide an abstract view of resources in your physical file system or on a remote server such as, another FTP server. This capability enables users and client applications to access a variety of file structures in a uniform way. Although the information in a virtual folder might be physically stored across one or more local or remote file systems in your enterprise, it appears as a cohesive data collection in the VFS. You can create a VFS by creating one or more *virtual folders*, which you typically arrange in a file system hierarchy.

For example, you can create a group of virtual folders to categorize your organization's sales for various years. At the top level of folders, you can create a group of separate virtual folders, each representing one year of sales. Inside each yearly virtual folder, you can create 12 virtual folders to represent the monthly sales data for that year.

After you create a virtual folder, you can assign users to the folder and specify each user's access privileges to the folder. When the users log on to ActiveTransfer, they can view the folders they have access to and resources within those folders. This way, you can store different types of data (for example, sales data and customer profile information) on the same physical file system, yet control user access to that data accordingly.

A VFS also bridges the differences between file systems on various operating systems so that users and applications can access files without having to know the type of file system they access.

Any configuration changes in the VFS now get applied to all the active user sessions as well. This behavior appears for webMethods ActiveTransfer version 10.7 and later.

## Features in Virtual Folders

---

This topic provides information about specific features you can use to configure virtual folders in ActiveTransfer:

### Encryption and Decryption Options for a Virtual Folder

You can define specific file-based encryption and decryption PGP keys for a virtual folder. When files are uploaded or downloaded to the virtual folder through the ActiveTransfer Server, ActiveTransfer encrypts or decrypts the files in the stream. Encrypted files are decrypted only if they are transferred back through ActiveTransfer using the private key or public key that was used to encrypt them.

The encryption and decryption settings are applicable only when a user connects to ActiveTransfer Server and performs an upload or download operation. ActiveTransfer does not use these keys when the virtual folder is used in an action. If you want to use the encryption and decryption keys in an action, create an encryption or decryption task in the action.

When encryption and decryption keys are configured at multiple levels (user, listener, and virtual folder), ActiveTransfer enforces the following order of preference:

1. Users

2. Virtual folders
3. Listeners

For example, if user *A* accesses port *10* and uploads a file in VFS *MN*, then ActiveTransfer checks if the encryption or decryption key is available for user *A*. If no key is available at the user level, then ActiveTransfer checks for the virtual folder settings for a key. If no key is present at the folder level, then ActiveTransfer checks the server level settings for the key.

## User, Group, and Role Permission Propagation for a Folder

ActiveTransfer propagates user, role, or group permissions for virtual folders as follows:

- If you grant user, role, or group permissions to a parent folder, the user will also have the same permissions to all subfolders.
- If you grant a user, role, or group permissions to a subfolder, the user will automatically have the permission to traverse through the parent folders.
- You can override the inherited permissions and specify a different set of permissions to a folder for a user, role, or group. These new permissions are then inherited by the subfolders within the folder.

## Use of Special Characters in Search

ActiveTransfer allows you to use the following special characters in search strings.

### Wildcard Search

Depending on whether you want a broad or narrow search results containing the search strings provided, you can either use an asterisk or question mark as wildcard characters.

- \*. The asterisk, along with other search characters, gives you all matches that include the search string characters.

*Example:* The search string `*abc.txt` gives these results:

`kweihdabc.txt, abc.txt, 874abc.txt, 1abc.txt, aabc.txt, _abc.txt`

- ?. The question mark, along with other search string characters, gives you only those matches that include one character in place of the question mark and the other search string characters.

*Example:* The search string `?abc.txt` gives these results:

`1abc.txt, aabc.txt, _abc.txt`

### Exact Match Search

For exact keyword searches, place the search string within single quotation marks.

*Example:* The search string `'abc.txt'` returns only `abc.txt` as the search result.

## Adding a Virtual Folder

---

You can add a virtual folder using the quick add feature. To configure additional settings for the virtual folder, see [“Configuring Additional Settings for a Virtual Folder” on page 66](#). When you create a virtual folder, you can either associate or not associate the virtual folder with a physical location.

- If you associate the virtual folder with a physical location, the virtual folder represents an existing physical folder on a local or remote file system.
- If you do not associate a virtual folder with a physical location, the virtual folder represents a collection of physical folders and files located on one or more local or remote file systems.

**Note:**

You cannot add a virtual folder within a virtual folder that is associated with any physical location.

➤ **To create a virtual folder**

1. On the navigation pane, select **Virtual folders**.
2. On the Virtual folders page, click **+**.
3. In the Add virtual folder dialog box, specify the following details:

Field	Description
<b>Folder Name</b>	Type a unique name for the virtual folder.

---

4. Click **Add**.

The new virtual folder appears in the folders list.

## Configuring Additional Settings for a Virtual Folder

---

You can configure additional settings for a virtual folder.

➤ **To configure additional settings**

1. On the navigation pane, select **Virtual folders**.
2. On the Virtual folders page, click on the virtual folder for which you want to configure additional settings, and specify the required details:

Field	Description
<b>Folder name</b>	Type a different virtual folder name.
<b>Partner</b>	<p>You can perform one of the following:</p> <ul style="list-style-type: none"> <li>■ If you do not want to associate the virtual folder with a partner or your enterprise, select <b>No partner</b>.</li> <li>■ If you want to associate the virtual folder with your enterprise, select <b>Enterprise</b>.</li> </ul> <p>If you want to associate the virtual folder with a partner:</p> <ol style="list-style-type: none"> <li>1. Select <b>Partner</b>.</li> <li>2. Select a partner from the list or type a new partner name.</li> <li>3. Click <b>Create</b>.</li> </ol>
<b>Location</b>	
<b>This folder has a physical location</b>	Select this option if you want to associate the virtual folder with a physical location.
<b>Local file path</b>	To specify a file path in your local file system, select this option, and type the complete file path or browse the file path location. For example, FILE://c:/ProjectFolder/download/ or FILE:///host/SharedFolder/.
<b>Remote path</b>	<p>To specify a file path in a remote server, select this option, a protocol (transport mechanism) from the list, and type the file path location. For example, FTP://host:port/DestinationFolder/.</p> <ul style="list-style-type: none"> <li>■ Type a <b>User name</b> and <b>Password</b> for the remote server.</li> <li>■ If you select FTPES, FTPS, SFTP, or HTTPS protocol, type the certificate alias for the <b>Keystore alias</b>(Optional).</li> <li>■ For the SFTP protocol, select <b>Two-factor authentication</b> if you want ActiveTransfer to authenticate the user with both password and private key when establishing a connection with an SFTP server.</li> </ul> <p>You can configure the preferred cipher from the list of supported cipher in <b>Preferred cipher</b> field. Additionally, if you want to remove a cipher from the supported cipher list, then you set configure it on the <b>Excluded cipher</b> field.</p> <ul style="list-style-type: none"> <li>■ If you select <b>SMB</b> protocol, you can select the SMB version that you want to connect to. Additionally, you need to select SMB 2.0 to use the services of the SMB version 2.0 or later. The SMB protocol supports controlling of SMB dialect variants and</li> </ul>

Field	Description
-------	-------------

encryption of data for SMB3. Dialects are versions of the SMB protocol that are defined based on additions and changes relative to a previous version. SMB client and server negotiate the matched set of capabilities based on the SMB dialect selected.

Fields	Description/Action
--------	--------------------

<b>Dfs enabled</b>	The Distributed File System (DFS) functions provide the ability to logically group shares on multiple servers and to transparently link shares into a single hierarchical namespace.
--------------------	--

<b>Data encryption enabled</b>	Adds the capability to make data transfers secure by encrypting data.
--------------------------------	---

**Note:**

You can add the property `mft.smb.v2.dialect.default` to the `property.cnf` file and assign any of the following dialects. However, the dialect selection on the ActiveTransfer user interface takes priority over this property file, if you have made a selection in the ActiveTransfer user interface.

- SMB\_2\_0\_2
- SMB\_2\_1
- SMB\_3\_0
- SMB\_3\_0\_2
- SMB\_3\_1\_1

- If you want to configure the VFS with **Amazon-S3** storage type, then use the following fields:

Fields	Description/Action
--------	--------------------

<b>Bucket name</b>	Specify the <b>Amazon-S3</b> bucket name.
--------------------	---

<b>Folder path</b>	Specify the folder path for the bucket which you define in the <b>Bucket name</b> .
--------------------	---

**Note:**

If you do not specify the folder path, then the root of the bucket will be considered by default.

<b>Region name</b>	Choose the AWS ( Amazon Web Services ) region from the drop-down list. This is the location where your bucket resides.
--------------------	--

Field	Description
-------	-------------

Fields	Description/Action
<b>Access key ID</b>	Specify the access key id to access the <b>Amazon-S3</b> bucket. .
<b>Secret access key</b>	Specify the secret key which corresponds to the <b>Access Key ID</b> that has the access to <b>Amazon-S3</b> bucket.

- If you want to configure the VFS with **Hosted-S3** storage type, then use the following fields:

Fields	Description/Action
<b>Bucket name</b>	Specify the <b>Hosted-S3</b> bucket name.
<b>Folder path</b>	Specify the folder path for the bucket which you define in the <b>Bucket name</b> . If you do not specify the folder path, then the root of the bucket will be considered by default.
<b>Access key ID</b>	Specify the access key id to access the <b>Hosted-S3</b> bucket. .
<b>Secret access key</b>	Specify the secret key which corresponds to the <b>Access Key ID</b> that has the access to <b>Hosted-S3</b> bucket.
<b>Endpoint</b>	Specify the <b>Endpoint</b> to access the <b>Hosted-S3</b> bucket.
<b>URL Style</b>	Choose one of the following addressing models: <ul style="list-style-type: none"> <li>■ <b>Path.</b> In this URL model, the hostname is <b>s3-hosted.example.com</b> and the bucket name is specified in the path as <b>/bucket-name/</b>. For example, <code>https://s3-hosted.example.com/bucket-name/</code></li> <li>■ <b>Virtual host.</b> This URL model involves including the bucket name as a subdomain of the hostname. For example, <code>https://bucket-name.s3-hosted.example.com/</code></li> </ul>

Field	Description
-------	-------------

**Note:**

New remote protocols will be added to the **Virtual folders** page exclusively. Scheduled and post-processing actions can opt for a virtual folder option that directs to the remote location. This will be applicable from **Hosted-S3** onwards.

- If you want to configure the VFS with *Azure* storage type, then select the **AZURE-FILE** or **AZURE-BLOB** from the drop-down list.

**Note:**

ActiveTransfer currently supports only **AZURE-FILE** shares and **AZURE-BLOB** containers.

- To configure the VFS with **AZURE-FILE**, use the following fields:

Fields	Description/Action
--------	--------------------

**Authentication type** Specifies the authentication information that must be sent to the *Azure* storage type for authorizing the access to specific resources. File shares supports **Shared Key** and **Shared access signature (SAS)** authentication type. Choose one of the following ways to provide the authentication information:

- **Shared Key:** The shared key type passes a header with each request that is signed using the respective storage account access key. Enter the values for the following fields:
  - **Account name:** Specify the account name that corresponds to the *Azure* account for the **AZURE-FILE** location.
  - **Account key:** Specify the key which you create at the *Azure* portal for the corresponding **Account name**.
- **Shared access signature (SAS):** The shared access signature type provides secure delegated access to resources in your storage account without compromising the security of your data.

Field	Description
-------	-------------

Fields	Description/Action
--------	--------------------

Additionally you can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

- **Account name:** Specify the account name that corresponds to the *Azure* account for the **AZURE-FILE** location.
- **SAS token:** The SAS token is a string that you generate in the *Azure* portal for an account.

<b>Location</b>	Specify the location where the folder for the file shares resides.
-----------------	--

- To configure the VFS with **AZURE-BLOB**, use the following fields:

Fields	Description
--------	-------------

**Authentication type** Specifies the authentication information that must be sent to the *Azure* storage for authorizing the access to resources. The **AZURE-BLOB** supports **Shared Key**, **Shared access signature (SAS)**, and **Anonymous public access** authentication types. Choose one of the following ways to provide the authentication information:

- **Shared Key:** The shared key type passes a header with each request that is signed using the respective Storage Account Access Key. Enter the values for the following fields:
  - **Account name:** Specify the account name that corresponds to the *Azure* account for the blob location.
  - **Account key:** Specify the key which you create at the *Azure* portal for the corresponding **Account name**.

Field	Description														
	<table border="1"> <thead> <tr> <th>Fields</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td> <ul style="list-style-type: none"> <li>■ <b>Shared access signature (SAS):</b> The shared access signature type provides secure delegated access to resources in your storage account without compromising the security of your data.  Additionally you can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.</li> <li>■ <b>Account name:</b> Specify the account name that corresponds to the Azure account for the blob location.</li> <li>■ <b>SAS token:</b> The SAS token is a string that you generate in the <i>Azure</i> portal for an account.</li> <li>■ <b>Anonymous public read access:</b> The anonymous public read access type provides you with read access within a publicly accessible container without authorizing the request.</li> </ul> </td> </tr> <tr> <td><b>Storage sub-type</b></td> <td> <p>The below mentioned are the two types of storage sub-type:</p> <ul style="list-style-type: none"> <li>■ <b>Block Blob:</b> It stores the unstructured data such as files, media, images, documents, and so on in blocks.</li> <li>■ <b>Append Blob:</b> It appends the unstructured data such as files, media, images, documents and so on.</li> </ul> </td> </tr> <tr> <td><b>Location</b></td> <td>Specify the Azure container folder path for the <b>Location</b> field.</td> </tr> <tr> <td colspan="2"><b>Upload Options</b></td> </tr> <tr> <td><b>Storage size</b></td> <td>Specifies the size of each part of the file which gets uploaded to the blob container.</td> </tr> <tr> <td><b>Azure headers</b></td> <td>Add the additional header parameters to set the extra metadata for the blob container. Click </td> </tr> </tbody> </table>	Fields	Description		<ul style="list-style-type: none"> <li>■ <b>Shared access signature (SAS):</b> The shared access signature type provides secure delegated access to resources in your storage account without compromising the security of your data.  Additionally you can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.</li> <li>■ <b>Account name:</b> Specify the account name that corresponds to the Azure account for the blob location.</li> <li>■ <b>SAS token:</b> The SAS token is a string that you generate in the <i>Azure</i> portal for an account.</li> <li>■ <b>Anonymous public read access:</b> The anonymous public read access type provides you with read access within a publicly accessible container without authorizing the request.</li> </ul>	<b>Storage sub-type</b>	<p>The below mentioned are the two types of storage sub-type:</p> <ul style="list-style-type: none"> <li>■ <b>Block Blob:</b> It stores the unstructured data such as files, media, images, documents, and so on in blocks.</li> <li>■ <b>Append Blob:</b> It appends the unstructured data such as files, media, images, documents and so on.</li> </ul>	<b>Location</b>	Specify the Azure container folder path for the <b>Location</b> field.	<b>Upload Options</b>		<b>Storage size</b>	Specifies the size of each part of the file which gets uploaded to the blob container.	<b>Azure headers</b>	Add the additional header parameters to set the extra metadata for the blob container. Click 
Fields	Description														
	<ul style="list-style-type: none"> <li>■ <b>Shared access signature (SAS):</b> The shared access signature type provides secure delegated access to resources in your storage account without compromising the security of your data.  Additionally you can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.</li> <li>■ <b>Account name:</b> Specify the account name that corresponds to the Azure account for the blob location.</li> <li>■ <b>SAS token:</b> The SAS token is a string that you generate in the <i>Azure</i> portal for an account.</li> <li>■ <b>Anonymous public read access:</b> The anonymous public read access type provides you with read access within a publicly accessible container without authorizing the request.</li> </ul>														
<b>Storage sub-type</b>	<p>The below mentioned are the two types of storage sub-type:</p> <ul style="list-style-type: none"> <li>■ <b>Block Blob:</b> It stores the unstructured data such as files, media, images, documents, and so on in blocks.</li> <li>■ <b>Append Blob:</b> It appends the unstructured data such as files, media, images, documents and so on.</li> </ul>														
<b>Location</b>	Specify the Azure container folder path for the <b>Location</b> field.														
<b>Upload Options</b>															
<b>Storage size</b>	Specifies the size of each part of the file which gets uploaded to the blob container.														
<b>Azure headers</b>	Add the additional header parameters to set the extra metadata for the blob container. Click 														

Field	Description
<b>Fields</b>	<p><b>Description</b></p> <p>to add the <b>Header key</b> and <b>Header value</b> information respectively. The following are the list if supported headers:</p> <ul style="list-style-type: none"> <li>■ cacheControl</li> <li>■ contentType</li> <li>■ contentEncoding</li> <li>■ contentLanguage</li> <li>■ contentDisposition</li> </ul>

**Note:**

For more information on **AZURE-FILE** shares and **AZURE-BLOB** containers, refer Azure documentation.

**Note:**

For a list of known endpoint specific limitations, see “[Limitations](#)” on page 251.

- Select **Use proxy** if you want to route file transfers to remote servers through a proxy server, and select one of the following options:
  - **Global proxy settings:** If you want ActiveTransfer to use the default proxy server alias set up in Integration Server or ActiveTransfer.
  - **Select proxy alias:** If you want to use a specific proxy server alias for the virtual folder, then select the appropriate proxy server alias to use from the available list.
- Click **Test Connection** to check the connection to the remote location.
- Select **High availability download recovery** if you want ActiveTransfer Server to recover from a download that was not completed.
- Select **Passive** if you want to enable ActiveTransfer Server to connect to a remote server using the passive mode. ActiveTransfer Server uses the active mode by default. This option is applicable for FTP, FTPS, and FTPES protocols.

Field	Description
	<ul style="list-style-type: none"> <li>Select <b>Force CWD to extract directory</b> if the FTP server you are connecting to allows file operations only on the current directory. Enabling this option forces a change to the target directory before executing the file operations.</li> </ul> <p><b>Note:</b> Sending <b>MKDIR</b> or <b>CWD</b> to a directory with no files results in error.</p> <p><b>Note:</b> Sending <b>RMD</b> after deleting all files in a directory results in error.</p>
<b>Permissions</b>	<p>Add a user, role, or group to the virtual folder and configure the following permissions as required: <b>User name</b>, <b>Role name</b>, or <b>Group name</b> for a user, role, and group respectively, <b>View</b>, <b>Download</b>, <b>Upload</b>, <b>Delete</b>, <b>Create folder</b>, <b>Delete folder</b>, <b>Rename</b>, <b>Resume</b>, <b>Share/Publish</b>, or <b>Quota limit (MB)</b>. Support for these permissions is dependent on the specific VFS that you are configuring.</p> <p><b>Note:</b> The <b>Share/Publish</b> permission is disabled for remote path locations by default.</p> <p>For more information about users, roles, or groups to associate with virtual folders, see <a href="#">“Overview” on page 132</a>.</p>
<b>Encryption/Decryption</b>	
<b>File-based encryption</b>	<p>Select the public PGP certificate alias in the <b>Public PGP Key alias</b> box.</p> <p><b>Note:</b> When a file is uploaded, it gets encrypted.</p>
<b>File-based decryption</b>	<p>Select the private PGP certificate alias in the <b>Private PGP Key alias</b> box.</p> <p><b>Note:</b> When the same file is downloaded, it gets decrypted.</p>

- (Optional) Click  to configure pagination for virtual folders, specify the following details, and click **Apply**:
  - No. of folders to display:** Type the no. of folders for display in the Virtual folders page.

- **Count folder depth up to:** Type the folder depth upto which you want to apply the folder count. The folder depth value is 1 for root folder and 2, 3, and so on for subfolder depths.

For example, if **No. of folders to display** is 100 and **Count folder depth up to** is 3, then each page in the folder frame displays 100 folders with a depth of 1, 2, or 3. All sub folders after depth level 4 appear but not be considered for pagination.

4. Click **Save**.

The virtual folder is updated with the additional settings.

## Modifying a Virtual Folder

---

You can edit the configuration settings of an existing virtual folder.

### > To modify a virtual folder

1. On the navigation pane, select **Virtual folders**.
2. On the Virtual folders page, click on a virtual folder that you want to edit.
3. Modify the required configuration settings for the virtual folder.
4. Click **Save**.

The virtual folder is updated with the modified settings.

## Searching for Virtual Folders

---

You can search the virtual folder list to locate a virtual folder based on the folder name, its associated users or partners by specifying the required search criteria.

### > To search for a virtual folder

1. On the navigation pane, select **Virtual folders**.
2. On the Virtual folders page, specify all or one of the following search criteria:

Field	Description
<b>Partner</b>	Select one of the following:

Field	Description
	<ul style="list-style-type: none"><li>■ <b>All partners:</b> To search for virtual folders associated with all the partners in ActiveTransfer.</li><li>■ <b>Specific partner:</b> To search for virtual folders associated with a specific partner in ActiveTransfer. Select this option, type the name of the partner, and click <b>Ok</b>.</li></ul>
<b>User</b>	Select one of the following: <ul style="list-style-type: none"><li>■ <b>All user/role/group:</b> To search for virtual folders associated with all the users, roles or groups in ActiveTransfer.</li><li>■ <b>Specific user/role/group:</b> To search for virtual folders associated with a specific user, role or group in ActiveTransfer. Select this option, type the name of the user, role or group, and click <b>Ok</b>.</li></ul>
<b>Folder name</b>	Type the name of the specific virtual folder you want to view.

3. Click **Reset** and **Apply** for the changes to take effect.

The virtual folders list is populated with the virtual folders matching your search criteria.

# 7 Managing Actions

■ Overview .....	78
■ Adding a Post-Processing Action .....	78
■ Adding a Scheduled Action .....	81
■ Adding a Monitor folder Action .....	84
■ Task Configuration Definitions .....	88
■ Operating Actions .....	125
■ Modifying a Post-Processing, Scheduled, or Monitor folder Action .....	126
■ Searching for a Post-Processing, Scheduled, or Monitor folder Action .....	127
■ Parameterizing Scheduled Action Tasks .....	127

## Overview

You can define actions and trigger them to enable ActiveTransfer Server to perform a configured task or set of tasks. There are three types of ActiveTransfer actions:

### Important:

The references to *Events* and *Actions* in ActiveTransfer 10.2 and earlier versions are now changed to *Actions* and *Tasks* respectively in the new ActiveTransfer user interface.

- *Post-Processing actions* enable ActiveTransfer Server to perform a specific task or set of tasks when a user uploads, downloads, or deletes a file.

Any configuration changes in the post-processing action now get applied to all the active user sessions as well.

This behavior appears for webMethods ActiveTransfer version 10.7 and later.

- *Scheduled actions* enable ActiveTransfer Server to perform a set of tasks at a specified date and time.
- *Monitor Folder actions* enable ActiveTransfer Server to monitor a directory in local or shared file system. It allows you to perform a specific task or set of tasks when a file or folder is created or deleted in the monitoring directory.

## Adding a Post-Processing Action

You can define a post-processing action for execution when a user uploads, downloads, or deletes a file.

### ➤ To add a post-processing action

1. On the navigation pane, select **Actions> Post-Processing**.
2. On the Post-Processing actions page, you can do one of the following:
  - If you want to create a new action, click .
  - If you want to create a copy of an action that already exists, select an existing action, and click .
3. To define the conditions that trigger the action, specify the following details:

Field	Description
<b>Action name</b>	Type a unique name for the post-processing action.
<b>Description</b>	Type a brief description for the post-processing action.

Field	Description
<b>Active</b>	Click the toggle button to activate (  ) or deactivate (  ) the action.
<b>Criteria</b>	Click  . In the Criteria dialog box, configure the criteria for ActiveTransfer Server to execute the tasks, and click <b>OK</b> .
<b>Execute the tasks below when user performs the file operation :</b>	Select the file operation from the list. <b>Note:</b> If you specify an action based on the deletion of a file, make sure that any subsequent tasks you define for the action do not rely on the presence of the deleted file.
<b>Virtual folder</b>	To specify any folder or a particular folder, select <b>Any folder</b> or <b>Specific folder</b> respectively.  For <b>Specific folder</b> , type a specific folder name in the box. You can use wildcard characters in the folder name box (for example, *baseName). By default, ActiveTransfer Server considers file activity in any folder structure when evaluating action criteria.
<b>File transfer status</b>	To specify a file transfer status, select <b>Success or Failure</b> , <b>Success</b> , or <b>Failure</b> .
<b>Task execution by</b>	To enable ActiveTransfer Server to execute the action for file operations performed by particular users, groups, or roles, select <b>Any user, role, group</b> or <b>Specific users, roles, groups</b> and click  , select the users, groups, or roles, and click <b>OK</b> .
<b>Execute tasks</b>	To specify whether to execute the tasks immediately, after the user exits all sessions, or after the user is idle for few seconds, select <b>Immediately</b> , <b>After the user exists all sessions</b> , or <b>After the user is idle for</b> and type the number of seconds to wait before executing the action in the box.
<b>Tasks</b>	Select one or more of the following tasks, and define configurations for each of the tasks in the <b>Properties</b> section accordingly: <ul style="list-style-type: none"> <li>■ File operations <ul style="list-style-type: none"> <li>■ <a href="#">“Find Task Configuration” on page 89</a></li> <li>■ <a href="#">“Copy Task Configuration” on page 93</a></li> <li>■ <a href="#">“Move Task Configuration” on page 97</a></li> <li>■ <a href="#">“Delete Task Configuration” on page 102</a></li> </ul> </li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ “Rename Task Configuration” on page 103</li> <li>■ “Encrypt Task Configuration” on page 104</li> <li>■ “Decrypt Task Configuration” on page 105</li> <li>■ “Zip Task Configuration” on page 107</li> <li>■ “Unzip Task Configuration” on page 109</li> <li>■ “Write Content Task Configuration” on page 111</li> <li>■ “Execute Integration Server Service Task Configuration” on page 113</li> <li>■ “Execute Script Task Configuration” on page 114</li> <li>■ “Execute Trading Networks Service Task Configuration” on page 116</li> <li>■ “Send Universal Messaging/Broker Notification Task Configuration” on page 118</li> <li>■ “Send Email Task Configuration” on page 120</li> <li>■ “Write File to Database Task Configuration” on page 121</li> <li>■ “Jump Task Configuration” on page 123</li> <li>■ “Exclude Task Configuration” on page 124</li> <li>■ “Error Task Configuration” on page 125</li> </ul>
	<p>For descriptions of fields for task configurations, see “Task Configuration Definitions” on page 88.</p>
	<p><b>Tip:</b></p> <p>Click  to disable a task. Click  to enable a task. Click  to delete the task. Click  to copy the task. By default, a task is enabled when created.</p>
<b>Parallel processing</b>	
<b>Enable parallel processing</b>	Select this option if you want to enable parallel processing of files in multiple threads.
<b>Start parallel processing for files after</b>	Select the task after which ActiveTransfer must start parallel processing of files in multiple threads from the list. ActiveTransfer first executes the task you select here, and any other tasks before it, sequentially.

Field	Description
<b>Maximum number of parallel processes</b>	Type the maximum number (between one and 999) of parallel threads that ActiveTransfer can create to simultaneously process files.

4. Click **Add**.

The new post-processing action appears in the post-processing actions list.

## Adding a Scheduled Action

You can define a scheduled action for execution at a specific date and time.

### > To add a scheduled action

1. In the navigation pane, select **Actions > Scheduled**.
2. On the Scheduled actions page, you can do one of the following:
  - If you want to create a new action, click .
  - If you want to create a copy of an action that already exists, select an existing action, and click .
  - If you want to test the scheduled action, select an existing action, and click .
3. To define the conditions that trigger the action, specify the following details:

Field	Description
<b>Action name</b>	Type a unique name for the scheduled action.
<b>Description</b>	Type a brief description for the scheduled action.
<b>Active</b>	Click the toggle button to activate (  ) or deactivate (  ) the action.
<b>Schedule settings</b>	Click  . In the Configure criteria dialog box, select one of the following options from the list to specify how often ActiveTransfer Server should execute the tasks associated with an action, and click <b>Ok</b> :

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Run once:</b> Specify the <b>Date</b> and <b>Time</b> to execute the task. Click the calendar icon to select a date from the calendar.</li> <li>■ <b>Yearly:</b> Specify a date range, the months, the days within the month, and the time interval you want to execute the task each year.</li> <li>■ <b>Monthly:</b> Specify a date range, the days within the month, and the time interval you want to execute the task each month.</li> <li>■ <b>Weekly:</b> Specify a date range, the days of the week, and the time interval you want to execute the task each week.</li> <li>■ <b>Daily:</b> Specify a date range and the time interval you want to execute the task each day.</li> <li>■ <b>Hourly:</b> Specify a date range and the time interval you want to execute the task each hour.</li> <li>■ <b>Fixed interval:</b> Specify a date range and the time interval that ActiveTransfer Server should wait before executing the next task for a scheduled action.</li> <li>■ <b>Manual:</b> Use the <code>wm.mft.schedule:executeEvent</code> service to execute the tasks defined for this action.</li> </ul>

---

## Tasks

Select one or more of the following tasks and define configurations for each of the tasks in the **Properties** section accordingly:

- File operations
  - [“Find Task Configuration” on page 89](#)
  - [“ Copy Task Configuration” on page 93](#)
  - [“Move Task Configuration” on page 97](#)
  - [“Delete Task Configuration” on page 102](#)
  - [“Rename Task Configuration” on page 103](#)
  - [“Encrypt Task Configuration” on page 104](#)
  - [“Decrypt Task Configuration” on page 105](#)
  - [“Zip Task Configuration” on page 107](#)
  - [“Unzip Task Configuration” on page 109](#)
  - [“Write Content Task Configuration” on page 111](#)

Field	Description
	<ul style="list-style-type: none"> <li>■ “Execute Integration Server Service Task Configuration” on page 113</li> <li>■ “Execute Script Task Configuration” on page 114</li> <li>■ “Execute Trading Networks Service Task Configuration” on page 116</li> <li>■ “Send Universal Messaging/Broker Notification Task Configuration” on page 118</li> <li>■ “Send Email Task Configuration” on page 120</li> <li>■ “Write File to Database Task Configuration” on page 121</li> <li>■ “Jump Task Configuration” on page 123</li> <li>■ “Exclude Task Configuration” on page 124</li> <li>■ “Error Task Configuration” on page 125</li> </ul> <p>For descriptions of fields for task configurations, see “Task Configuration Definitions” on page 88.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Tip:</b>  Click  to disable a task. Click  to enable a task. Click  to delete the task. Click  to copy the task. By default, a task is enabled when created.</p> </div>
<b>Parallel processing</b>	
<b>Enable parallel processing</b>	Select this option if you want to enable parallel processing of files in multiple threads.
<b>Start parallel processing for files after</b>	Select the task after which ActiveTransfer must start parallel processing of files in multiple threads from the list. ActiveTransfer first executes the task you select here, and any other tasks before it, sequentially.
<b>Maximum number of parallel processes</b>	Type the maximum number (between one and 999) of parallel threads that ActiveTransfer can create to simultaneously process files.

4. Click **Add**.

The new scheduled action appears in the scheduled actions list.

5. (Optional) Click **Test action** to test the scheduled action.

**Note:**

You can test only deactivated scheduled actions.

- a. In the Test scheduled action dialog box, type the values for the parameters defined in tasks.
- b. Click **Test action**.

**Note:**

If a value for a parameterized numeric field is not provided, then the default value for that specific field is considered for the task execution during runtime.

The test result and a link to view the logs appears. You can do the following:

- Click **Click here** to view the details of the test execution on the Action log page in a new tab.
- On the Action log page, click  to reload the page to view the latest status of test execution.

## Adding a Monitor folder Action

You can define a monitor folder action to monitor a directory in the local file system or shared file system. You can further trigger the action based on the file operation you select.

### ➤ To add a monitor folder action

1. In the navigation pane, select **Actions > Monitor folder**.
2. On the Monitor folder actions page, you can do one of the following:
  - If you want to create a new action, click .
  - If you want to create a copy of an action that already exists, select an existing action, and click .
3. To define the conditions that trigger the action, specify the following details:

Field	Description
<b>Action name</b>	Type a unique name for the monitor folder action.
<b>Description</b>	Type a brief description for the monitor folder action.
<b>Active</b>	Click the toggle button to activate (  ) or deactivate (  ) the action.

Field	Description
-------	-------------

## Criteria

Click . In the **Criteria** dialog box, fill the following fields and click **Ok**:

- **Monitor folder:** Type the folder name or browse to the folder to monitor. When ActiveTransfer Server starts monitoring a folder, a lock file with format `_{event_id}.mftlock` gets automatically created. This is to ensure that only a single instance of the monitor folder action can monitor the particular folder.

After the lock file is created successfully, ActiveTransfer Server starts monitoring the folder. However, if the lock gets deleted by an external entity, then ActiveTransfer Server stops monitoring the folder.

- **Select the file operation:** Select the file operation that triggers the action:

- **Create file:** If you choose this option, ActiveTransfer Server triggers the monitor folder action on creating a file in the monitored folder.

In case of successful execution of the action, ActiveTransfer Server moves the newly created file to the **Completion folder**. If the execution fails, the newly created file is moved to the **Error folder**.

ActiveTransfer Server performs a stability check on a newly created file for 30 seconds. It triggers an action if there is no update on the file for last 30 seconds or the file is not in use by another process.

- **Delete file:** If you choose this option, ActiveTransfer Server triggers the monitor folder action on deleting a file in the monitored folder.

### Note:

- If you specify an action based on the deletion of a file, make sure that any subsequent tasks you define for the action does not rely on the presence of the deleted file.
- TMP files created or deleted by the operating system in the monitored folder do not trigger monitor folder action.

- **File filter:** Type the name of the file if you want to filter the files with specific names. By default, ActiveTransfer Server considers all the files. If you want to use regular expression, specify a valid regular expression in **File filter** and select the **Use regular expression** option.

### Note:

You can use wildcard characters to filter the file names. For example, type `*.zip` to trigger the action only when the ZIP files are created or deleted. To trigger an action based on a name string in the ZIP files, prefix and suffix the name string in the **File filter** box with wildcard characters. For example, type `*invoice*.zip` to trigger the action based

Field	Description
	<p>on the file names, when ZIP files containing the character string <code>invoice</code> in their file names are created or deleted.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*</code>: Excludes files with the file name containing <code>purchaseorder</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul> <ul style="list-style-type: none"> <li>■ <b>Completion folder</b>: Type the folder name or browse to the folder to move the file after the successful execution of an action.</li> <li>■ <b>Error folder</b>: Type the folder name or browse to the folder to move the file after an execution fails for the action.</li> <li>■ <b>Watch frequency (sec)</b>: Specify the time interval in seconds to monitor the folder.</li> <li>■ <b>Retention period (days)</b>: Specify the number of days you want to retain the files in <b>Completion folder</b> or <b>Error folder</b>.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ If you want to retain the files permanently in <b>Completion folder</b> or <b>Error folder</b>, set the value for this field to <code>0</code>.</li> <li>■ If the specified value for the retention period is greater than <code>0</code>, and if the monitor folder action for those files is active, then the files get deleted from the completion folder or error folder after the specified number of days.</li> <li>■ When ActiveTransfer Server starts monitoring the folder, it tries to process the existing files in the monitored folder. If the completion folder or error folder is missing, then ActiveTransfer Server does not process the existing files.</li> </ul>

**Tasks** Select one or more of the following tasks and define configurations for each of the tasks in the **Properties** section as required:

- File operations
  - [“Find Task Configuration” on page 89](#)
  - [“Copy Task Configuration” on page 93](#)
  - [“Move Task Configuration” on page 97](#)
  - [“Delete Task Configuration” on page 102](#)

Field	Description
	<ul style="list-style-type: none"> <li>■ <a href="#">“Rename Task Configuration” on page 103</a></li> <li>■ <a href="#">“Encrypt Task Configuration” on page 104</a></li> <li>■ <a href="#">“Decrypt Task Configuration” on page 105</a></li> <li>■ <a href="#">“Zip Task Configuration” on page 107</a></li> <li>■ <a href="#">“Unzip Task Configuration” on page 109</a></li> <li>■ <a href="#">“Write Content Task Configuration” on page 111</a></li> <li>■ <a href="#">“Execute Integration Server Service Task Configuration” on page 113</a></li> <li>■ <a href="#">“Execute Script Task Configuration” on page 114</a></li> <li>■ <a href="#">“Execute Trading Networks Service Task Configuration” on page 116</a></li> <li>■ <a href="#">“Send Universal Messaging/Broker Notification Task Configuration” on page 118</a></li> <li>■ <a href="#">“Send Email Task Configuration” on page 120</a></li> <li>■ <a href="#">“Write File to Database Task Configuration” on page 121</a></li> <li>■ <a href="#">“Jump Task Configuration” on page 123</a></li> <li>■ <a href="#">“Exclude Task Configuration” on page 124</a></li> <li>■ <a href="#">“Error Task Configuration” on page 125</a></li> </ul>
	<p>For descriptions of the fields for these task configurations, see <a href="#">“Task Configuration Definitions” on page 88</a>.</p>
	<p><b>Tip:</b>  Click  to disable a task. Click  to enable a task. Click  to delete the task. Click  to copy the task. By default, a task is enabled when created.</p>
<b>Import</b>	Click  to import a task from an existing post-processing action. You can import all the tasks from a particular post-processing action. However, ActiveTransfer Server enables you to import tasks only when the monitor folder action does not have any task defined for it. For information on post-processing action, refer <a href="#">“Adding a Post-Processing Action” on page 78</a> .

4. Click **Add**.

The new monitor folder action appears in the monitor folder actions list.

**Note:**

If the auto-generated lock file from the monitor folder gets deleted, ActiveTransfer Server will not execute the action even if it is active. In such case, to restart the same action, you need to update the action.

**Note:**

We recommend that you use **File name filters** to avoid execution of monitor folder action for unexpected files.

**Important:**

While configuring the action, please note the behavior of each task mentioned below:

- **Rename** : If the existing file and the file to be renamed point to the same monitored folder, then the rename task can lead to an unexpected result.
- **Zip**: If the destination location point to the monitored folder, then the zip task can lead to an unexpected result.
- **Unzip**: If the destination location point to the monitored folder, then the unzip task can lead to an unexpected result.
- **Encrypt**: You must be careful while configuring the encrypt task for monitor folder action, as it can lead to creating temporary files while encrypting the files. These temporary files may trigger the action again. However, you can execute an encrypt task on the files that are created after performing the copy or move actions and not the original file.
- **Decrypt**: You must be careful while configuring the decrypt task for monitor folder action, as it can lead to creating temporary files while decrypting the files. These temporary files may trigger the action again. However, you can execute a decrypt task on the files that are created after performing the copy or move actions and not the original file.

**Note:**

If a folder is already being monitored, then you cannot monitor the same folder with any other monitor folder action that is active. However, if you want to execute any other monitor folder action on the same folder which is monitored, then you must deactivate the current action and reactivate the new action to take effect.

## Task Configuration Definitions

---

After you add an action and define the conditions that trigger the action, you must define one or more tasks to execute when the action is triggered. After you define tasks for a post-processing, scheduled, or monitor folder action, activate the action as described in [“Operating Actions” on page 125](#).

A post-processing action is triggered for each file based on the criteria configured in the action. The action is triggered by a file upload, file download, or a file delete. The action is executed for one file at a time. If an error occurs in the action, the file processing is stopped after processing the files in the current task.

For scheduled action, the “find” task is the first task that you define, by default. Otherwise, the scheduled action will fail. The files listed by the find task is the source of input files for the action. If the find task returns more than one file, the subsequent tasks will operate on all the files. Each

task configured in the action will complete the operation on all the files in the list and pass on the set of files to the subsequent task.

A monitor folder action is triggered for each file based on the criteria configured in the action. The action is triggered by a file create or a file delete in a local or shared file system. The action is executed for one file at a time. If an error occurs in the action, the file processing is stopped after processing the files in the current task.

One type of task that ActiveTransfer Server can execute when an action is triggered is a file operation. File operations include finding, copying, moving, renaming, deleting, encrypting and decrypting, zipping or unzipping files, or writing content to a file. For each file operation, you should define specific properties that apply to that operation.

If an error task is configured in the action, one error task is executed for each file transaction that has an error. If the find task returns an empty list, subsequent tasks will be executed with 0 files as input.

**Note:**

For outbound file transfers triggered through scheduled actions or by invoking the `wm.mft.schedule.executeEvent` service, consider transferring the files by way of a virtual folder instead of directly connecting to an external server using a find, copy, or move file operation. Files transferred by way of virtual folders are automatically logged on the Transaction log page.

## Find Task Configuration

You can configure the following properties for the Find file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>Source location</b>	<p>Select one of the following options to configure the location where the file will be searched for:</p> <ul style="list-style-type: none"> <li>■ <b>Local file path</b>, if the destination location is on your local machine, type or browse to the location. To specify a file URL for a shared location, use the <code>FILE:///host/SharedFolder/</code> syntax. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.</li> <li>■ <b>Remote path</b>, if the destination location is on a remote server or network, select a protocol (transport mechanism) from the list, and type or browse to the file path location. For example, <code>protocol://&lt;host&gt;:&lt;port&gt;/DestinationFolder/</code>.</li> </ul>

**Note:**

If you want to find and copy files from remote, third-party HTTP(S) servers, ensure that you provide appropriate

Field	Description
	<p>certificate alias here. Deselect <b>ActiveTransfer HTTP(S) Server</b> box for third-party HTTP(S) servers and specify the <b>File Name Identification</b> to locate the file name either from the URL or a specific file name.</p> <ul style="list-style-type: none"> <li>■ Type the <b>User name</b> and <b>Password</b> for the remote server.</li> <li>■ Select <b>Use proxy</b> if you want to route file transfers to remote servers through a proxy server, and select one of the following options: <ul style="list-style-type: none"> <li>■ <b>Global proxy settings</b>, if you want ActiveTransfer to use the default proxy server alias set up in Integration Server or ActiveTransfer.</li> <li>■ <b>Select proxy alias</b>, if you want to use a specific proxy server alias for the folder. Then, select the appropriate proxy server alias to use from the available list.</li> </ul> </li> <li>■ Click <b>Test Connection</b> to check the connection to the remote server with or without a proxy server.</li> </ul> <p><b>Tip:</b> If you want to connect to a remote server using a secure protocol (FTPES, FTPS, HTTPS or SFTP) and want to configure authentication using secure key exchange, create a folder for the remote server and configure the certificate alias parameters. You can then use the folder that you configured in the <b>Virtual folder</b> option of the <b>Source location</b> in the task.</p> <ul style="list-style-type: none"> <li>■ <b>Virtual folder:</b> To specify a virtual folder, type or browse to the location of the folder. If you want to point to a subfolder within the folder, append the URL in the box with the details of the subfolder.</li> </ul> <p><b>Note:</b> The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the action is configured.</p>
<b>Any file name</b>	Select this option if you want find files with any name.
<b>Specific file name</b>	Select this option if you want to filter files with specific names (for example, *.xml) and type the file name in the text box. This option is disabled if you select <b>Any file name</b> .
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

Field	Description
<b>Advanced</b>	
<b>Exclude folders</b>	Select this option if you want ActiveTransfer to ignore folders and their contents in the find task.
<b>Folder depth</b>	Specify the folder depth if you want to include subfolders in the search criteria for the find task. The default value is 1 which restricts the search to the root folder.
<b>Maximum items to find</b>	Specify the number of records to restrict in the find task results. The default is 0 which includes all the records that match the search criteria for the find task.
<b>Last file modification</b>	<p>Specify one of the following time period in which the file was last modified to narrow the search:</p> <ul style="list-style-type: none"> <li>■ <b>before</b>, if you want to specify the time before which files were modified.</li> <li>■ <b>within</b>, if you want to specify the time (including the current date) within which files were modified.</li> </ul> <p><b>Note:</b> You must specify at least one time criteria if you select a time variable.</p> <p>In the <b>Days, Hours, Minutes</b> boxes respectively, type the days, hours, and minutes at which to apply the selected time variable.</p> <p>For example, let us assume that you have specified the time variable as <b>Before</b>, with 2 days and 6 hours as the time variable. When ActiveTransfer executes the find task on 30 April, it searches for all files that were modified before 4 p.m. on 27 April. If you change the time variable to <b>Within</b>, when ActiveTransfer executes the find task at 12 pm on 30 April, it searches for files that were modified between 28 April and 30 April 4 a.m.</p>
<b>Fail if no files are found</b>	Select this option if you want the find operation to fail if no files are found.
<b>File stability and scanning</b>	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Exclude files that are being updated</b>, if you want to ignore files for which processing is in-progress.</li> </ul>
<b>Scan file for update</b>	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Exclude file after first scan</b>, if you want the find operation to scan and check only once.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Scan file multiple times</b>, if you want the file operation to check at regular intervals. Type the seconds and minutes.</li> </ul>
<b>Retry</b>	Select this option to retry a failed find task. Type the number of <b>Retry attempts</b> and the <b>Retry interval</b> in seconds.
<b>Assign partner</b>	<p>Select this option if you want to assign a partner for the action and do one of the following:</p> <ul style="list-style-type: none"> <li>■ Select the partner to assign from the list of configured partners in ActiveTransfer.</li> <li>■ Type a parameterized value for the partner in the following format: [partner_name], where [partner_name] is a server variable or an action parameter that contains the actual partner name during the execution of an action.</li> </ul> <p><b>Note:</b> For virtual folders, use this option only if you want to override the partners configured for the folders.</p>
<b>Sort files</b>	<p>Select this option to enable ActiveTransfer to search for files in a particular order. You can sort files based on last modified date, file size, and file name under <b>Sort field</b>, and ascending or descending order under <b>Sort order</b>.</p> <p><b>Note:</b> If you configure <b>Maximum items to find</b> with a specific value (for example, 4) and select this option, then ActiveTransfer reads every file within the folder and finds files based on the <b>Sort files</b> criteria. This might result in a decrease in the performance of the Find task.</p>

A find task retrieves a list of files from a specified location. The files listed by a find task are passed on to the subsequent task for processing. If there are multiple find tasks for an action, the files found by each “find” task are added to the list passed on to it from the previous task.

For example, consider the following sequence of tasks and the ActiveTransfer behavior for each task:

Sequence Number	What does ActiveTransfer do?
1	Finds files in the given source location <i>A</i> . Let us call these files list 1.
2	Executes the Integration Service on file list 1.
3	Finds files in the given source location <i>B</i> . Let us call these files list 2.
4	Executes the Integration Server service on both list 1 and list 2 files.

Sequence Number	What does ActiveTransfer do?
5	Encrypts the files in list 1 and list 2.

## Copy Task Configuration

You can configure the following properties for the Copy file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$:</code> Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*)123\$:</code> Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*)):</code> Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Destination location</b>	<p>Select one of the following options to configure the location where the file will be copied to:</p> <ul style="list-style-type: none"> <li>■ <b>Local file path</b>, if the destination location is on your local machine, type or browse to the location. To specify a file URL for a shared location, use the <code>FILE:///host/SharedFolder/</code> syntax. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li data-bbox="500 260 1385 401">■ <b>Remote path</b>, if the destination location is on a remote server, select a protocol (transport mechanism) from the list, and type or browse to the file path location. For example, <code>protocol://&lt;host&gt;:&lt;port&gt;/DestinationFolder/</code>.</li> </ul> <div data-bbox="548 422 1365 583" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> If you want to find and copy files from remote, third-party HTTP(S) servers, ensure that the you provide appropriate certificate alias here.</p> </div> <ul style="list-style-type: none"> <li data-bbox="500 600 1385 636">■ Type the <b>User name</b> and <b>Password</b> for the remote system.</li> <li data-bbox="500 657 1385 888">■ Select <b>Use proxy</b> if you want to route file transfers to remote servers through a proxy server, and select one of the following options: <ul style="list-style-type: none"> <li data-bbox="597 789 1385 888">■ <b>Global proxy settings</b>, if you want ActiveTransfer to use the default proxy server alias set up in Integration Server or ActiveTransfer.</li> <li data-bbox="597 915 1385 1014">■ <b>Select proxy alias</b>, if you want to use a specific proxy server alias for the folder, then select the appropriate proxy server alias to use from the available list.</li> </ul> </li> <li data-bbox="500 1041 1385 1119">■ Select if you want ActiveTransfer Server to recover from a download that was not completed.</li> <li data-bbox="500 1140 1385 1203">■ Click <b>Test Connection</b> to check the connection to the remote server with or without a proxy server.</li> </ul> <div data-bbox="548 1224 1365 1503" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Tip:</b> If you want to connect to a remote server using a secure protocol (FTPES, FTPS, HTTPS or SFTP) and want to configure authentication using secure key exchange, create a folder for the remote server and configure the certificate alias parameters. You can then use the folder that you configured in the <b>Virtual folder</b> option of the <b>Destination location</b> in the task.</p> </div> <ul style="list-style-type: none"> <li data-bbox="500 1518 1385 1623">■ <b>Virtual folder:</b> To specify a folder, type or browse to the location of the folder. If you want to point to a subfolder within the folder, append the URL in the box with the details of the subfolder.</li> </ul> <div data-bbox="548 1644 1365 1797" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> The folder that you select should be configured on the same ActiveTransfer Server instance on which the action is configured.</p> </div>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

Field	Description
<b>Advanced</b>	
<b>Rename file to</b>	Select this option to rename the file to the specified name in the box.
<b>Check if the file exists at destination</b>	<p>Select this option to check if the file already exists at the destination and perform one of the following options:</p> <ul style="list-style-type: none"> <li> <b>Skip the transfer if file exists:</b> This option skips the file transfer if the file with the same file name exists at the destination. However, further actions will not be performed on that particular file at the destination. <p><b>Example:</b> Consider you want to perform Copy and Rename tasks respectively on a file. The Copy task skips that particular file if the file already exists at the destination. Additionally, the Rename task also will not be performed on that particular file.</p> </li> <li> <b>Fail the action if file exists:</b> This option fails the action if a file with the same filename exists at the destination location. In this case, the execution of the action stops and is a marked failure. <p>During parallel execution, only the particular file which is already at the destination will not be processed. However, the remaining files will complete their processing and is transferred to the destination.</p> <p><b>Example:</b></p> <ul style="list-style-type: none"> <li> <b>For parallel execution:</b> <p>Let us consider that you want to perform Copy and Rename tasks on multiple files. Also, one of the files is already at the destination. So, the Copy and Rename tasks fail only for that particular file which is at the destination. However, ActiveTransfer will continue processing the remaining files for Copy and Rename tasks respectively.</p> </li> <li> <b>For non-parallel execution:</b> <p>Let us consider that you want to perform Copy and Rename tasks on multiple files. Also, one of the files is already at the destination. So, the Copy and Rename tasks fail only for that particular file which is at the destination. However, ActiveTransfer will copy the remaining files but will not process the Rename task for these files. Additionally, any subsequent task for these files will not be performed.</p> </li> </ul> </li> </ul>
<b>Note:</b>	

Field	Description
	If you rename a particular file using <b>Rename file to</b> option, then <b>Fail the action if file exists</b> option checks for the renamed filename at the destination. The renamed file will be added to the destination only if it does not match the rest of the filename.
<b>Use temporary file name</b>	Select this option and type a temporary name for the file to use while copying the file. The file is renamed to its original name after the copy file operation is complete.
<b>Preserve file modification date</b>	Select this option to retain the time stamp indicating when the file was last modified.
<b>Check for stability</b>	If you want the file operation to check its progress at regular intervals, specify the time in seconds in the following format: <b>Every [ ] seconds up to [ ] seconds</b> , where, [ ] is the text box to type the value in seconds.
<b>Retry</b>	Select this option to retry a failed copy task. Type the number of <b>Retry attempts</b> and the <b>Retry interval</b> in seconds.
<b>Resume transfer from the point of interruption</b>	Select this option to resume an interrupted or failed copy operation from the point of interruption.
<b>Command before upload</b>	If you want to execute a SITE command before copy task, then choose this option. For example, while working with Mainframe servers, value for record size and block size can be sent to the server before upload by setting the following value to this new configuration field: <code>SITE LRECL=&lt;record_size&gt; BLKSIZE=&lt;block_size&gt;</code> .
<b>Simple mode</b>	Select this option to change the file transfer mode to simple mode and if you are transferring files to AS/400 systems. This mode is applicable to FTP, FTPS, or FTPES protocols.
<b>ASCII mode</b>	<p>Select this option to change the file transfer mode to ASCII mode and select one of the following <b>Convert line endings</b> options for ActiveTransfer Server to change the line endings of the file: <b>CRLF - Windows, CR - MAC OS Classic, LF - Unix</b>, or <b>No change</b>.</p> <p>This mode is applicable for FTP, FTPS, or FTPES protocols.</p> <p>By default, ActiveTransfer Server uses the Binary file transfer mode for the copy operation.</p>
<b>Assign partner</b>	<p>Select this option if you want to assign a partner for the action and do one of the following:</p> <ul style="list-style-type: none"> <li>■ Select the partner to assign from the list of configured partners in ActiveTransfer.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>Type a parameterized value for the partner in the following format: [partner_name], where [partner_name] is a server variable or an action parameter that contains the actual partner name during the execution of an action.</li> </ul>
	<p><b>Note:</b> For virtual folders, use this option only if you want to override the partners configured for the folders.</p>

A copy task copies all the files passed on from the previous task to the location specified in **Destination location**. However, the files copied to the specified destination will not be available to the subsequent task for processing. The list of files in the source location is passed on to the subsequent task.

## Move Task Configuration

You can configure the following properties for the Move file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type *.zip to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type *invoice*.zip to trigger the action based on the file URLs, when ZIP files containing the character string invoice in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>^(?!.*purchaseorder).*\$: Excludes files with the file URL containing purchaseorder.</li> <li>*/out/.*: Include files with the file URL containing the folder out.</li> <li>^abc(.*)123\$: Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ NEW-((*.doc)   (*_backup_*)): Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_.</li> </ul>
<b>Destination location</b>	<p>Select one of the following options to configure the location where the file will be copied to:</p> <ul style="list-style-type: none"> <li>■ <b>Local file path</b>, if the destination location is on your local machine, type or browse to the location. To specify a file URL for a shared location, use the <code>FILE:///host/SharedFolder/</code> syntax. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.</li> <li>■ <b>Remote path</b>, if the destination location is on a remote server, select a protocol (transport mechanism) from the list, and type or browse to the file path location. For example, <code>protocol://&lt;host&gt;:&lt;port&gt;/DestinationFolder/</code>.</li> </ul> <div data-bbox="548 800 1365 972" style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> If you want to find and move files from remote, third-party HTTP(S) servers, ensure that the you provide appropriate file path here.</p> </div> <ul style="list-style-type: none"> <li>■ Type the <b>User name</b> and <b>Password</b> for the remote system.</li> <li>■ Select <b>Use proxy</b> if you want to route file transfers to remote servers through a proxy server, and select one of the following options: <ul style="list-style-type: none"> <li>■ <b>Global proxy settings</b>, if you want ActiveTransfer to use the default proxy server alias set up in Integration Server or ActiveTransfer.</li> <li>■ <b>Select proxy alias</b>, if you want to use a specific proxy server alias for the folder, then select the appropriate proxy server alias to use from the available list.</li> </ul> </li> <li>■ Select if you want ActiveTransfer Server to recover from a download that was not completed.</li> <li>■ Click <b>Test Connection</b> to check the connection to the remote server with or without a proxy server.</li> </ul> <div data-bbox="548 1608 1365 1881" style="background-color: #f0f0f0; padding: 5px;"> <p><b>Tip:</b> If you want to connect to a remote server using a secure protocol (FTPES, FTPS, HTTPS or SFTP) and want to configure authentication using secure key exchange, create a folder for the remote server and configure the certificate alias parameters. You can then use the folder that you configured in the <b>Virtual folder</b> option of the <b>Source location</b> in the task.</p> </div>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Virtual folder:</b> To specify a virtual folder, type or browse to the location of the folder. If you want to point to a subfolder within the folder, append the URL in the box with the details of the subfolder.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the action is configured.</p> </div>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .
<b>Advanced</b>	
<b>Create directory</b>	Select this option to enable ActiveTransfer to create the destination folder if the folder specified in <b>Destination location</b> is not present. If <b>Destination location</b> path does not include a folder, ActiveTransfer copies the file directly to the specified directory path.
<b>Rename file to</b>	Select this option to rename the file to the specified name in the box.
<b>Check if the file exists at destination</b>	Select this option to check if the file already exists at the destination location and perform one of the following options: <ul style="list-style-type: none"> <li>■ <b>Skip the transfer if file exists:</b> This option skips the file transfer if the file with the same file name exists at the destination. However, further actions will not be performed on that particular file at the destination.</li> </ul> <p><b>Example:</b> Consider you want to perform Move and Rename tasks respectively on a file. The Move task skips that particular file if the file already exists at the destination. Additionally, the Rename task also will not be performed on that particular file.</p> <ul style="list-style-type: none"> <li>■ <b>Fail the action if file exists:</b> This option fails the action if a file with the same filename exists at the destination location. In this case, the execution of the action stops and is a marked failure.</li> </ul> <p>During parallel execution, only the particular file which is already at the destination will not be processed. However, the remaining files will complete their processing and is transferred to the destination.</p> <p><b>Example:</b></p> <ul style="list-style-type: none"> <li>■ For parallel execution: <p style="margin-left: 20px;">Let us consider that you want to perform Move and Rename tasks on multiple files. Also, one of the files is already at the</p> </li> </ul>

Field	Description
	<p>destination. So, the Move and Rename tasks fail only for that particular file which is at the destination. However, ActiveTransfer will continue processing the remaining files for Move and Rename tasks respectively.</p> <ul style="list-style-type: none"> <li>■ For non-parallel execution:</li> </ul> <p>Let us consider that you want to perform Move and Rename tasks on multiple files. Also, one of the files is already at the destination. So, the Move and Rename tasks fail only for that particular file which is at the destination. However, ActiveTransfer will move the remaining files but will not process the Rename task for these files. Additionally, any subsequent task for these files will not be performed.</p> <p><b>Note:</b></p> <p>If you rename a particular file using <b>Rename file to</b> option, then <b>Fail the action if file exists</b> option checks for the renamed filename at the destination. The renamed file will be added to the destination only if it does not match the rest of the filename.</p>
<b>Use temporary file name</b>	<p>Select this option and type a temporary name for the file to use while moving the file. The file is renamed to its original name after the move file operation is complete.</p> <p><b>Note:</b></p> <p>Temporary file name will not be used for a file being moved within an operating system or server.</p>
<b>Preserve file modification date</b>	<p>Select this option to retain the time stamp indicating when the file was last modified.</p>
<b>Check for stability</b>	<p>If you want the file operation to check its progress at regular intervals, specify the time in seconds in the following format: <b>Every [ ] seconds up to [ ] seconds</b>, where, [ ] is the text box to type the value in seconds.</p>
<b>Retry</b>	<p>Select this option to retry a failed move task. Type the number of <b>Retry attempts</b> and the <b>Retry interval</b> in seconds.</p>
<b>Resume transfer from the point of interruption</b>	<p>Select this option to resume an interrupted or failed move operation from the point of interruption.</p>
<b>Command before upload</b>	<p>If you want to execute a SITE command before move task, then choose this option. For example, while working with Mainframe servers, value for record size and block size can be sent to the server before upload by setting the following value to this new configuration field: <code>SITE LRECL=&lt;record_size&gt; BLKSIZE=&lt;block_size&gt;</code>.</p>

Field	Description
<b>Simple mode</b>	Select this option to change the file transfer mode to simple mode and if you are transferring files to AS/400 systems. This mode is applicable for FTP, FTPS, or FTPES protocols.
<b>ASCII mode</b>	<p>Select this option to change the file transfer mode to ASCII mode and choose one of the following <b>Convert line endings</b> options for ActiveTransfer Server to change the line endings of the file:</p> <ul style="list-style-type: none"> <li>■ <b>CRLF - Windows</b></li> <li>■ <b>CR - MAC OS Classic</b></li> <li>■ <b>LF - Unix</b></li> <li>■ <b>No change</b></li> </ul> <p>This mode is applicable for FTP, FTPS, or FTPES protocols.</p> <p>By default, ActiveTransfer Server uses the <b>Binary</b> file transfer mode for the <b>Move</b> operation.</p>
<b>Assign partner</b>	<p>Select this option if you want to assign a partner for the action and do one of the following:</p> <ul style="list-style-type: none"> <li>■ Select the partner to assign from the list of configured partners in ActiveTransfer.</li> <li>■ Type a parameterized value for the partner in the following format: [partner_name], where [partner_name] is a server variable or an action parameter that contains the actual partner name during the execution of an action.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> For virtual folders, use this option only if you want to override the partners configured for the folders.</p> </div>

A move task moves all the files passed on from the previous task to the location specified in **Destination location**. The files are removed from the source folder. The list of files in the destination location is passed on to the subsequent task.

For example, an action configured with the following tasks:

1. Find task: Find files in **Source location** = <source folder>
2. Encrypt task: Encrypt the files.
3. Move task: Moves the files to the **Destination location** = <destination folder>

The action results in the following:

1. Find task lists all the files in the <source folder>.

2. Encrypt task encrypts all the files listed by the find task.
3. Move task moves the files that are encrypted by the encrypt task to the *<destination folder>*.

## Delete Task Configuration

You can configure the following properties for the Delete file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> </div> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Retry [ ] times at an interval of [ ] seconds</b>	Select this option to retry a failed delete operation for the specified number of times at the interval specified in seconds.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

A “delete” task deletes the files that are passed on from the previous task. The deleted files are not passed on to the subsequent task. If a file filter is configured in the task, only then the files that do not match the file filter are passed on to the next task.

## Rename Task Configuration

You can configure the following properties for the Rename file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$:</code> Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$:</code> Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*)):</code> Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>New file name</b>	Type a new file name for the file.
<b>Retry [ ] times at an interval of [ ] seconds</b>	Select this option to retry a failed rename operation for the specified number of times at the interval specified in seconds.
<b>Skip renaming subfolders if parent folder is renamed</b>	Select this option to rename a parent folder but not the folder beneath the folder.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

A rename task renames the files passed on from the previous task. The files that are renamed are not passed on to the next task.

## Encrypt Task Configuration

You can configure the following properties for the Encrypt file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> </div> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Encrypt with Public PGP Key alias</b>	Type the certificate alias for the public key file.
<b>Add signature</b>	Type the certificate alias for the private key file.
<b>ASCII-Armor</b>	Select this option to wrap PGP files in BASE64-encoded format to make them more secure when emailing them.
<b>Delete original file</b>	Select this option to delete the original file and retain only the encrypted files.

Field	Description
<b>Encrypt with integrity check</b>	Select this option to configure Modification Detection Code (MDC) to decrypt files that are encrypted with ActiveTransfer's event.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails.

An encrypt task encrypts files passed on from the previous task. ActiveTransfer supports only PGP-based file encryption. The encrypted file is saved with the name `original-filename.PGP`. After the successful execution of an encrypt task, the source folder location contains both, the original files and the corresponding encrypted files, but only the encrypted files are passed on to the subsequent task for processing. If you select **Delete original file**, the original files are deleted. If you configure a move task after an encrypt task, the move task moves the encrypted file and not the original file.

**Note:**

You need to migrate all assets to certificate IDs using ActiveTransfer built-in service `wm.mft.admin:updateFileBasedCertToDB` before exporting and importing to higher environments, if these assets have any configurations pointing to a filepath as created by using Software AG Designer. Run the `wm.mft.admin:updateFileBasedCertToDB` service, to scan all the assets for certificates and store them into a database linking them to the assets using certificate IDs. If you later want to revert this behavior, run the `wm.mft.admin:updateCertFromDBToFile` service.

## Decrypt Task Configuration

You can configure the following properties for the Decrypt file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.

**Note:**

You can use wildcard characters to filter the file names. For example, type `*.zip` to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the **File filter** box, preceded and followed by wildcard characters. For example, type `*invoice*.zip` to trigger the action based on the file URLs, when ZIP files containing the character string `invoice` in their file names are uploaded or downloaded. If you define a **File filter** for a task, the task acts only on files that are filtered out.

Field	Description
	<p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Decrypt with Private PGP key alias</b>	<p>Type the certificate alias for the private key file.</p> <p><b>Note:</b>ActiveTransfer Server can decrypt the file only if the file is encrypted with the corresponding public key.</p>
<b>Verify signature</b>	<p>Type the certificate alias for the public key file.</p> <p><b>Note:</b>ActiveTransfer Server can verify the signature only if it was added during encryption.</p>
<b>Derive file name from input file</b>	Select this option to retain the original filename of the encrypted file.
<b>Delete original file</b>	Select this option to delete the original file and retain only the decrypted files.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

A decrypt task decrypts files passed on from the previous task and creates decrypted files without the `.PGP` extension. The source folder location contains both, the original files and the corresponding decrypted files. If you select **Delete original file**, the original files are deleted. For example, you have configured a post-processing action which is triggered by a file uploaded to a folder (for example, a folder named `incoming`) that points to a physical location. You have also configured the following tasks in the action:

1. Move task: To move a file that matches the filter, `*invoice*.PGP` from the `incoming` folder to the `working` folder.
2. Decrypt task: To decrypt the file with the **Delete original file** option is selected.

After the action is executed successfully, the decrypted file (without the PGP extension) is available in the `working` folder, and ActiveTransfer deletes the original encrypted file. If you want to make the files from the `incoming` folder available to an task that is configured to execute after the decrypt task, ensure that you do the following:

- Do not select **Delete original file** for the decrypt task.
- Configure a find task to find the original files from the incoming folder in the incoming folder.

## Zip Task Configuration

You can configure the following properties for the Zip file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> </div> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Destination location</b>	<p>Select one of the following options to configure the location where the file will be zipped:</p> <ul style="list-style-type: none"> <li>■ <b>Local file path</b>, if the destination location is on your local machine, type or browse to the location. To specify a file URL for a shared location, use the <code>FILE:///host/SharedFolder/</code> syntax. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.</li> <li>■ <b>Remote path</b>, if the destination location is on a remote server, select a protocol (transport mechanism) from the list, and type or browse to the file path location. For example, <code>protocol://&lt;host&gt;:&lt;port&gt;/DestinationFolder/</code>.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ Type the <b>User name</b> and <b>Password</b> for the remote system.</li> <li>■ Select <b>Use proxy</b> if you want to route file transfers to remote servers through a proxy server, and select one of the following options: <ul style="list-style-type: none"> <li>■ <b>Global proxy settings</b>, if you want ActiveTransfer to use the default proxy server alias set up in Integration Server or ActiveTransfer.</li> <li>■ <b>Select proxy alias</b>, if you want to use a specific proxy server alias for the folder, then select the appropriate proxy server alias to use from the available list.</li> </ul> </li> <li>■ Select if you want ActiveTransfer Server to recover from a download that was not completed.</li> <li>■ Click <b>Test Connection</b> to check the connection to the remote server with or without a proxy server.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Tip:</b> If you want to connect to a remote server using a secure protocol (FTPES, FTPS, HTTPS or SFTP) and want to configure authentication using secure key exchange, create a folder for the remote server and configure the certificate alias parameters. You can then use the folder that you configured in the <b>Virtual folder</b> option of the <b>Source location</b> in the task.</p> </div> <ul style="list-style-type: none"> <li>■ <b>Virtual folder:</b> To specify a virtual folder, type or browse to the location of the folder. If you want to point to a subfolder within the folder, append the URL in the box with the details of the subfolder.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the action is configured.</p> </div>
<b>Create directory</b>	Select this option to enable ActiveTransfer to create the destination folder if the folder specified in <b>Destination location</b> is not present.
<b>ZIP file name</b>	Type a name for the ZIP file. Alternatively, you can provide a variable name such as <i>{stem}.zip</i> as the ZIP file name. <i>{stem}.zip</i> is the default file name.
<b>Assign partner</b>	<p>Select this option if you want to assign a partner for the action and do one of the following:</p> <ul style="list-style-type: none"> <li>■ Select the partner to assign from the list of configured partners in ActiveTransfer.</li> <li>■ Type a parameterized value for the partner in the following format: [partner_name], where [partner_name] is a server variable or an action parameter that contains the actual partner name during the execution of an action.</li> </ul>

Field	Description
	<p><b>Note:</b> For virtual folders, use this option only if you want to override the partners configured for the folders.</p>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The zip task compresses a specified file or a set of files and copies the compressed file to the location specified in **Destination location**. After the successful execution of the zip task, the original source files and the target zip file are available to the subsequent task. If the input path is that of a folder, ActiveTransfer does not compress the files/contents of the specified folder.

In single-thread, sequential processing, each action results in a single zip file. However, if the zip task occurs after parallel processing starts, each thread results in a separate zip file.

## Unzip Task Configuration

You can configure the following properties for the Unzip file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.

**Note:**

You can use wildcard characters to filter the file names. For example, type \*.zip to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the **File filter** box, preceded and followed by wildcard characters. For example, type \*invoice\*.zip to trigger the action based on the file URLs, when ZIP files containing the character string `invoice` in their file names are uploaded or downloaded. If you define a **File filter** for a task, the task acts only on files that are filtered out.

Few examples for regular expressions are:

- `^(?!.*purchaseorder).*$`: Excludes files with the file URL containing purchaseorder.
- `*/out/*.*`: Include files with the file URL containing the folder out.
- `^abc(.*?)123$`: Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def.

Field	Description
	<ul style="list-style-type: none"> <li>■ <code>NEW-(*.doc) (*_backup_*)</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Delete original ZIP file</b>	Select this option to delete the original ZIP file after it is unzipped.
<b>Destination location</b>	<p>Select one of the following options to configure the location to which the contents of the file will be extracted:</p> <ul style="list-style-type: none"> <li>■ <b>Local file path</b>, if the destination location is on your local machine, type or browse to the location. To specify a file URL for a shared location, use the <code>FILE:///host/SharedFolder/</code> syntax. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.</li> <li>■ <b>Remote path</b>, if the destination location is on a remote server, select a protocol (transport mechanism) from the list, and type or browse to the file path location. For example, <code>protocol://&lt;host&gt;:&lt;port&gt;/DestinationFolder/</code>. <ul style="list-style-type: none"> <li>■ Type the <b>User name</b> and <b>Password</b> for the remote system.</li> <li>■ Select <b>Use proxy</b> if you want to route file transfers to remote servers through a proxy server, and select one of the following options: <ul style="list-style-type: none"> <li>■ <b>Global proxy settings</b>, if you want ActiveTransfer to use the default proxy server alias set up in Integration Server or ActiveTransfer.</li> <li>■ <b>Select proxy alias</b>, if you want to use a specific proxy server alias for the folder, then select the appropriate proxy server alias to use from the available list.</li> </ul> </li> <li>■ Select if you want ActiveTransfer Server to recover from a download that was not completed.</li> <li>■ Click <b>Test Connection</b> to check the connection to the remote server with or without a proxy server.</li> </ul> </li> </ul> <p><b>Tip:</b> If you want to connect to a remote server using a secure protocol (FTPES, FTPS, HTTPS or SFTP) and want to configure authentication using secure key exchange, create a folder for the remote server and configure the certificate alias parameters. You can then use the folder that you configured in the <b>Virtual folder</b> option of the <b>Source location</b> in the task.</p> <ul style="list-style-type: none"> <li>■ <b>Virtual folder:</b> To specify a virtual folder, type or browse to the location of the folder. If you want to point to a subfolder within the folder, append the URL in the box with the details of the subfolder.</li> </ul> <p><b>Note:</b></p>

Field	Description
	The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the action is configured.
<b>Assign partner</b>	<p>Select this option if you want to assign a partner for the action and do one of the following:</p> <ul style="list-style-type: none"> <li>■ Select the partner to assign from the list of configured partners in ActiveTransfer.</li> <li>■ Type a parameterized value for the partner in the following format: [partner_name], where [partner_name] is a server variable or an action parameter that contains the actual partner name during the execution of an action.</li> </ul> <p><b>Note:</b> For virtual folders, use this option only if you want to override the partners configured for the folders.</p>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The unzip task decompresses the specified zip file. After a successful unzip task, both the original zip file and the extracted files are passed on to the subsequent task. If the “unzip” task occurs after parallel processing starts, all files resulting from the “unzip” task are treated as part of a single thread. Therefore, in the **Activities** section of the Action Log page, ActiveTransfer maintains the **File Seq No** of the original zip file for the particular thread until the action execution is completed.

## Write Content Task Configuration

You can configure the following properties for the Write content file operation task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type *.zip to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type *invoice*.zip to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded</p>

Field	Description
	<p>or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing purchaseorder.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder out.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_.</li> </ul>
<b>File path</b>	Type the path containing the file to write to.
<b>Overwrite file contents</b>	Select this option if the file already exists and you want to replace the entire contents of the existing file with new content.
<b>Contents if file does not exist</b>	Type or paste the content to write to the file if the file does not exist.
<b>Add before</b>	<p>Select this option to insert new content before existing content in the file and do the following:</p> <ul style="list-style-type: none"> <li>■ If you want to insert the content at the beginning of the file, select <b>Beginning of file</b> and then type or paste the new content in the <b>Contents</b> box.</li> <li>■ If you want to insert the content before a specific string of existing content in the file, select <b>Find</b>, type the string in the box beneath this option, and then type or paste the new content in the <b>Contents</b> box.</li> </ul>
<b>Add after</b>	<p>Select this option to insert new content after existing content in the file and do the following:</p> <ul style="list-style-type: none"> <li>■ If you want to insert the content at the end of the file, select <b>End of file</b> and then type or paste the new content in the <b>Contents</b> box.</li> <li>■ If you want to insert the content after a specific string of existing content in the file, select <b>Find</b>, type the string in the box beneath this option, and then type or paste the new content in the <b>Contents</b> box.</li> </ul>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The write content task adds the specified information about the list of files to an existing file in **File path** or to a new file created for this purpose. After the successful execution of the task, the

list of files from the previous task is passed on to the subsequent task. The file created or modified by this task is not passed on to the next task.

Example: An action configured with the following task:

1. Find task: Find files in **Source location** = *<source folder>*
2. Write content task: Writes information regarding the files in a specified file.
3. Move task: Moves the files to the **Destination location** = *<destination folder>*

The action results in the following:

1. Find task lists all the files in the *<source folder>*.
2. Write content task writes information on the files passed on to it by the find task. For example, the task could write the file names of all the files passed on to it to a *<file.ext>* file specified in the task.
3. Move task moves the files that are encrypted by the encrypt task to the *<destination folder>*.

## Execute Integration Server Service Task Configuration

You can configure the following properties for the *Execute Integration Server service* task:

Field	Description
<b>Task name</b>	Type a unique name for the task.

<b>File filter</b>	Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.
--------------------	--

### Note:

You can use wildcard characters to filter the file names. For example, type *\*.zip* to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the **File filter** box, preceded and followed by wildcard characters. For example, type *\*invoice\*.zip* to trigger the action based on the file URLs, when ZIP files containing the character string *invoice* in their file names are uploaded or downloaded. If you define a **File filter** for a task, the task acts only on files that are filtered out.

Few examples for regular expressions are:

- *^(?!.\*purchaseorder).\*\$*: Excludes files with the file URL containing *purchaseorder*.
- *\*/out/\*.\**: Include files with the file URL containing the folder *out*.

Field	Description
	<ul style="list-style-type: none"> <li>■ <code>^abc(.* )123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Service</b>	Browse to select or type the Integration Server package that contains the service you want to execute from the list.
<b>Include file path</b>	Select this option if you want ActiveTransfer to provide the path of the target file to the respective service. The file path information is passed to the service as input parameter <i>filePath</i> .
<b>Include file content</b>	Select this option to pass the contents of the file to the service and select the transmission method ( <b>As bytes</b> or <b>As stream</b> ). The file content is passed to the service as input parameters <i>fileContent</i> and <i>fileBytes</i> , or as <i>fileContent</i> and <i>fileStream</i> . Code your input parameter as <i>fileContent + fileBytes</i> or <i>fileContent + fileStream</i> . <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> You can ignore this option if your service does not require the file content as input (for example, if the service only writes the name of the files being uploaded, or the names of the users who uploaded them).</p> </div>
<b>Extract service output</b>	Click  to add the variables with <b>Variable name</b> that you want to assign to the output parameters of the service and the <b>Variable path</b> (iData path) of the output parameter.
<b>Execute action even if there are no files</b>	Select this option if you want to execute the task even when no files are passed on to this task from the previous task. For example, you might have a requirement to trigger an Integration Server service from a scheduled action after all the files in a folder have been successfully deleted. Another example could be invoking an Integration Server service for audit purposes even if there are no files available to be processed.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The “Execute Integration Server service” task, runs the specified Integration Server service for each file in the list that is passed on to the task by the previous task. This task does not modify the list of files from the previous task.

## Execute Script Task Configuration

You can configure the following properties for the *Execute script* task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Command</b>	Type a command. Keep in mind that running a batch ( <code>.bat</code> ) file requires running <code>cmd.exe</code> at a command prompt and passing it the arguments to execute the batch file.
<b>Arguments</b>	Type the command's arguments. For example, enter <code>{real_path}/archive/{name}:</code> . If the file is uploaded to <code>/uploads/stuff.zip</code> , it will be copied to <code>/archive/stuff.zip</code> .
<b>Separator</b>	Type a regular expression to separator arguments.
<b>Working directory</b>	<p>Type the path to the directory where the command will be executed. For example, when an application searches for a resource such as a configuration file, the application searches in the location specified here.</p> <p><b>Note:</b> Make sure the path ends with <code>"/</code> to identify the location as a folder and not a file.</p>

Field	Description
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

You should configure the execute script task properties depending on your operating system. An example each for the Windows and Unix/Linux platforms are listed as follows:

- **Windows Platform:** If you want to execute the batch file `C:\SAG\batchfiles\test.bat`, the properties that you need to specify for the execute script task are:

**Command** `C:\Windows\System32\cmd.exe`

**Argument** `/c;start;test.bat`

**Separator** ;

**Working Directory** `C:\SAG\batchfiles\`

- **Unix/Linux Platforms:** You can directly specify the script file name. If you want to execute the batch file `/home/data/batchfiles/test.sh`, use the following properties in the execute script task:

**Command** `/bin/bash`

**Argument** `test.sh;arg1;arg2`

**Separator** ;

**Working Directory** `/home/data/batchfiles`

The above configuration properties can vary depending on the specific operating system that hosts your ActiveTransfer Server. In some of the operating systems, you might require an exit command at the end of the script file to properly terminate the command process.

The “execute script” task runs a script for each file in the list that is passed on to the task by the previous task. The script should be available in the same location as the files. The script is run on the machine on which ActiveTransfer is installed. The execute script task waits for the script to complete execution before passing on the control to the next task. The script that is executed as part of this task should include an `exit` command so that the execution control is transferred back to ActiveTransfer. This task does not modify the list of files from the previous task.

## Execute Trading Networks Service Task Configuration

You can configure the following properties for the *Execute Trading Networks service* task:

### Prerequisites

- If you need to send large files to Trading Networks, configure your target Trading Networks appropriately. For details on how to configure Trading Networks to process large files, see the Trading Networks documentation.

- For remote installations of ActiveTransfer and Trading Networks, list the remote server aliases of the remote Trading Networks instances in the parameter `mft.aliases.tn`.
- If you have ActiveTransfer, list remote server aliases of ActiveTransfer nodes in the parameter `mft.group.aliases`.

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> </div> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Category</b>	Select the Integration Server package that contains the service you want to execute from the list.
<b>Service</b>	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>XML</b>, if you want to execute the Trading Networks service <code>wm.tn:receive</code> to process XML document types.</li> <li>■ <b>EDI</b>, if you want to execute the Trading Networks service <code>wm.tn:receive</code> to process EDI document types.</li> <li>■ <b>Flat File</b>, you want to execute a particular Trading Networks service to process flat file document types and do the following:</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ Select a package from the <b>Package</b> list.</li> <li>■ Select your document gateway service for processing and sending the flat file to Trading Networks from the <b>Service</b> list.</li> </ul> <p>For details about flat file processing, see the Trading Networks documentation.</p> <p><b>Note:</b> If you submit flat files to a remote Trading Networks instance, you must have the document gateway service defined on your local Integration Server. For more information about the document gateway service, see the Trading Networks documentation.</p>
<b>Service input</b>	<p>Click  and type the <b>Parameter name</b> and <b>Value</b> for the input parameters of the Trading Networks service that you selected, and add any content types as required, respectively. For more information about the Trading Networks services and their signatures, see the Trading Networks documentation.</p> <p><b>Note:</b> ActiveTransfer post-processing and scheduled actions on remote Trading Networks does not support TN_params document type as input for the Trading Networks Service task execution. For Flat File documents, the input parameter field supports only <b>String</b> values for services.</p>
<b>Execute error task</b>	<p>Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a>.</p>

The “Execute Trading Networks service” task runs the specified Trading Networks service for each file in the list that is passed on to the task by the previous task. This task does not modify the list of files from the previous task.

## Send Universal Messaging/Broker Notification Task Configuration

**Note:**  
This feature is deprecated.

You can configure the following properties for the *Send UniversalMessaging/Broker notification* task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression,

Field	Description
	<p>specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Document type</b>	Select the Integration Server package that contains the service you want to execute from the list.
<b>Include file path</b>	Select this option if you want ActiveTransfer to provide the path of the target file to the respective service. The file path information is passed to the service as input parameter <code>filePath</code> .
<b>Include file content</b>	<p>Select this option to pass the contents of the file to the service and select the transmission method (<b>As bytes</b> or <b>As stream</b>). The file content is passed to the service as input parameters <code>fileContent</code> and <code>fileBytes</code>, or as <code>fileContent</code> and <code>fileStream</code>. Code your input parameter as <code>fileContent + fileBytes</code> or <code>fileContent + fileStream</code>.</p> <p>Specify content for the document type that you selected, and add any content types as required. For more information about document types, Universal Messaging, or Broker notifications, see the Broker and Integration Server documentation.</p> <p><b>Note:</b> You can ignore this option if your service does not require the file content as input (for example, if the service only writes the name of the files being uploaded, or the names of the users who uploaded them).</p>

Field	Description
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The Send Broker notification task, sends an Broker notification for each file in the list that is passed on to the task by the previous task. This task does not modify the list of files from the previous task.

## Send Email Task Configuration

You can configure the following properties for the *Send email* task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type *.zip to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type *invoice*.zip to trigger the action based on the file URLs, when ZIP files containing the character string <i>invoice</i> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> </div> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing purchaseorder.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder out.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_.</li> </ul>
<b>From</b>	The value you specify in <b>From</b> overrides the value specified in the <code>mft.user.email.from</code> parameter for this task.
<b>To</b>	Type the email address of the recipient.

Field	Description
<b>Cc</b>	Type the email addresses of additional recipients.
<b>Bcc</b>	Type the email addresses of recipients that must be hidden.
<b>Subject</b>	Type text to appear in the subject line of the email (for example, <i>Disconnect:?User %user_name%</i> ).  The value you specify in <b>Subject</b> overrides the value specified in the <code>mft.user.email.subject</code> parameter for this task.
<b>Variables/Templates</b>	Select an option to assist you in completing the body of the email from the list. There are several examples of common email messages available.
<b>Body</b>	Modify the content populated from the your selection in <b>Variables/Templates</b> or type your own text.  You can use variables in the body of the email.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

Based on the name of files specified in the source filter, the send email task sends emails to the recipients configured in a file task. Transfer of the specified files triggers the send email task.

In single-thread, sequential processing, ActiveTransfer runs the send email task only once for all files of an action, and includes the information for all files in a single, consolidated email. Therefore, each action results in one email. However, if the send email task occurs after parallel processing of files starts in an action, the number of emails ActiveTransfer sends depends on the number of threads in the action. Let us consider the example of an action having three parallel threads for processing. When the action execution is completed, ActiveTransfer sends one email for each thread, resulting in a total of three emails for the action.

## Write File to Database Task Configuration

You can configure the following properties for the *Write file to database* task:

Field	Description
<b>Task name</b>	Type a unique name for the task.
<b>File filter</b>	Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.  <b>Note:</b> You can use wildcard characters to filter the file names. For example, type <code>*.zip</code> to trigger the action only when ZIP files are uploaded or downloaded.

Field	Description
	<p>To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <code>*invoice*.zip</code> to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <code>purchaseorder</code>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <code>out</code>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <code>abc</code> and ends with <code>123</code>. Matches <code>abc123</code>, <code>abcxyz123</code>, but not <code>abcxyz123def</code>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <code>NEW-</code> that either ends in <code>.doc</code>, or is followed by the string <code>_backup_</code>.</li> </ul>
<b>Service</b>	Select the Integration Server package that contains the service you want to execute from the list.
<b>Include file path</b>	Select this option if you want ActiveTransfer to provide the path of the target file to the respective service. The file path information is passed to the service as input parameter <code>filePath</code> .
<b>Include file content</b>	<p>Select this option to pass the contents of the file to the service and select the transmission method (<b>As bytes</b> or <b>As stream</b>). The file content is passed to the service as input parameters <code>fileContent</code> and <code>fileBytes</code>, or as <code>fileContent</code> and <code>fileStream</code>. Code your input parameter as <code>fileContent + fileBytes</code> or <code>fileContent + fileStream</code>.</p> <p><b>Note:</b> You can ignore this option if your service does not require the file content as input (for example, if the service only writes the name of the files being uploaded, or the names of the users who uploaded them).</p>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The Write file to database task delivers the contents of a file to an Integration Server service for the purpose of writing the content to the database. ActiveTransfer Server provides the content in bytes or stream form to the service according to the format that the service’s input signature requires. This task does not modify the list of files from the previous task.

## Jump Task Configuration

You can define a Jump task that causes ActiveTransfer Server to skip one or more tasks and execute a designated task in the action. A Jump task is unconditional by default. You can also define a jump condition based on which Jump task is executed. ActiveTransfer Server executes the tasks defined in an action sequentially until it encounters a Jump task. The Jump task is triggered if any one file in the list satisfies the Jump condition.

You can configure the following properties for the *Jump* task:

Field	Description
<b>Task name</b>	<p>Type a different name for the task or retain the name that is automatically assigned by ActiveTransfer Server.</p> <p><b>Note:</b> Each task in an action must have a unique name. ActiveTransfer Server assigns a default name for a task which is the task type itself. For example, <i>Jump</i> for a Jump task. When you add a task that already exists in the action with its default name, ActiveTransfer Server appends the default name with a numeral starting at 1. For example, <i>Jump1</i>.</p>
<b>File filter</b>	<p>Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.</p> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type <i>*.zip</i> to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type <i>*invoice*.zip</i> to trigger the action based on the file URLs, when ZIP files containing the character string <i>invoice</i> in their file names are uploaded or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*\$</code>: Excludes files with the file URL containing <i>purchaseorder</i>.</li> <li>■ <code>*/out/*.*</code>: Include files with the file URL containing the folder <i>out</i>.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with <i>abc</i> and ends with <i>123</i>. Matches <i>abc123</i>, <i>abcxyz123</i>, but not <i>abcxyz123def</i>.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with <i>NEW-</i> that either ends in <i>.doc</i>, or is followed by the string <i>_backup_</i>.</li> </ul>

Field	Description
<b>Jump condition</b>	Select a condition you want ActiveTransfer Server to execute for a jump task from the list, select the <b>Qualifier</b> from the list, and type a <b>Value</b> of the server variable. For example, {ext} Equals xml triggers a jump task for all XML files.
<b>Jump to task</b>	Select a task to jump to from the list.
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

The Jump task changes the sequence in which the tasks are executed. The task specified in the “Jump” task is executed instead of the next task in the sequence. The “Jump” task however does not modify the list of files that are passed on from the task prior to the Jump task to the task that is triggered by the Jump task.

## Exclude Task Configuration

You can exclude files from a task or a set of tasks by defining an Exclude task prior to these tasks. The Exclude task uses a **File filter** to exclude files from all the tasks in the action that follow the Exclude task. The files that match the exclude criteria are not be passed on to the next task.

You can configure the following properties for the *Exclude* task:

Field	Description
<b>Task name</b>	Type a different name for the task or retain the name that is automatically assigned by ActiveTransfer Server.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> Each task in an action must have a unique name. ActiveTransfer Server assigns a default name for a task which is the task type itself. For example, Jump for a Jump task. When you add a task that already exists in the action with its default name, ActiveTransfer Server appends the default name with a numeral starting at 1. For example, Jump1.</p> </div>
<b>File filter</b>	Type the name of the file if you want to filter files with specific names. By default, ActiveTransfer Server considers all files. If you want to use regular expression, specify a valid regular expression in <b>File filter</b> and select <b>Use regular expression</b> option.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> You can use wildcard characters to filter the file names. For example, type *.zip to trigger the action only when ZIP files are uploaded or downloaded. To trigger an action based on a name string in the ZIP files, use the name string in the <b>File filter</b> box, preceded and followed by wildcard characters. For example, type *invoice*.zip to trigger the action based on the file URLs, when ZIP files containing the character string <code>invoice</code> in their file names are uploaded</p> </div>

Field	Description
	<p>or downloaded. If you define a <b>File filter</b> for a task, the task acts only on files that are filtered out.</p> <p>Few examples for regular expressions are:</p> <ul style="list-style-type: none"> <li>■ <code>^(?!.*purchaseorder).*</code>: Excludes files with the file URL not containing purchaseorder.</li> <li>■ <code>*/out/*</code>: Include files with the file URL containing the folder out.</li> <li>■ <code>^abc(.*?)123\$</code>: Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def.</li> <li>■ <code>NEW-((*.doc) (*_backup_*))</code>: Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_.</li> </ul>
<b>Execute error task</b>	Select this option to execute an error task if the file operation fails. For more details, see <a href="#">“Error Task Configuration” on page 125</a> .

## Error Task Configuration

You can configure an error task ActiveTransfer execute if any of the configured tasks for a post-processing, scheduled, or monitor folder action fail. You can define any of the tasks that ActiveTransfer offers as the error task. For example, if a file copy task fails, you can use the send email task to notify an administrator of the failure.

The error task is subjected to the following conditions:

- You can create only one error task per action.
- You must configure a task to execute the error task by selecting the **Execute error task** option for the task.
- You must configure the error task just as you would configure any other task for a post-processing or scheduled action.

## Operating Actions

By default, a newly created post-processing, scheduled action, or monitor folder action is inactive. This enables you to work on configuring an action without any concern that the partially configured action is running. After you fully configure the action, you can activate it to associate it with a service.

You can also activate or deactivate more than one action at a time.

### ➤ To perform operations on actions

1. On the navigation pane, select **Actions**.

2. On the Post-Processing actions, Scheduled actions, or Monitor folder actions page, select one or more actions, and do one of the following:

**Tip:**

Each page of the actions list displays a maximum of 50 actions. Only select the actions visible on a single page.

- Click  to activate the selected actions.

**Note:**

Ensure that you define the execution **Criteria** for all the scheduled actions you want to activate. ActiveTransfer ignores any scheduled action that has no execution **Criteria** defined.

- Click  to deactivate the selected actions.
- Click  to copy the selected actions.
- Click  to delete the selected actions.

The selected actions are activated or deactivated based on your selection.

**Tip:**

If you have more actions to select in the additional pages of the actions list, click **Next** or the required page number, and repeat step 2.

## Modifying a Post-Processing, Scheduled, or Monitor folder Action

---

You can edit the configuration settings of an existing post-processing, scheduled, or monitor folder action.

### > To modify an action

1. On the navigation pane, select **Actions**.
2. On the Post-Processing actions, Scheduled actions, or Monitor folder actions page, click on an action that you want to edit.
3. Modify the required configuration settings for the action.
4. Click **Save**.

The action is updated with the modified settings.

## Searching for a Post-Processing, Scheduled, or Monitor folder Action

You can search the post-processing or scheduled actions list to locate an action based on the action name and status.

### ➤ To search for an action

1. On the navigation pane, select **Actions**.
2. On the Post-Processing actions or Scheduled actions page, specify all or one of the following search criteria:

Field	Description
<b>Action name</b>	Type the name of the action you want to view.
<b>Status</b>	Select either <b>Active</b> or <b>Inactive</b> to filter the actions based on active or inactive actions respectively.

3. Click **Reset** and **Apply** for the changes to take effect.

The actions list is populated with the actions matching your search criteria.

## Parameterizing Scheduled Action Tasks

You can parameterize the settings of a scheduled action tasks at runtime. By parameterizing the action task settings, you reduce the number of actions you would otherwise need to configure, especially when files are transferred across several source and destination file systems.

### ➤ To parameterize a configuration setting of a scheduled action tasks

1. In the navigation panel, click **Action > Scheduled** tab.
2. Select the event in the action list or add a new action.
3. Select the task that you want to configure.
4. Type `[variable_name]` in the setting to parameterize.

Where, *variable\_name* is the variable assigned to the configuration setting that you want to parameterize.

For more information on parameterization of specific settings, see [“Additional Information on Parameterizing Event Actions” on page 128](#).

5. Click **Save**.

## Additional Information on Parameterizing Event Actions

You can parameterize the settings of a scheduled event action at runtime. By parameterizing the event action settings, you reduce the number of events you would otherwise need to configure, especially when files are transferred across several source and destination file systems.

- For any remote file path, you can parameterize the URL but not the username and password. The runtime value for the URL should contain the username and password to be used. Provide the URL information in the format `<protocol>://<username>:<password>@<host>:<port>/<path>/`. For example, `FTP://user:password@ftp.softwareag.com/outbound/`

### Note:

If you use this format to parameterize the file path URL with values for the username and password, at runtime, ActiveTransfer ignores the values specified for the username and password parameters. This rule is applicable to the remote file URLs configured in the following actions:

Action	URL
Find action	: Find URL
Copy action	: Destination URL
Move action	: Destination URL
Unzip action	: Destination URL
Zip action	: Zip File Path

- Use the `wm.mft.schedule:createRemoteURL` service to create URLs in the ActiveTransfer Server format.
- You can parameterize only the following event action settings:

Action	Action Settings
Find	File URL File Name Source Filter Folder Depth Stability Check Delay Stability Check Minutes Maximum Items to Find

Action	Action Settings
	Last Modification Days Last Modification Hours Last Modification Minutes Retry Interval Retry Count
Copy	Destination URL Rename file to Source Filter File Name Wait for Sec Give up After Retry Interval Retry Count
Decrypt	Decryption Key File Source Filter
Delete	Retry Interval Retry Count
Send Email	From To CC BCC Subject Body Source Filter
Encrypt	Decryption Key File Source Filter
Execute Script	Command Arguments

Action	Action Settings
	Separator
	Working Directory
	Source Filter
Jump	variable
	variable2
	Source Filter
Move	Destination URL
	Rename file to
	Source Filter
	File Name
	Wait for Sec
	Give up After
	Retry Interval
	Retry Count
Rename	New File Name
	Source Filter
	Retry Interval
	Retry Count
Unzip	Destination URL
	Source Filter
Write Content	File Path
	Source Filter
Zip	Zip File Path
	File Name
	Source Filter
	Zip File Name

# 8 Managing Users and Templates

■ Overview .....	132
■ Templates .....	144

## Overview

---

ActiveTransfer profile of a user contains all of the settings required for users to log on to ActiveTransfer Server to transfer files and perform other ActiveTransfer tasks.

You can add users in ActiveTransfer by defining user profiles in one of the following ways:

- If a user is already defined in Central Users, through an internal system directory service or an external directory service such as LDAP, you create an ActiveTransfer profile for the user by associating the user with ActiveTransfer.

**Note:**

Ensure that you have Universal Messaging installed to enable the synchronization of users created with Integration Server and ActiveTransfer.

- If the user is not already defined in Central Users, you can create the user in an internal or external system directory service and define an ActiveTransfer profile for the user at the same time. For details, see [“Creating a New User” on page 134](#).

**Note:**

Install **Central User Management** to configure users in Common Directory Services in Integration Server

In Central Users, members of a group or role can be any user, any role, or any group. Groups and roles can also have multiple groups and roles in a parent-child hierarchy. Inheritance of permissions and settings for groups and roles work as follows:

- When a user is a member of any child group or child role, the user also inherits the parent group or role. For example, the user Mary is added to *group B*, and *group A* is the parent of *group B*. Consequently, Mary is also a member of *group A*.
- Any settings applied to the parent groups and roles in ActiveTransfer user management configuration, folder configuration, and post-processing action configuration are inherited by all child groups and roles. For example, the role *Admin\_all* is the parent of the role *Admin\_a* and *Admin\_a* is the parent of group *Admin\_bldEast*. *Admin\_all* is provided access to the folder *Enterprise*. Therefore, all members of the role *Admin\_a* and group *Admin\_bldEast* also have access to *Enterprise*.
- A user is able to log in to ActiveTransfer if the user is a member of any role or group for which ActiveTransfer login is enabled.
- A user's ActiveTransfer login permission is disabled only when login is disabled for all groups and roles of which the user is a member. If, however, ActiveTransfer login is disabled only for a few groups or roles, the user will continue to have login permission to ActiveTransfer.

## Features in Users Templates

This topic provides information about specific features you can use to configure advanced settings for user and templates in ActiveTransfer:

## Restrictions for a User

You can define the following restrictions for a user:

- Restrict server availability to specified times and days of the week.
- Restrict particular actions for files that match a specified pattern and restrict access to subfolders in a folder structure that match a specified pattern.
- Restrict login volume and duration and specify authentication settings.
- Restrict connections by protocol or IP address and specify default character encoding.

These settings will override any restrictions set in the template associated with the user, role, or group.

## Restrictions for Authentication and Login

You can set authentication and login restrictions that specify the maximum number of users who can log in simultaneously, the maximum login and idle times per session, public key and password requirements, and the paths to trusted public SSH key files.

## Restrictions for Files

You can restrict particular actions for files that match a specified pattern. For example, you can restrict users from uploading files that end with `.exe`. You can also restrict access to subfolders in the file system that match a specified pattern.

## Restrictions for Connections

You can restrict connections to ActiveTransfer Server or an ActiveTransfer Gateway instance by choosing the protocols or client IP addresses for access. You can also specify the default character encoding for the connection between the user and ActiveTransfer Server.

## Active Time Window

You can specify the days of the week and the time during which users can connect to ActiveTransfer Server.

**Note:**

The days and times are represented in the time zone of the ActiveTransfer Server.

## Encryption and Decryption

You can define specific file-based encryption and decryption PGP keys for users. These settings will override any encryption assignments set in the template associated with the user, role, or group.

When encrypted, files are stored on the user's drive. Encrypted files are decrypted only if they are transferred back through ActiveTransfer using the same key that was used to encrypt them. When encryption and decryption keys are configured at multiple levels (user, server, and folder), ActiveTransfer enforces the following order of preference:

1. Users
2. Folders
3. Servers

For example, if user *A* accesses port *10* and uploads a file in a VFS *MN*, then ActiveTransfer checks if the encryption or decryption key is available for user *A*. If no key is available at the user level, then ActiveTransfer checks for the folder settings for a key. If no key is present at the VFS level, then ActiveTransfer checks the server level settings for the key.

## File-based Encryption for Templates

You can define specific file-based encryption and decryption PGP keys for users assigned to a template. When files are encrypted, they are stored on a user's drive in a format that cannot be read outside of ActiveTransfer. Encrypted files are decrypted only if they are transferred back through ActiveTransfer using the same key that was used to encrypt them.

### Note:

You must obtain the appropriate keystores and ensure that these keystore files reside on the machines that host the ActiveTransfer Server or ActiveTransfer Gateway on which you perform these configuration tasks.

You can override the template-level encryption and decryption options for a specific user.

“.” on page 137

“.” on page 145

## Creating a New User

If a user is not already defined as a Central Users user and does not have an ActiveTransfer profile, then you can create the user in the Common Directory Services and define an ActiveTransfer profile for the user.

### ➤ To create a new user

1. On the navigation pane, select **User > Users**.
2. On the Users page, click  **+ Add**.
3. In the Add users dialog box, select **Create new user** and type the **User ID**, **First name**, **Last name**, and **Email address** in the respective boxes.
4. Click **Advanced**. If you want to change the user's password, do one of the following:
  - Select **Generate random password** if you want ActiveTransfer to create a password.
  - Select **Create new password** if you want to create a specific password.

5. In the **Listeners shared with user over email** section, specify the ActiveTransfer Server listeners to include in emails sent to users along with the user credentials:
  - To include listener that are listed as **Default in emails** on the **Listeners** page, select **Default listeners**.
  - To include specific listeners, select **Select listeners**, and then select the required listeners.
6. Click **Add new user**.

**Note:**

This button is enabled only when you provide the user information. You can continue to add more users to the selected users' list.

7. Click **Add**.

ActiveTransfer Server adds an ActiveTransfer profile for the user appears in the users list.

## Associating an Existing User with ActiveTransfer

If a user is already defined as a Central Users but does not have an ActiveTransfer profile, you can associate the user with ActiveTransfer.

### ➤ To associate an existing Central User with ActiveTransfer

1. On the navigation pane, select **Users > Users**.
2. On the Users page, click  **+ Add**.
3. In the Add users dialog box, select **Search existing users** and type the search criteria, such as user name, first name, or last name in the box.
4. Click **Search**.
5. In the search results, select the users you want to associate with ActiveTransfer, and click **Ok**.
6. Click **Add**.

ActiveTransfer Server adds an ActiveTransfer profile for the user and appears in the users list.

## Associating an Existing Role with ActiveTransfer

You can associate user roles already defined in Central Users with ActiveTransfer.

**> To associate an existing Central User role with ActiveTransfer**

1. On the navigation pane, select **Users > Roles**.
2. On the Roles page, click  **+ Add**.
3. In the Add existing roles dialog box, type the search criteria, such as role name in the box.
4. Click **Search**.
5. In the search results, select the roles you want to associate with ActiveTransfer, and click **Ok**.
6. Click **Add**.

The roles are added in ActiveTransfer and appear in the roles list.

## Associating an Existing Group with ActiveTransfer

You can associate groups already defined in Central Users with ActiveTransfer. For more information about how to create a group, see *Managing Users with Common Directory Services*.

**> To associate an existing group in Common Directory Services with ActiveTransfer**

1. On the navigation pane, select **Users > Groups**.
2. On the Groups page, click  **+ Add**.
3. In the Add existing groups dialog box, type the search criteria, such as group ID or group name in the box.
4. Click **Search**.
5. In the search results, select the groups you want to associate with ActiveTransfer, and click **Ok**.
6. Click **Add**.

The groups are added in ActiveTransfer and appear in the groups list.

## Configuring Advanced Settings for Users

Once associated with ActiveTransfer, you can configure advanced settings for users.

### > To configure advanced settings

1. On the navigation pane, select **Users > Users**.
2. In the Users page, click on the user, role, or group for which you want to configure additional settings.
3. If you want to change the user's password, click **Change Password**.

#### Note:

This step is not applicable for roles and groups.

- a. In the Change password dialog box, do one of the following:
    - Select **Generate random password** if you want ActiveTransfer to create a password.
    - Select **Create new password** if you want to create a specific password.

Select **Would you like to inform the changed password to user?** to inform the user about the password change, and click **Ok**.
  - b. Under **Basic**, you can update the user's **First name**, **Last name**, **Email address**, and the default **Template** associated with the user.
4. You can specify the following details:

Field	Description
<b>Basic</b>	
<b>Distinguished name</b>	Displays the uniquely identified user, role, or group in LDAP or in the Directory Service. For example, <i>uid=john,ou=people,o=system,o=mws</i> .
<b>Disable login</b>	Select this option if you want to disable a user's ID and prevent the user from logging on to the server. The same applies to roles and groups.
<b>Associated partner</b>	
<b>No partner</b>	Select this option if you do not want to associate the user, role, or group with either a partner or your enterprise.

Field	Description
<b>Enterprise</b>	Select this option if you want to associate the user, role, or group with your enterprise.
<b>Partner</b>	Select this option if you want to associate the user, role, or group with a partner, and either select a partner from the list or type a new partner name and click <b>Create</b> .  <b>Note:</b> Trading Networks partners are available only if Trading Networks is installed either on the local or remote machine and if the <code>mft.partners.useTNPartners</code> property is set to true. If <code>mft.partners.useTNPartners</code> is set to false, then you must create partners in ActiveTransfer manually.
<b>Upload preferences:</b> These settings will override any throttling options set in the template associated with the user, role, or group.	
<b>Maximum speed (Kb/sec)</b>	Type the maximum permissible speed in kilobytes per second for an upload operation.
<b>Maximum individual file size (MB)</b>	Type the maximum permissible size in megabytes for an uploaded file.
<b>Maximum amount per session (MB)</b>	Type the maximum amount of data in megabytes that can be uploaded per session.
<b>Maximum amount per day (MB)</b>	Type the maximum amount of data in megabytes that can be uploaded per day.
<b>Maximum amount per month (MB)</b>	Type the maximum amount of data in megabytes that can be uploaded per month.
<b>Download preferences</b>	
<b>Maximum speed (Kb/sec)</b>	Type the maximum permissible speed in kilobytes per second for n download operation.
<b>Maximum amount per session (MB)</b>	Type the maximum amount of data in megabytes that can be downloaded per session.
<b>Maximum amount per day (MB)</b>	Type the maximum amount of data in megabytes that can be downloaded per day.
<b>Maximum amount per month (MB)</b>	Type the maximum amount of data in megabytes that can be downloaded per month.
<b>Active time window</b>	Do one of the following:

Field	Description
	<ul style="list-style-type: none"> <li>■ If you want to restrict access to particular days of a week, then under <b>Days</b>, select the required days you want the server to be available to the user.</li> <li>■ If you want to restrict access to particular time slots, then under <b>Time selector</b>, click . Select the <b>From Time</b> and <b>To Time</b> from the lists, respectively.</li> </ul>
<b>File name filters</b>	<p>You can configure the file name filters to allow or deny commands (Upload, Download, List, Rename) for files that match a specified pattern. For example, you can restrict a user from uploading files that end with ".exe".</p> <ul style="list-style-type: none"> <li>■ When you configure the file name filters for Listener Preferences and Users, the User file name filter configuration overrides the Listener Preferences configuration.</li> <li>■ The file name filter is applied on the filename received by the server. For example, if a .pdf file is uploaded after changing the file extension to .txt, then webMethods.io MFT considers it as a .txt file when applying the filters.</li> </ul>
<b>Patterns</b>	<p>Click  to add one or more patterns to restrict actions to particular files, and specify the following details:</p> <ul style="list-style-type: none"> <li>■ <b>Command:</b> Select a command ( <b>List</b>, <b>Download</b>, <b>Upload</b> or <b>Rename</b>) from the list.</li> <li>■ <b>Filter type:</b> Select a filter type (<b>Starts with</b>, <b>Ends with</b>, or <b>Contains</b>) from the list.</li> <li>■ <b>File name:</b> Type a portion of the file name that the <b>Filter type</b> criterion should evaluate (for example, "exe").</li> </ul> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> Any characters except wildcard characters and regular expressions are permitted. ActiveTransfer Server treats those characters as part of the file name.</p> </div>
<b>Block paths matching these patterns</b>	<p>Click  to restrict a user's access to specific folders in the file system, and specify the following details:</p> <ul style="list-style-type: none"> <li>■ <b>Pattern and Actions:</b> Type the folder path you want to block.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Tip:</b> You can use simple pattern matching by preceding the pattern with the tilde (~) character. For example, to deny user access to the folder /system/bin, you must type: ~/system/bin/*</p> </div>

Field	Description
<b>Authentication and login</b>	
<b>Maximum simultaneous logins</b>	Type the maximum number of simultaneous logins allowed for the same user.  <b>Note:</b> File transfer clients like FileZilla or WinSCP may create additional login sessions to optimize file transfer.
<b>Require public key and password (For SFTP listener)</b>	Select this option if you want ActiveTransfer Server to require the user to provide a public key and password.
<b>Maximum login time per session (min)</b>	Type the maximum number of minutes a user can remain logged in per session.
<b>Maximum idle time per session (min)</b>	Type the maximum number of minutes a user session can remain idle.
<b>Trusted Public SSH key alias</b>	
<b>Public SSH key alias</b>	Click  and specify certificate alias for the trusted public SSH key files.
<b>Connection</b>	
<b>Allowed protocols</b>	Select the protocols for which you want to allow connections for from the list.
<b>Default character encoding</b>	Select the appropriate default character encoding from the list. The default is <b>UTF-8</b> .
<b>IP restrictions</b>	Click  to add one or more IP addresses for which ActiveTransfer Server can accept or deny connection requests and specify the following details: <ul style="list-style-type: none"> <li>■ Select <b>Allow</b> or <b>Deny</b> from the list.</li> <li>■ Type the IP address range in the <b>From</b> and <b>To</b> boxes.</li> </ul>
<b>File-based encryption</b>	
<b>Public PGP key alias</b>	Type or browse the certificate alias for the public PGP key.  <b>Note:</b> You can use the <code>wm.mft.security.pgp:generatePGPKeyFiles</code> service to generate an OpenPGP key pair. For details, see <i>webMethods ActiveTransfer Built-In Services Reference</i> .
<b>File-based decryption</b>	

Field	Description
<b>Private PGP key alias</b>	Type or browse the certificate alias for the private PGP key.
<b>Active tunnels</b>	
<b>Tunnels</b>	Select the tunnel that you want to associate with this user, role, or group from the list of available tunnels on the Acceleration page.
	<p><b>Note:</b> You must only map one tunnel to a user. If you map more than one tunnel to a user, ActiveTransfer Server ignores all but the first tunnel you mapped.</p>

5. Click **Save** or **Save & Close**.

The user, role, or group is updated with the additional settings.

## Modifying a User

You can edit the configuration settings of an existing user, role, or group.

### > To modify a user, role, or group

1. On the navigation pane, select **Users > Users, Roles, or Groups**.
2. In the Users, Roles, or Groups page, click on a user, role, or group that you want to edit.
3. Modify the required configuration settings for the user, role, or group respectively.
4. Click **Save** or **Save & Close**.

The user, role, or group is updated with the modified settings.

## Password Change (By Administrators)

ActiveTransfer administrators can manage user passwords by following the steps mentioned below.

### > To set or change a password

1. On the navigation pane, select **Users>Users**

2. In the Users page, click on the user to configure additional settings.
3. If you want to change the user's password, click **Change Password**.
4. In the **Change Password** dialog box, do one of the following
  - a. Select **Generate random password**. The user will receive a password reset link on their mail ID.

**Note:**

ActiveTransfer Server and ActiveTransfer Gateway need to be restarted for the changes made on the SMTP Server configurations to reflect on the password reset link.

- a. Select **Create new password** if you want to create a specific password. Select **Would you like to inform the changed password to user?** to inform the user about the password change, and click **Ok**.

## Password Change (By Partner Users)

ActiveTransfer partner users can now set or change their password from the login page of ActiveTransfer Webclient.

➤ **To set or change a password:**

1. Click on the generate password button on the login page.
2. Enter the username or registered mail id and click proceed.
3. A password reset link will be sent on your registered mail id.
4. Click on the password reset link in your mail.

**Note:**

This password reset link expires 24 hours from the time you requested for a password change.

5. You will be redirected the Change password page after clicking on the link.
6. Enter password that matches the minimum requirements in both Password and Confirm Password boxes.
7. Click Proceed.
8. You will receive a password reset confirmation on both mail and on your current screen.

9. 1. You can proceed to login by clicking on login.

## Searching for Users

You can search the users list to locate a user by specifying the required search criteria.

### > To search for users

1. On the navigation pane, select **Users**.
2. On the Users page, specify all or one of the following search criteria:

Field	Description
<b>User ID</b>	Type the user ID associated with the user.
<b>First name</b>	Type the first name of the user.
<b>Last name</b>	Type the last name of the user.

3. Click **Reset** and **Apply** for the changes to take effect.

The user list is populated with the the users matching your search criteria.

## Searching for Roles

You can search the roles list to locate a role by specifying the required search criteria.

### > To search for roles

1. On the navigation pane, select **Roles**.
2. On the Roles page, specify the name of the role search criteria in the **Role name** box.
3. Click  to search the list of roles.

The role list is populated with the the roles matching your search criteria.

## Searching for Groups

You can search the group list to locate a group by specifying the required search criteria.

### > To search for groups

1. On the navigation pane, select **Groups**.
2. On the Groups page, specify the name of the group search criteria in the **Group name** box.
3. Click  to search the list of groups.

The group list is populated with the the groups matching your search criteria.

## Templates

---

A template contains predefined settings such as, limits for upload and download file sizes, server connection restrictions, encryption and decryption settings, and settings to help speed up file transfers. ActiveTransfer Server applies these settings to all the users associated with a template.

ActiveTransfer provides a *Default Template*. The default template provides default settings, which you can modify to meet your requirements. You can also create additional templates and specify any template to use as the default for new users.

**Note:**

You can assign a different template to an existing user and override individual settings for the user.

You can add templates in ActiveTransfer by configuring basic settings, such as name and description using the quick add feature. To configure additional settings for templates, see [“Configuring Additional Settings for a Template” on page 145](#).

## Adding a Template

You can add a template to ActiveTransfer Server using the quick add feature. To configure additional settings for the template, see [“Configuring Additional Settings for a Template” on page 145](#).

### > To add a template

1. On the navigation pane, select **Users > Templates**.
2. On the Templates page, click .
3. In the Add template dialog box, specify the following details:

Field	Description
<b>Name</b>	Type a unique name for the template.
<b>Description</b>	Type a description for the template.

4. Click **Add**.

The new template appears in the templates list.

## Configuring Additional Settings for a Template

You can configure additional settings for a template.

### > To configure additional settings

1. On the navigation pane, select **Users > Templates**.
2. In the Templates page, click on the template for which you want to configure additional settings.
3. You can specify the following details:

Field	Description
<b>Basic</b>	
<b>Name</b>	Type a unique name for the template.
<b>Description</b>	Type a description.
<b>Default template for new user</b>	Select this option if you want to set this template as the default template for new users.
	<p><b>Note:</b> Only one template can be set as the default template. To specify a different default template, save your edits to the current template and switch to the template you want to configure as the default.</p>
<b>Upload preferences</b>	
<b>Maximum speed (Kb/sec)</b>	Type the maximum permissible speed in kilobytes per second for an upload operation.
<b>Maximum individual file size (MB)</b>	Type the maximum permissible size in megabytes for an uploaded file.
<b>Maximum amount per session (MB)</b>	Type the maximum amount of data in megabytes that can be uploaded per session
<b>Maximum amount per day (MB)</b>	Type the maximum amount of data in megabytes that can be uploaded per day.

Field	Description
<b>Maximum amount per month (MB)</b>	Type the maximum amount of data in megabytes that can be uploaded per month.
<b>Download preferences</b>	
<b>Maximum speed (Kb/sec)</b>	Type the maximum permissible speed in kilobytes per second for an download operation.
<b>Maximum amount per session (MB)</b>	Type the maximum amount of data in megabytes that can be downloaded per session.
<b>Maximum amount per day (MB)</b>	Type the maximum amount of data in megabytes that can be downloaded per day.
<b>Maximum amount per month (MB)</b>	Type the maximum amount of data in megabytes that can be downloaded per month.
<b>Active time window</b>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>■ If you want to restrict access to particular days of a week, then under <b>Days</b>, select the required days you want the server to be available to the user.</li> <li>■ If you want to restrict access to particular time slots, then under <b>Time selector</b>, click . Select the <b>From Time</b> and <b>To Time</b> from the lists, respectively.</li> </ul>
<b>File name filters</b>	<p>You can configure the file name filters to allow or deny commands (Upload, Download, List, Rename) for files that match a specified pattern. For example, you can restrict a user from uploading files that end with ".exe".</p> <ul style="list-style-type: none"> <li>■ When you configure the file name filters for Listener Preferences and Users, the User file name filter configuration overrides the Listener Preferences configuration.</li> <li>■ The file name filter is applied on the filename received by the server. For example, if a .pdf file is uploaded after changing the file extension to .txt, then webMethods.io MFT considers it as a .txt file when applying the filters.</li> </ul>
<b>Patterns</b>	<p>Click  to add one or more patterns to restrict particular actions for certain files, and specify the following details:</p> <ul style="list-style-type: none"> <li>■ <b>Command:</b> Select a command ( <b>List</b>, <b>Download</b>, <b>Upload</b> or <b>Rename</b>) from the list.</li> <li>■ <b>Filter type:</b> Select a filter type (<b>Starts with</b>, <b>Ends with</b>, or <b>Contains</b>) from the list.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>File name:</b> Type a portion of the file name that the <b>Filter type</b> criterion should evaluate (for example, “exe”).</li> </ul> <p><b>Note:</b> Any characters except wildcard characters and regular expressions are permitted. ActiveTransfer Server treats those characters as part of the file name.</p>
<b>Block paths matching these patterns</b>	<p>Click  to restrict access to specific folders in the file system, and specify the following details:</p> <ul style="list-style-type: none"> <li>■ <b>Pattern and Actions:</b> Type the folder path you want to block.</li> </ul> <p><b>Tip:</b> You can use simple pattern matching by preceding the pattern with the tilde (~) character. For example, to deny user access to the folder /system/bin, you must type: ~/system/bin/*</p>
<b>Authentication and login</b>	
<b>Maximum simultaneous logins</b>	Type the maximum number of simultaneous logins allowed for the same user.
<b>Require public key and password (for SFTP listener)</b>	Select this option if you want ActiveTransfer Server to require the user to provide a public key and password.
<b>Maximum login time per session (min)</b>	Type the maximum number of minutes a user can remain logged in per session.
<b>Maximum idle time per session (min)</b>	Type the maximum number of minutes a user session can remain idle.
<b>Trusted Public SSH key alias</b>	
<b>Public SSH key alias</b>	Click  and specify certificate alias for the trusted public SSH key files.
<b>Connection</b>	
<b>Connection protocols</b>	Select the protocols for which you want to allow connections for from the list.
<b>Default character encoding</b>	Select the appropriate default character encoding from the list. The default is <b>UTF-8</b> .
<b>IP restrictions</b>	Click  to add one or more IP addresses for which ActiveTransfer Server can accept or deny connection requests and specify the following details:

Field	Description
	<ul style="list-style-type: none"><li>■ Select <b>Allow</b> or <b>Deny</b> from the list.</li><li>■ Type the IP address range in the <b>From</b> and <b>To</b> boxes.</li></ul>
<hr/> <b>File-based encryption</b> <hr/>	
<b>Public PGP key alias</b>	Type or browse the certificate alias for the public PGP key.  <b>Note:</b> You can use the <code>wm.mft.security.pgp:generatePGPKeyFiles</code> service to generate an OpenPGP key pair. For details, see <i>webMethods ActiveTransfer Built-In Services Reference</i> .
<hr/> <b>File-based decryption</b> <hr/>	
<b>Private PGP key alias</b>	Type or browse the certificate alias for the private PGP key. <hr/>
<b>Active tunnels</b> <hr/>	
<b>Tunnels</b>	Select the tunnel that you want to associate with this template from the list of available tunnels on the Acceleration page.  <b>Note:</b> You must only map one tunnel to a template. If you map more than one tunnel to a template, ActiveTransfer Server ignores all but the first tunnel you mapped.

4. Click **Save** or **Save & Close**.

The template is updated with the additional settings.

## Modifying a Template

You can edit the configuration settings of an existing template.

### ➤ To modify a template

1. On the navigation pane, select **Templates**.
2. On the Templates page, click on a template that you want to edit.
3. Modify the required configuration settings for the template.
4. Click **Save** or **Save & Close**.

The template is updated with the modified settings.



# 9 Viewing and Downloading Logs

■ Overview .....	152
■ Viewing the Transaction Log .....	152
■ Viewing the Action Log .....	155
■ Rerun a Post-Processing Action .....	156
■ Viewing the Audit Log .....	159
■ Viewing the Analytical Details .....	160
■ Viewing the Agent Action Log .....	161
■ Viewing the Agent Activity Log .....	162
■ Downloading Log Data .....	164

## Overview

You can view the activities within your environment using the following logs:

- **Transaction log:** ActiveTransfer Server logs all the details for file transactions.
- **Action Log:** ActiveTransfer Server logs all the details for post-processing and scheduled action executions.
- **Audit log:** ActiveTransfer Server logs all the details of updates to ActiveTransfer assets such as listeners, Gateways, virtual folders, and so on.
- **Agent action log:** ActiveTransfer Server logs all the details for agent action executions.
- **Agent activity log:** ActiveTransfer Server logs all the details of activities such as, download of configurations from ActiveTransfer Server, agent action execution, and agent action authentication when connecting to ActiveTransfer Server. All agent activities are logged:
  - On the agent host machine, in *Installation\_directory*\profiles\MAG\log\sag.osgi.log.
  - On ActiveTransfer Server, in the configured ActiveTransfer log file. ActiveTransfer Server log also fetches the agent logs and writes them to the ActiveTransfer log.

## Viewing the Transaction Log

You can view file transactions on your ActiveTransfer Server. By default, the search list is populated with the file transaction details of the current day. You can further filter the file transaction log based on criteria such as date and time, trigger source, status of the file transfer, search text, transaction ID, and file name.

### > To view a file transaction log

1. On the navigation pane, select **Logs > Transaction log**.
2. On the Transaction log page, you can filter the log based on the following criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range with a time range in the HH:MM:SS (12-hour clock) format, and click <b>Ok</b> .
<b>Trigger source</b>	Select a source that triggered the file transaction from the following options:
<b>User</b>	This option filters the transactions initiated by a user or group of users.  You can specify the following additional filters:

Field	Description
	<ul style="list-style-type: none"> <li data-bbox="873 260 1482 363">■ <b>Partner:</b> Select either <b>All partners</b> or <b>Specific partner</b>, type the partner name in the box, and click <b>Ok</b>.</li> <li data-bbox="873 390 1482 493">■ <b>User:</b> Select either <b>All users</b> or <b>Specific user</b>, type the user name in the box, and click <b>Ok</b>.</li> <li data-bbox="873 520 1482 590">■ <b>Operation:</b> Select <b>All</b>, <b>Upload</b>, or <b>Download</b> based on transaction type.</li> <li data-bbox="873 617 1482 825">■ <b>Protocols:</b> Select one or more transmission protocols. You can select <b>All</b>, <b>All secure protocols</b> (FTPS, SFTP, HTTPS, SCP, and WebDAVs), <b>Non-secure protocols</b> (HTTP, FTP, and WebDAV), or individual protocols.</li> </ul>
<b>Action</b>	<p data-bbox="873 852 1482 888">You can specify the following additional filters:</p> <ul style="list-style-type: none"> <li data-bbox="873 915 1482 1018">■ <b>Source location:</b> Use this option to query the files which match the transactions from a particular source.   <p data-bbox="922 1045 1482 1148">You can either specify the partial or complete source location, which can include protocols as well.</p> <p data-bbox="922 1176 1482 1278">The source location will have the following format: <code>&lt;protocol&gt;://&lt;source location&gt;/&lt;filename&gt;</code>.</p> <p data-bbox="922 1306 1482 1444">Example, for FTP protocol, the source location can be, <code>FTP://dcmft01.eur.ad.sag:2121/var/www/ftp/ftpuser/test1/ATG_10.0.xml</code>.</p> </li> <li data-bbox="873 1472 1482 1575">■ <b>Destination location:</b> Use this option to query the files which match the transactions from a particular destination.   <p data-bbox="922 1602 1482 1705">You can either specify the partial or complete destination location, which can include protocols as well.</p> <p data-bbox="922 1732 1482 1835">The destination location will have the following format: <code>&lt;protocol&gt;://&lt;destination location&gt;/&lt;filename&gt;</code>.</p> </li> </ul>

Field	Description
	Example, for SFTP protocol, the destination location can be, SFTP:// dcmft01.eur.ad.sag:2121/var/www/sftp/ sftpuser/test1/ATG_10.0.xml.
<b>Agent</b>	You can select this option to display the <b>Agent</b> related file transactions.
<b>Trading Networks</b>	You can select this option to display the <b>Trading Networks</b> related file transactions.
<b>Status</b>	Select an option to display <b>All</b> , <b>Success</b> , or <b>Failed</b> transactions from the list.
<b>Transaction Comment</b>	Type the text to search for the <b>Comment</b> and <b>Activities</b> related information.
<b>Transaction ID</b>	Type the transaction ID of the file transfer.
<b>File name</b>	Type either the partial or complete name of the file based on which you want to search for transactions that match the specified file name. Select the <b>Match complete file name</b> option if you want to search for a file with the exact name that you specify.  <b>Match complete file name</b> performs the query faster when you have large volumes of data that can utilize the underlying database optimization.

- Click **Reset** and **Apply** for the changes to take effect.

In the **Comment** text box, you can modify the message that appears for the result of the file transaction.

In the results list, click the record you want to view the details for.

You can view the following information in the **Transaction details** section:

- **Transaction ID:** Transaction ID for the file transfer.
- **Transfer date and time:** Start time of the transfer.
- **Elapsed time:** Time elapsed since start time of the file transfer.
- **File size:** Size of the file.
- **User:** Name of the user initiating the file transfer.
- **Client IP Address:** IP address of the computer where the file transfer was initiated.
- **Protocol:** Protocol used for the file transfer.
- **Port name:** Name of the port used during the file transfer.

- **Transfer status:** Whether the transfer was successful or unsuccessful.
- **Source file:** The file that is transferred from the source.
- **Source location:** The location of file that is located in the source.
- **Trigger source:** Source of the file transaction. Could be a **User** or an **Action**.
- **Destination file:** The file that is transferred to the destination.
- **Destination location:** The location of file that is located in the destination.

You can view the following information in the **Activities** section:

- **Timestamp:** Date and time of the associated activity.
- **Transaction type:** Whether the file transaction is an upload or download operation.
- **Status:** Whether the transfer is successful or unsuccessful.
- **Action name:** Name of the action in ActiveTransfer Server.
- **Result:** The message for the outcome of the file transaction.
- **Details:** The details for the outcome of the file transaction.

## Viewing the Action Log

You can view the action execution details for post-processing and scheduled actions on your ActiveTransfer Server. By default, the search list is populated with the action execution details of the current day. You can further filter the action log based on criteria such as date and time, action type, action execution status, and file name.

### > To view an action log

1. On the navigation pane, select **Logs > Action log**.
2. On the Action log page, you can filter the log based on the following criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range with a time range in the HH:MM:SS (12-hour clock) format, and click <b>Ok</b> .
<b>Action type</b>	Select one of the following options: <ul style="list-style-type: none"> <li>■ <b>All:</b> Select this option to display all the post-processing and scheduled actions.</li> <li>■ <b>Post-Processing action:</b> Select this option, and select either <b>All actions</b> or <b>Specific action</b> and type the name of a particular post-processing action.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Scheduled action:</b> Select this option, and select either <b>All actions</b> or <b>Specific action</b> and type the name of a particular scheduled action.</li> <li>■ <b>Monitor folder action:</b> Select this option, and select either <b>All actions</b> or <b>Specific action</b> and type the name of a particular monitor folder action.</li> </ul>
<b>Status</b>	Select an option to display <b>All</b> , <b>Success</b> , <b>Failed</b> , or <b>In Progress</b> action executions from the list.
<b>File name</b>	Type either the partial or complete name of the file based on which you want to search for actions that match the specified file name. Select the <b>Match complete file name</b> option if you want to search for a file with the exact name that you specify.  <b>Match complete file name</b> performs the query faster when you have large volumes of data that can utilize the underlying database optimization.

3. Click **Reset** and **Apply** for the changes to take effect.

The activity logs retrieved appear in the results list.

4. If you want to view the details of a particular log, click the log ID.

You can view the following information in the **Action details** section:

- **Timestamp:** Date and time of the associated activity.
- **Task type:** The action type, post-processing or scheduled action.
- **Status:** Whether the action was successful or unsuccessful.
- **Message:** Actual activity executed during the file transaction.
- **Details:** Full list of the parameters and their values that were applied to the file transaction activity.
- **File seq no.:** The sequence in which the files are processed.

All files in an action are assigned a **File Seq No.** starting from zero when ActiveTransfer picks them up sequentially for the first task. Even after parallel processing starts, for all subsequent tasks, ActiveTransfer maintains the initial sequence number on each thread until the action execution is complete.

## Rerun a Post-Processing Action

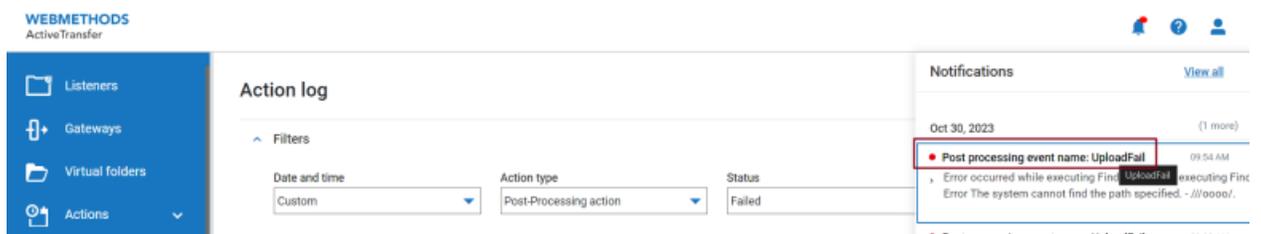
You can trigger a post-processing action when you upload, download or delete a file in ActiveTransfer Server. However, post-processing actions can sometimes fail due to situations such as network errors.

➤ **To rerun a failed post-processing action**

1. Click the **Notifications** icon. The notifications list provides you with the previous seven days of failed post-processing actions. ActiveTransfer Server only supports rerun of the last seven days of failed post-processing actions.

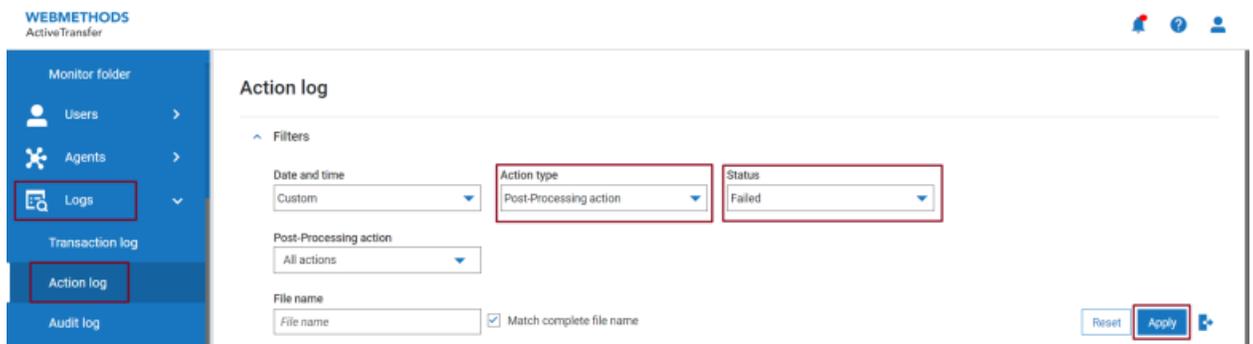


2. Click on your failed post-processing action in the notifications list.



3. If your action is not listed, go to **Logs > Action log**, and apply the following filters:

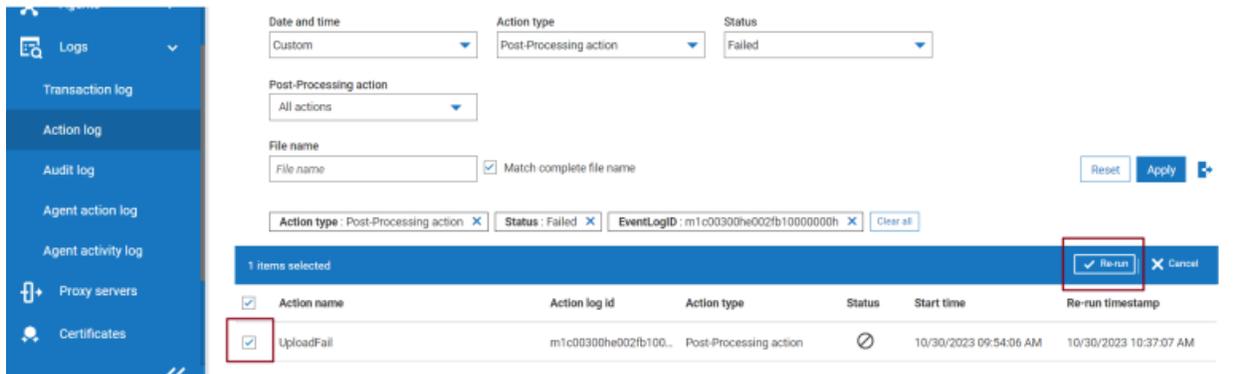
- Action type: **Post-Processing action**
- Status: **Failed**



Checkbox selection is enabled only if the above filters are applied. Default action log listing does not provide you with the rerun option.

4. Select your **Post-Processing action**, and click **Re-run**. You can select multiple post-processing actions for rerun, when the above filter is applied. To know the status of your rerun, click **Apply** again on the **Action log** filter after allowing the action the stipulated amount of time

for a rerun.



**Next Steps:**

- **Re-run timestamp** provides you with the latest instance of a given post-processing action's re-run. If the rerun succeeds, the post-processing action does not list anymore under the **Failed** status filter, or under the **Notifications** list. You need to clear the filters to view a successful rerun.

<input type="checkbox"/>	Action name	Action log id	Action type	Status	Start time	Re-run timestamp
<input type="checkbox"/>	UploadFail	m1c00300he002fb100...	Post-Processing action	Failed	10/30/2023 09:54:06 AM	10/30/2023 10:56:40 AM

- ActiveTransfer Server only supports rerun of the last seven days of failed post-processing actions.
- Rerun of post processing actions is not allowed for successful actions, first-time actions, and after rerun.
- The action execution starts from the first action. For example, if an action acts on a file that is uploaded, the file needs to be present in the location.
- Everytime you rerun a failed action, a new **Reexecuting** entry is added in the activity log. Click **Apply** again on the **Action log** filter, to view the latest status of the activity log.

Timestamp	Task type	Status	Message	Details	File seq no
11/06/2023 05:56:16 AM	Find	Failed	Executing action 'Find'.	Finding file(s) in File Path, URL:FILE Filename Filter = * Aborting Find, error = Error executing Find. Error The system cannot find the path specified. - Action failed : Error executing Find. Error The system cannot find the path specified.	0
11/06/2023 05:56:23 AM		Success	Reexecuting	Reexecuting the Post processing action.	0
11/06/2023 05:56:23 AM	Find	Failed	Executing action 'Find'.	Finding file(s) in File Path, URL:FILE Filename Filter = * Aborting Find, error = Error executing Find. Error The system cannot find the path specified. - Action failed : Error executing Find. Error The system cannot find the path specified.	0

## Viewing the Audit Log

You can view the updates to assets on your ActiveTransfer Server. By default, the search list is populated with the asset details of the current day. You can further filter the audit log based on criteria such as date and time, operation, asset type, asset name, asset ID, search text, and user.

### Note:

When an asset is saved without making any changes to it, an entry stating that no changes are made is added to the audit log.

### > To view an audit log

1. On the navigation pane, select **Logs > Audit log**.
2. On the Audit log page, you can filter the log based on the following criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range with a time range in the HH:MM:SS (12-hour clock) format, and click <b>Ok</b> .
<b>Operation</b>	Select <b>All</b> , <b>Created</b> , <b>Updated</b> , or <b>Deleted</b> to display all, created, updated, or deleted assets respectively from the list.
<b>Asset</b>	Select <b>All</b> or one of the asset from the list.
<b>Asset name</b>	Type the name of the asset for the asset selected under <b>Asset type</b> .
<b>Asset ID</b>	Type the ID of the asset for the asset selected under <b>Asset type</b> .
<b>Search text</b>	Type the text based on which you want to search for assets.
<b>User</b>	Select either <b>All users</b> or <b>Specific user</b> , type the user name in the box, and click <b>Ok</b> .

3. Click **Reset** and **Apply** for the changes to take effect.

In the results list, click the record you want to view the details for.

You can view the following information in the **Summary** section:

- **ID:** ID of the asset that is updated.
- **Asset:** Type of the asset that is updated. For example, scheduled action, user, virtual folder, and so on.
- **Timestamp:** Date and time when the asset is updated.
- **User:** System user who updated the asset. For example, administrator.

- **Action:** Type of asset modification. For example, created, updated, deleted, and so on.
- **Brief message:** Brief information about the update to the asset.

You can view the following information in the **Details** section:

- **Field:** Property of the asset that is updated.
- **New value:** New value of the property.
- **Old value:** Old value of the property.

## Viewing the Analytical Details

---

ActiveTransfer data sources contain analytical data. Software AG MashZone Server connects to the appropriate data sources, retrieves the data to create the analytical details, and displays this information on the Analytics page. If you want to view analytical details other than those that ActiveTransfer provides, contact your Software AG sales representative.

For information about setting up the MashZone NextGen environment to display dashboards in ActiveTransfer, see [Windows Deployment](#).

### Note:

Analytical details are available only in English. However, Software AG MashZone supports the localization of these details. For more information, see the MashZone NextGen documentation.

ActiveTransfer Server offers a variety of analytical details such as transfer volume, rates, and other metrics:

- The ActiveTransfer transfer analysis details display file transfer volume trends and summary, details about all successful and failed file transfers, and details about the top 10 largest files.
- The ActiveTransfer transfer rate details display the average transfer rate by partners (number of files and MB per second) and the average file size by partners.
- The ActiveTransfer “Top 10 Metrics” details include the top 10 largest files, top 10 partners by file volume, and top 10 busiest servers.

You can view the activities within your environment using the ActiveTransfer analytics dashboard. The dashboard provides insight into all the file transfers that happen within your environment by displaying metrics, making comparisons, and summarizing key activities.

### > To view analytical details

1. On the navigation pane, select **Logs > Analytics**.
2. On the Analytics page, expand **Search**. You can filter the dashboard based on the following criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range, and click <b>Ok</b> .
<b>Operation</b>	Select <b>All</b> , <b>Upload</b> , or <b>Download</b> option based on transaction type
<b>Status</b>	Select whether to show <b>All</b> , <b>Success</b> , or <b>Failed</b> actions.
<b>Sender</b>	Select either <b>All partners</b> or <b>Specific partner</b> , type the partner name in the box, and click <b>Ok</b> .
<b>Receiver</b>	Select either <b>All partners</b> or <b>Specific partner</b> , type the partner name in the box, and click <b>Ok</b> .
<b>User</b>	Select either <b>All users</b> or <b>Specific user</b> , type the user name in the box, and click <b>Ok</b> .
<b>Protocols</b>	Select one or more transmission protocols. You can select <b>All</b> , <b>All secure protocols</b> (FTPS, SFTP, HTTPS, SCP, and WebDAVs), <b>All non-secure protocols</b> (HTTP, FTP, and WebDAV), or individual protocols.

3. Click **Reset** and **Apply** for the changes to take effect.

The dashboard based on the criteria that you selected appear.

**Note:**

Configure the **mft.ui.security.csp.allowed.resources** property with the Mashzone URL(s) you want to include in the Analytics dashboard.

Provide multiple URLs separated by commas in the following format:

```
mft.ui.security.csp.allowed.resources = <Mashzone URL1>, <Mashzone URL2>
```

## Viewing the Agent Action Log

View the execution details for agent actions on ActiveTransfer Server. By default, the search list is populated with the agent action execution details of the current day. You can further filter the agent action log based on criteria such as date and time, agent action execution status, and agent action name.

### ➤ To view an agent action log

1. In the navigation pane, select **Logs > Agent action log**.
2. Filter the log based on the following criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range with a time range in the HH:MM:SS (12-hour clock) format, and click <b>Ok</b> .
<b>Status</b>	Select an agent action execution status from the list: <ul style="list-style-type: none"> <li>■ <b>All</b>: All the agent action executions.</li> <li>■ <b>Success</b>: Agent action executions that are successful.</li> <li>■ <b>Completed with error</b>: Agent action executions that are completed with errors.</li> <li>■ <b>In progress</b>: Agent action executions that are in progress.</li> <li>■ <b>Not started</b>: Agent action executions that are not triggered.</li> <li>■ <b>Failed</b>: Agent action executions that have failed.</li> </ul>
<b>Agent action name</b>	<ol style="list-style-type: none"> <li>a. Select either <b>All agent actions</b> or <b>Specific agent action</b>.</li> <li>b. Type the agent action name in the box.</li> <li>c. Click <b>Ok</b>.</li> </ol>

3. Click **Reset** and **Apply** for the changes to take effect.

The results list is populated with the following information:

- **Agent action name**: Name of the agent action.
- **Status**: Status of the agent action execution.
- **Start time**: Start time of the agent action execution.
- **End time**: End time of the agent action execution.
- **Agent action log ID**: Log ID of the agent action. The log ID is used in debugging failed agent actions to map the log ID of the agent action with specific actions of agents in the activity log or associate the log ID agent action with log files.

**Tip:**

Clicking on any record in the results list will navigate you to the respective agent action's details page.

## Viewing the Agent Activity Log

View the activity details for agent actions on ActiveTransfer Server. By default, the search list is populated with the agent action activity details of the current day. You can further filter the agent activity log based on criteria such as date and time, activity type, status, agent name, agent action name, and file name.

➤ To view an activity log for agent actions

1. In the navigation pane, select **Logs > Agent activity log**.
2. Filter the activity log for agent actions based on the following criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range with a time range in the HH:MM:SS (12-hour clock) format, and click <b>Ok</b> .
<b>Activity type</b>	Select an activity type from the list: <ul style="list-style-type: none"> <li>■ <b>All</b>: All the activities of the agent actions.</li> <li>■ <b>Agent action download</b>: Agent action download of assets (agent configuration details, agent actions, agent group details) from ActiveTransfer Server.</li> <li>■ <b>Agent action execution</b>: Agent action executions.</li> <li>■ <b>Authentication</b>: Agent authentication logs when connecting to ActiveTransfer Server.</li> <li>■ <b>Action config error</b>: Agent action configuration error.</li> </ul>
<b>Status</b>	Select an activity type status for agent or agent action executions from the list: <ul style="list-style-type: none"> <li>■ <b>All</b>: All the activities of the agent actions.</li> <li>■ <b>Success</b>: Activities of agent actions that are successful.</li> <li>■ <b>Completed with error</b>: Activities of agent actions that are completed with errors.</li> <li>■ <b>In progress</b>: Activities of agent actions that are in progress.</li> <li>■ <b>Not started</b>: Activities of agent actions that are not triggered.</li> <li>■ <b>In queue</b>: Activities of agent actions that are in the queue.</li> <li>■ <b>Failed</b>: Activities of agent actions that have failed.</li> </ul>
<b>Agent name</b>	<ol style="list-style-type: none"> <li>a. Select either <b>All agents</b> or <b>Specific agent</b>.</li> <li>b. Type the agent name in the box.</li> <li>c. Click <b>Ok</b>.</li> </ol>
<b>Agent action name</b>	<ol style="list-style-type: none"> <li>a. Select either <b>All agent actions</b> or <b>Specific agent action</b>.</li> <li>b. Type the agent action name in the box.</li> </ol>

Field	Description
	c. Click <b>Ok</b> .
<b>File name</b>	Type either the partial or complete name of the file to search for agents or agent actions that match the specified file name.  Select the <b>Match complete file name</b> option if you want to search for a file with the exact name that you specify. <b>Match complete file name</b> performs the query faster when you have large volumes of data that can utilize the underlying database optimization.

3. Click **Reset** and **Apply** for the changes to take effect.

The results list displays the following information:

- **Agent name:** Name of the agent.
- **Agent action name:** Name of the agent action.
- **Activity type:** Activity of agent action based on assets downloaded, agent actions executed, agents authenticated, or all.
- **Start time:** Start time of the agent action activity.
- **Status:** Status of the agent action activity.
- **End time:** End time of the agent action activity.
- **Agent URL:** Host name of the agent or the SPM URL on the agent host.
- **Trigger source:** Source from where the agent activity is triggered.
- **Node alias:** Alias for the agent instance.
- **Node ID:** Agent ID generated during installation.
- **Scheduled time:** Scheduled time for the agent activity when the agent action execution status is *Not Started*.

This is the time when the agent action is scheduled for execution. However, the start time might be different from the scheduled time either because the agent action did not receive an approval for execution during the scheduled time or the agent is down during the scheduled time.

#### Tip:

Clicking on any record in the results list will navigate you to the respective agent's details page.

## Downloading Log Data

You might want to share audit data, agent log data, file transaction data, scheduled action details or post-processing action details with management personnel, business analysts or other members

of your organization. ActiveTransfer enables you to export any log data available on ActiveTransfer Server to a CSV file and save it.

By default, you can download the data for 1000 logs in a single download action. If you want to modify this number, you can do so by using the `mft.query.maxrows` parameter in the `properties.cnf` file. You can also provide a filter criteria to download the logs.

For details on the `mft.query.maxrows` parameter, see . [“Server Configuration Parameters and Variables” on page 221.](#)

### ➤ To download log data to a CSV file

1. In the navigation pane, select the required log.

For example, **Action Log**.

2. On the log page, select the required filter criteria.

3. Do one of the following to export and download the logs:

- Click  to export all available logs to a single CSV file.
- If you only want to download the details of a particular activity log, click the log ID and click .

**Note:**

Only **Action Log** lets you to download the details of a particular activity log .

ActiveTransfer downloads all the logs with the file name as follows:

Log details format for..	File name
Any log	<i>LogPageName_YYYYMMDDHHMMSS.csv</i> . For example, TransactionLog_20191006123351.csv, AuditLog_202002201121.csv.
Action activity log	<i>ActivityLogPageNameDetails_YYYYMMDDHHMMSS.csv</i> . For example, ActionLogDetails_20200123091101.csv.



# 10 Managing Proxy Servers

■ Overview .....	168
■ Proxy Server Alias Usage Scenarios .....	168
■ Adding Proxy Servers .....	170

## Overview

If you have installed ActiveTransfer behind a firewall, you might need proxy servers in order to connect to external remote servers outside the firewall. ActiveTransfer provides support for HTTP, HTTPS, and SOCKS proxy servers for protocols that support these proxy server types.

File transfers through proxy servers to remote servers require proxy server aliases set up either in Integration Server or ActiveTransfer. The file transfer protocols, supported proxy server types, and supported ActiveTransfer proxy server alias types are:

File Transfer Protocol	Supported Proxy Server Type	ActiveTransfer Proxy Server Alias Type
FTP	SOCKS	SOCKS
SFTP	<ul style="list-style-type: none"> <li>■ HTTPS</li> <li>■ SOCKS</li> </ul>	<ul style="list-style-type: none"> <li>■ HTTPS</li> <li>■ SOCKS</li> </ul>
HTTP	<ul style="list-style-type: none"> <li>■ HTTP</li> <li>■ SOCKS</li> </ul>	<ul style="list-style-type: none"> <li>■ HTTP</li> <li>■ SOCKS</li> </ul>
HTTPS	<ul style="list-style-type: none"> <li>■ HTTPS</li> <li>■ SOCKS</li> </ul>	<ul style="list-style-type: none"> <li>■ HTTPS</li> <li>■ SOCKS</li> </ul>
WebDAV	SOCKS	SOCKS
WebDAVs	SOCKS	SOCKS

Each time you add, modify, or delete proxy server aliases in the Proxy server page, ActiveTransfer shares the changes with Integration Server. These changes appear in the **Integration Server Administrator > Settings > Proxy Servers** page. Similarly, Integration Server shares proxy server aliases set up in Integration Server with ActiveTransfer. In ActiveTransfer, you can configure virtual folders and actions with tasks to use proxy servers while connecting to remote servers. For information on how to set up proxy server aliases in Integration Server, see *webMethods Integration Server Administrator's Guide*.

The details of file transactions using proxy server aliases are available in the Transaction log and Action log pages.

### Note:

The proxy server settings are specific to one instance of ActiveTransfer or Integration Server. If there are multiple ActiveTransfer instances as part of an ActiveTransfer group, then this setup must to be configured for all ActiveTransfer instances.

## Proxy Server Alias Usage Scenarios

ActiveTransfer supports proxy server alias in the following two scenarios:

- When you configure a virtual folder that points to an external remote server. The connection to the remote server is routed through the proxy server alias specified in the virtual folder configuration.
- When you configure a task for an action that requires a connection to an external remote server.

In both these scenarios, you can either configure the virtual folder or task for an action to use a specific proxy server alias or use the default proxy server alias setup in ActiveTransfer or Integration Server. For information on default proxy server aliases in Integration Server, see *webMethods Integration Server Administrator's Guide*.

Parameter location	Parameter name	Description
ActiveTransfer	<code>mft.client.outbound.useProxy</code>	<p>Set this parameter in <i>Integration Server_directory \ instances\instance_name \ packages\WmMFT\ config\properties.cnf</i>.</p> <p>The parameter determines if proxy server settings are enabled in ActiveTransfer.</p> <ul style="list-style-type: none"> <li>■ <i>true</i>: ActiveTransfer uses the proxy server configured and based on the value set for <code>watt.net.proxy.fallbackToDirectConnection</code>, ActiveTransfer connects to the remote server without using the proxy server or result in a failed connection.</li> <li>■ <i>false</i>: ActiveTransfer does not use the proxy server even if it is configured.</li> </ul>
Integration Server	<code>watt.net.proxy.fallbackToDirectConnection</code>	<p>Set this parameter in <i>Integration Server_directory \ instances\instance_name\config directory\cnfserver.cnf</i>.</p> <p>The parameter determines how ActiveTransfer handles connections through proxy servers:</p> <ul style="list-style-type: none"> <li>■ <i>true</i>: ActiveTransfer establishes a direct connection to the remote server when ActiveTransfer is not able to connect to the remote server through the proxy server.</li> <li>■ <i>false</i>: ActiveTransfer treats the connection attempt as failed.</li> </ul>
Integration Server	<code>watt.net.proxySkipList</code>	<p>Set this parameter in <i>Integration Server_directory \</i></p>

Parameter location	Parameter name	Description
		<p><code>instances\instance_name\config directory\cnfserver.cnf.</code></p> <p>If the IP address of the remote server is in this list, ActiveTransfer ignores the proxy server alias and connects directly to the remote server.</p>
Integration Server	<code>watt.net.proxy.useNonDefaultProxies</code>	<p>Set this parameter in <code>Integration Server_directory \ instances\instance_name\config directory\cnfserver.cnf.</code></p> <p>The parameter determines how ActiveTransfer must handle the absence of default proxy sever aliases.</p> <ul style="list-style-type: none"> <li>■ <i>true</i>: ActiveTransfer selects any proxy server alias enabled for the protocol.</li> <li>■ <i>false</i>: ActiveTransfer treats the connection attempt as failed.</li> </ul>

For information about the parameters, see *webMethods Integration Server Administrator's Guide*.

## Adding Proxy Servers

You can add proxy server aliases for file transfers to remote servers through proxy servers using the quick add feature. The proxy server alias you add here also appears in Integration Server Administrator > **Settings** > **Proxy Servers**.

1. On the navigation pane, select **Proxy servers**.
2. On the Proxy servers page, click .
3. In the Add proxy server dialog box, specify the following details:

Field	Description
<b>Alias</b>	Type a suitable name for the proxy server alias. The maximum limit is 50 characters.
<b>Protocol</b>	Select one of the following supported file transfer protocol to which this proxy server alias applies: <ul style="list-style-type: none"> <li>■ <b>HTTP</b></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>HTTPS</b></li> <li>■ <b>SOCKS</b></li> </ul>
<b>Host</b>	Type the host IP address of the proxy server.
<b>Port</b>	Type the port number of the proxy server to use.

- Click **Add**.

The new proxy server appears in the proxy servers list.

- Click on any proxy server to configure the following additional settings:

Field	Description
<b>Alias</b>	Modify the proxy server alias if required.
<b>Default</b>	Select this option if you want ActiveTransfer to use this alias as the default proxy server alias for the particular file transfer protocol.  <b>Note:</b> You can designate only one proxy server alias as the default proxy server alias for a particular file transfer protocol.
<b>Enabled</b>	Select this option to enable the proxy server alias.
<b>Protocol</b>	Select one of the following supported file transfer protocol to which this proxy server alias applies: <ul style="list-style-type: none"> <li>■ <b>HTTP</b></li> <li>■ <b>HTTPS</b></li> <li>■ <b>SOCKS</b> <ul style="list-style-type: none"> <li>■ <b>SOCKS v4</b></li> <li>■ <b>SOCKS v5</b></li> </ul> </li> </ul>
<b>Host</b>	Modify the host IP address of the proxy server, if required.
<b>Port</b>	Modify the port number of the proxy server to use, if required.
<b>User name</b>	Type the user name to connect to the proxy server.  <b>Note:</b> If you selected <b>SOCKS v4</b> for <b>Protocol</b> , you do not need to specify the user name and password.

Field	Description
<b>Password</b>	Type the password to connect to the proxy server.

---

6. Click **Save**.

The proxy server is updated with the additional settings.

# 11 Managing Certificates

■ Overview .....	174
■ Adding Certificates .....	174

## Overview

A digital certificate is an electronic password that allows you to securely exchange documents. In addition to exchanging of documents, certificates also lets you to identify the interaction between a user to user, a user to a machine, and a machine to another machine .

webMethods ActiveTransfer Server uses SSL certificate to communicate between ActiveTransfer Server and ActiveTransfer Gateway.

ActiveTransfer Server allows you to use the user-certificate mapping to validate a client login based on the client certificate, and to fetch the user details associated with the certificate.

### Important:

In ActiveTransfer versions 10.7 and lower, you must configure the certificate path in the asset configuration. Now, ActiveTransfer supports a new way of configuring certificates in assets such as events, listeners, and virtual folders. You must now associate the certificate with an asset using the certificate alias of the respective certificate.

For more information on configuring certificates, refer to the respective asset configuration sections.

## Adding Certificates

You add and view the certificates using ActiveTransfer.

### > To add a certificate

1. On the navigation pane, select **Certificates**.
2. On the Certificates page, click  **+ Add**.
3. In the Add certificate dialog box, specify the following details:

Field	Action/Description
<b>Certificate alias</b>	Type the certificate alias associated with ActiveTransfer Server. It must be a unique alias within ActiveTransfer Server.
<b>Certificate usage</b>	Click this option to check if the added certificate is used in any location in ActiveTransfer Server.
	<p><b>Note:</b> The button remains in the disabled state until you add and save a particular certificate.</p> <p><b>Note:</b></p>

Field	Action/Description
	The default certificates will not show any usage. However, it can be referenced in multiple MFT assets explicitly.
<b>Description</b>	Type a suitable description for the certificate you choose. The maximum limit is 1024 characters.
<b>Certificate type</b>	Select one of the following supported certificate by ActiveTransfer Server: <ul style="list-style-type: none"> <li>■ Keystore</li> <li>■ Truststore</li> <li>■ PGP Public Key</li> <li>■ PGP Private Key</li> <li>■ SSH Private Key</li> <li>■ SSH Public Key</li> </ul>
<b>Keystore password</b>	Type the password that protects the Keystore. This password is required to access the certificate in the Keystore file for ActiveTransfer Server.
<b>Key password</b>	Type the password associated with the certificate.
<b>Location</b>	Provide the location of the certificate from one of the following options: <ul style="list-style-type: none"> <li>■ Database</li> <li>■ File</li> </ul>
<b>Upload Certificate</b>	Copy the certificate from a location by either performing a drag-and-drop action or browsing to a particular location.

4. Click **Add** to save the changes.

**Note:**

- You can delete a certificate only after removing its references from all other assets.
- If a certificate is added by ActiveTransfer Server as a default host key, then the particular certificate cannot be deleted.
- To configure certificates, use the ActiveTransfer new user interface.



# 12 Managing ActiveTransfer Settings

■ Overview .....	178
■ Features in ActiveTransfer Global Settings .....	178
■ Configuring Listener Preferences .....	180
■ Acceleration .....	185
■ Configuring Audit Settings .....	188
■ Configuring File Share Settings .....	188
■ Configuring Server Properties .....	190
■ Configuring ActiveTransfer to Send Emails .....	191
■ Configuring Password Complexity for Users .....	194

## Overview

---

You can configure the following global settings in ActiveTransfer.

## Features in ActiveTransfer Global Settings

---

This topic provides information about specific features you can use to configure global settings for ActiveTransfer:

### Throttling

Throttling enables you to control the speed of file transfers. By imposing such a restriction on bandwidth, you help prevent a situation where your organization's entire bandwidth is used for file transfers. You can specify the following options:

- Maximum number of client connections that can be made to ActiveTransfer Server at any given time.
- Maximum outgoing and incoming speeds allowed across all listeners for an ActiveTransfer instance.
- IP patterns that define a range of IP addresses that are immune to the speed settings.

### Restrictions for Files

You can restrict particular operations for files that match a specified pattern. You can set the following server restrictions:

- Restrict server availability to specified days of the week.
- Restrict particular actions for files that match a specified pattern. For example, you can restrict users from uploading files that end with `.exe`.
- Restrict access to subfolders in a folder system that match a specified pattern.

### Hammering

At times, applications might attempt to access your ActiveTransfer Server or ActiveTransfer Gateway through a rapid succession of login attempts, a technique sometimes referred to as *hammering*. This can consume significant bandwidth and processing time, resulting in the denial of connection requests from other users.

**Note:**

Apply the settings to ActiveTransfer Server only in the absence of a Gateway instance. If you have an ActiveTransfer Server and a Gateway instance, apply the settings to the Gateway.

You can use the hammering settings to do the following:

- Set limits on the number of connection, password, or command execution attempts and the interval between them. Then, ban the user's IP address for a specified number of minutes when the defined limits are reached.
- Ban the IP address associated with a user after the user's first incorrect password attempt, either permanently or for a specified number of minutes.
- Block efforts to discover valid user credentials by holding the names of invalid users in the cache for a specified number of seconds.
- Discourage hack attempts by robots that scan for writable directories on the server by slowing down responses to such clients.

**Note:**

If the hammering settings are too restrictive, they can prevent users and applications from connecting to ActiveTransfer Server or ActiveTransfer Gateway to exchange files or perform file operations under normal operating conditions.

When the specified time interval elapses, ActiveTransfer Server and ActiveTransfer Gateway automatically lift the ban on IP addresses. You can also free banned IP addresses before the specified time interval by using the Integration Server service `wm.mft.server:unbanIPs`. For details on the `wm.mft.server:unbanIPs` service, see *webMethods ActiveTransfer Built-In Services Reference*.

**Restrictions for IP Addresses**

You can allow or deny a range of IP addresses for selective access to ActiveTransfer Server or ActiveTransfer Gateway. The default range is 0-255, which indicates that ActiveTransfer Server or ActiveTransfer Gateway allows all IP addresses to access the server and Gateway, respectively.

**Note:**

The IP version supported is IPv4.

**SSL Ciphers**

Ciphers are algorithms that are used to encrypt or decrypt data. You can specify the SSL ciphers that ActiveTransfer will apply to all SSL listeners associated with a server instance.

**File-based Encryption and Decryption**

File-based encryption and decryption enables you to encrypt files before you store them on your drive. Encrypted files are decrypted when they are transferred back through ActiveTransfer using the same key that was used to encrypt them.

ActiveTransfer Server encrypts and decrypts files instream rather than after the file is fully transferred.

When encryption and decryption keys are configured at multiple levels (user, server, and folder), ActiveTransfer enforces the following order of preference:

1. Users

2. Folders
3. Servers

For example, if user *A* accesses port *10* and uploads a file in a VFS *MN*, then ActiveTransfer checks if the encryption or decryption key is available for user *A*. If no key is available at the user level, then ActiveTransfer checks for the folder settings for a key. If no key is present at the VFS level, then ActiveTransfer checks the server level settings for the key.

## Configuring Listener Preferences

You can configure global settings for all listeners. These settings are applicable for all listeners associated with both, ActiveTransfer Server and Gateway instances.

1. In ActiveTransfer, go to **Settings > Listener preferences**.
2. On the **Listener preferences** page, from the **Instance** list, select ActiveTransfer Server or an ActiveTransfer Gateway instance.
3. You can specify the following settings:

Field	Description
<b>Throttling</b>	
<b>Maximum simultaneous user connections</b>	Type the maximum number of client connections allowed for the server at any given time.
<b>Maximum outgoing speed (Kb/sec)</b>	Type the maximum allowable speed in kilobytes per second for outbound transfers across all listeners.
<b>Maximum incoming speed (Kb/sec)</b>	Type the maximum allowable speed in kilobytes per second for inbound transfers across all listeners.
<b>IP patterns immune to speed</b>	Click  to add one or more IP patterns representing a range of IP addresses. For example, 168.21.* indicates that all addresses that begin with 168.21 are immune to speed settings.
<b>Active time window</b>	Select the days of a week you want the server to be available to the user.
<b>File name filters</b>	
<b>Patterns</b>	Click  to add one or more patterns to restrict particular operation for certain files, and specify the following details: <ul style="list-style-type: none"> <li>■ <b>Command.</b> Select a operation to restrict (<b>List</b>, <b>Upload</b>, <b>Download</b> or <b>Rename</b>) from the list.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Filter type.</b> Select a filter type (<b>Starts with</b>, <b>Ends with</b>, or <b>Contains</b>) from the list.</li> <li>■ <b>File name.</b> Type a portion of the file name that the <b>Filter type</b> criterion should evaluate (for example, "exe").</li> </ul> <p><b>Note:</b> Wildcard characters and regular expressions are not supported. That is, you cannot use characters such as * or % to represent any sequence of characters. ActiveTransfer Server treats those characters as part of the file name.</p>
<b>Block paths matching these patterns</b>	<p>Click  to restrict access to specific folders and subfolders in the file system, and specify the following:</p> <ul style="list-style-type: none"> <li>■ <b>Pattern:</b> Type the file system path you want to block. Regular expressions or wildcards characters are permitted.</li> </ul> <p><b>Tip:</b> Precede a pattern with a tilde character (~) to apply the pattern for all occurrences. For example, to deny user access to the folder /system/bin type: ~/system/bin/*</p>
<b>Hammering</b>	
<b>Ban IP address after unsuccessful attempts</b>	<p>Ban a user's IP address after a certain number of connection, password, or command execution attempts. Select the values for <b>Connection</b>, <b>Password</b>, and <b>Command</b> rows to configure the following settings:</p> <ul style="list-style-type: none"> <li>■ <b>Maximum attempts:</b> Type the maximum number of allowed attempts.</li> <li>■ <b>Max attempts within (sec):</b> Type the duration in seconds.</li> <li>■ <b>Ban duration (min):</b> Type the duration in minutes to ban the IP address.</li> </ul>
<b>Ban the IP addresses of users after the first incorrect password</b>	<p>Ban the IP address associated with a specific user after the user's first incorrect password attempt. Click  and type the user name for whom you want to ban the IP address. Repeat this step for other users whose IP address you want to ban.</p>
<b>Ban specified IP addresses</b>	<p>Do one of the following after adding the IP addresses associated with users after the first incorrect password attempt:</p> <ul style="list-style-type: none"> <li>■ Select <b>Permanently</b> to ban the user's IP address permanently.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>Select <b>Ban duration (min)</b> and type the duration in minutes to ban the user's IP address.</li> </ul>
<b>Cache invalid usernames for (sec)</b>	<p>Type the number of seconds to hold the name of invalid users in the cache temporarily.</p> <p>The temporary caching of invalid usernames is useful for blocking robots that make repeated attempts to discover valid user credentials. When a robot scans ActiveTransfer Server or ActiveTransfer Gateway during the user validation process, this option blocks subsequent login attempts made using an invalid username for the specified number of seconds. If the username is valid, the ActiveTransfer Server or ActiveTransfer Gateway ignores this setting.</p>
<b>Slow down hack attempt scans</b>	<p>Select this option to incrementally slow down responses to a client that appears to be a robot scanning for writable directories on your server by establishing an FTP connection.</p> <p>This setting doubles the response time of the server for each subsequent response to the client, thereby rendering such robots less effective. Selecting this option does not result in any extra load on the CPU.</p>
<b>IP restrictions</b>	<p>Click  to add one or more IP addresses for which ActiveTransfer Server can accept or deny connection requests and specify the following details:</p> <ul style="list-style-type: none"> <li>Select <b>Allow</b> or <b>Deny</b> from the list.</li> <li>Type the IP address range in the <b>From</b> and <b>To</b> boxes. For example, 160.30.*.</li> </ul>
<b>SSL</b>	
<b>Activate</b>	Select this option to activate SSL encryption.
<b>Keystore alias</b>	Browse the required certificate alias for keystore.
<b>Require valid client certificate</b>	<p>Select this option to block all connections from the client when the client does not have a valid client certificate key password.</p> <p><b>Note:</b> When this option is selected, ActiveTransfer Server expects the clients requesting a server connection to present a valid certificate. The certificate should match one of the certificates stored in the truststore. To store valid certificates, you must create a truststore file in the same location as the keystore file, with the name <i>keystoreName_trust</i>. For example, if the keystore file name is</p>

Field	Description
	server_ks.jks, the truststore name should be server_ks.jks_trust. You should add all the valid client certificates to this truststore.
<b>Require valid client certificate and password</b>	<p>Select this option to block all connections from the client when the client does not have a valid client certificate key and password.</p> <p><b>Note:</b> When this option is selected, ActiveTransfer Server expects the clients requesting a server connection to present a valid certificate. The certificate should match one of the certificates stored in the truststore. To store valid certificates, you must create a truststore file in the same location as the keystore file, with the name <i>keystoreName_trust</i>. For example, if the keystore file name is server_ks.jks, the truststore name should be server_ks.jks_trust. You should add all the valid client certificates to this truststore.</p>
<b>Enable advanced upload/download option in Web client</b>	Select this option to use the SSL keystore settings for file upload and download operations using acceleration.
<b>Prefer server cipher list order</b>	Select this option to provide preference to the order of server cipher list.
<b>Manage ciphers</b>	<p>Click  and select the required ciphers from the list.</p> <p>To list the ciphers in a particular order:</p> <p><b>Note:</b> Select the <b>Prefer cipher list order on server</b> option to force the order of the ciphers as listed on the server.</p> <ol style="list-style-type: none"> <li>Click .</li> <li>In the Order ciphers dialog box, select a cipher and do one of the following: <ul style="list-style-type: none"> <li>■ Click  to move the cipher up.</li> <li>■ Click  to move the cipher down.</li> </ul> </li> <li>Click <b>Ok</b>.</li> </ol> <p><b>Note:</b></p>

Field	Description
	If you reorder the ciphers for an SSL listener, then restart that respective SSL listener or all the SSL listeners for the change to take effect across all the SSL listeners.
<b>File-based encryption</b>	
<b>Activate</b>	Select this option to activate the file-based encryption.
<b>Public PGP key alias</b>	Type or browse the certificate alias for the public PGP key.
<b>File-based decryption</b>	
<b>Activate</b>	Select this option to activate the file-based decryption.
<b>Private PGP key alias</b>	Type or browse the certificate alias for the private PGP key.
<b>Protocol options</b>	
<b>Welcome message</b>	Type a welcome message for display in the client console (example, ActiveTransfer web client, FileZilla client, and so on) when a user logs in.
<b>Download in binary</b>	Select this option to download files only in binary mode. This prevents ActiveTransfer from altering the line endings of the ASCII text files even if the FTP client requests it.
<b>Upload in binary</b>	Select this option to upload files only in binary mode.
<b>Allow extended passive and port commands</b>	Select this option to allow extended passive and port commands such as, Extended Passive Mode (EPSV) and Extended Data Port (EPRT). This ensures compatibility between the client and server.  <b>Note:</b> Before you enable this option, ensure that your client supports these commands.
<b>Disable MTDM notifications</b>	Select this option to prevent the user from modifying the timestamp of when a file was uploaded.
<b>Delete partial uploads</b>	Select this option to delete any incomplete file uploads.
<b>ZIP compression level</b>	You can set the ZIP compression level according to your needs for file size and data transfer speed. Select one of the following options: <ul style="list-style-type: none"> <li>■ <b>None:</b> No compression. Results in the largest file size of the three options, with the longest transfer time.</li> <li>■ <b>Fast:</b> Fastest compression. Performs little compression, but compression time is the fastest of the three options.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Best:</b> Maximum compression. Provides the smallest file size possible after compression, with the shortest transfer time, but requires more time to perform the compression compared to the other two options.</li> </ul>
<b>Directory listing</b>	Select the <b>Use ls -la for destination directory listing (Mac OS X, UNIX, Linux)</b> option to configure ActiveTransfer to use the directory listing command <code>ls -la</code> to list the owner, group, and permission details of the destination directory when the operating system is Mac OS X, UNIX, or Linux.

**Note:**

If you reorder the ciphers for an SSL port, then restart that respective SSL port or all the SSL ports for the change to take effect across all the SSL ports.

4. Click **Save** to update the server instance with the global settings

## Acceleration

ActiveTransfer allows accelerated data transfer, referred to as *acceleration*. Through the use of tunnels, ActiveTransfer speeds up file transfers by using the server's full bandwidth regardless of network latency or distance.

You can configure tunnels by configuring basic settings, such as the tunnel name using the quick add feature. To configure additional settings for tunnels, see "[Configuring Additional Settings for a Tunnel](#)" on page 186.

The acceleration settings you specify in the following procedures will override any acceleration settings set for a template associated with a user. You can apply the same settings to roles and groups.

## Adding a Tunnel

You can add a tunnel to accelerate data transfer using the quick add feature. To configure additional settings for the tunnel, see "[Configuring Additional Settings for a Tunnel](#)" on page 186.

### > To add a tunnel

1. On the navigation pane, select **Settings > Acceleration**.
2. On the Acceleration page, click .
3. In the Add tunnel dialog box, type a **Tunnel name**.

4. Click **Add**.

The new tunnel is created and appears in the acceleration list.

## Configuring Additional Settings for a Tunnel

You can configure additional settings for a tunnel.

### > To configure additional settings

1. On the navigation pane, select **Settings > Acceleration**.
2. On the Acceleration page, click on the tunnel for which you want to configure additional settings.
3. You can specify the following details:

Field	Description
<b>Basic</b>	
<b>Tunnel name</b>	Type a unique name for the tunnel.
<b>Autostart tunnel when created</b>	Select this option if you want the tunnel to start as soon as it is ready without any user intervention.
<b>Server</b>	
<b>Server host</b>	The default host value for the destination server is 127.0.0.1. <b>Important:</b> Do not change this value.
<b>Port</b>	The default port value for the destination server is 55580. <b>Important:</b> Do not change this value.
<b>Client</b>	
<b>Local IP address</b>	The default host value for the destination server is 127.0.0.1. <b>Important:</b> Do not change this value.
<b>Port</b>	The default port value for the destination server is 55580.

Field	Description
	<b>Important:</b> Do not change this value.
<b>Reverse</b>	Select this option if you want to connect the tunnel to ActiveTransfer Server, create a tunnel back to your system, and then connect to a destination from there.
<b>Channels and Advanced</b>	
<b>Maximum no. of inbound channels</b>	Type the maximum number of inbound channels to use for file transfers. These values should correspond to the appropriate multiplier for the speed gain you are looking for. Use the smallest value that still gives you the performance you need, usually 10 to 20.
<b>Maximum no. of outbound channels</b>	Type the maximum number of outbound channels to use for file transfers. These values should correspond to the appropriate multiplier for the speed gain you are looking for. Use the smallest value that still gives you the performance you need, usually 10 to 20.
<b>Stability interval (sec)</b>	Type the number of seconds to build an average speed for a single connection. After this time is reached, channels are added.
<b>Channel ramp-up</b>	Type the number of channels to be added as the data transfer speed increases.
<b>Minimum fast speed (Kb/sec)</b>	Type the speed in KB per second for an existing channel to reach before a new channel is added to the tunnel.
<b>Minimum slow speed (Kb/sec)</b>	Type the speed in KB per second for an existing channel. If the speed of the channel goes below the specified speed, then the channel is removed from the tunnel.
<b>Speed threshold (%)</b>	Type the threshold of the speed in percentage for an existing channel. If the current speed is above the speed threshold value, then ActiveTransfer adds a new channel to the tunnel.

4. Click **Save** or **Save & Close**.

The tunnel is updated with the configured settings.

## Modifying a Tunnel

You can edit the configuration settings of an existing tunnel.

### > To modify a tunnel

1. On the navigation pane, select **Settings > Acceleration**.

2. On the Acceleration page, click on a tunnel that you want to edit.
3. Modify the required configuration settings for the tunnel.
4. Click **Save** or **Save & Close**.

The tunnel is updated with the modified settings.

## Configuring Audit Settings

---

You can configure logs to be recorded for all or specific ActiveTransfer assets through audit settings.

### > To configure audit settings

1. On the navigation pane, select **Settings > Audit Settings**.
2. On the Properties page, select the **Enable audit logs** option, and select either all or specific assets for which you want logs to be recorded. You must at least select one asset if you enable this option.

**Note:**

By default, the audit logs are disabled.

3. Click **Save**.

The logs for the selected assets are audited and appear in the Audit log page.

## Configuring File Share Settings

---

Depending on how you want the Web client users to share files, you can configure the default settings to display on the file share screen of the Web client users to share files with external users. You can also enforce the use of the default file share settings by the Web client users by disabling access to modify the settings.

**Note:**

Web client users can also share files from ActiveTransfer Gateway. In the file share email, the shared file link includes the configured ActiveTransfer Gateway machine name and port number.

### > To configure the default file share settings for Web client users

1. On the navigation pane, select **Settings > File share**.
2. On the File share page, deselect **Allow user to change file share settings in Web client** if you want to disable the modification of the default settings by Web client users.

## 3. Specify the following details:

Field	Description
<b>Share configuration</b>	<p>Select one of the following options on how ActiveTransfer should share a file:</p> <ul style="list-style-type: none"> <li>■ <b>Copy:</b> To create a copy of the original shared file and store it in a temporary folder. The file share recipient will have access only to this file copy. The link works even if the original file is deleted. When the link expires, the file is deleted from the temporary storage.</li> <li>■ <b>Move:</b> To move the original shared file to a temporary folder, which is, accessible to the file share recipient. When the link expires, the original file is deleted from the temporary folder.</li> <li>■ <b>Reference:</b> To create a pointer to the original shared file that is shared in a virtual folder. Any changes made by the file share recipient is to the original file.</li> </ul> <p>A reference is like an alias. As long as the file name is not changed, the users can access the file. Changing the name of the original file will break the link because the reference points to the original file.</p>
<b>Validity</b>	<p>Configure the following accessibility settings for the shared file:</p> <ul style="list-style-type: none"> <li>■ <b>Default validity (days):</b> Type the number of days that a shared file must be accessible to the file share recipient. This value cannot exceed the limit that you configure in <b>Maximum validity (days)</b>. Once the validity expires, the file share link in the file share email will not be accessible to the recipient.</li> <li>■ <b>Maximum validity (days):</b> Type the maximum number of days that the Web client users can share a file.</li> </ul>
<b>Email</b>	<p>Type the following default details to use in email notifications that file share recipients receive:</p> <ul style="list-style-type: none"> <li>■ <b>From:</b> Type a valid email address of an ActiveTransfer user or the server variable <code>%user_email%</code>. If you specify <code>%user_email%</code> as the default sender of the file share email, ActiveTransfer uses the email address of the Web client user initiating the file share.</li> <li>■ <b>Subject:</b> Type a subject line for the email.</li> <li>■ <b>Body:</b> Type the content to specify additional information for the email. The default format is: <ul style="list-style-type: none"> <li>A user would like to share a file with you: {web_link}</li> <li>This link will expire on {date} at {time}.</li> </ul> </li> </ul>

Field	Description
	User Name: {username} Password: {password}
	Where, <ul style="list-style-type: none"> <li>■ <i>{web_link}</i> is the link to the location of the shared file.</li> <li>■ <i>{date}</i> at <i>{time}</i> are the date and time on which the file share link will become inactive.</li> <li>■ <i>{username}</i> is the temporary user name to use when accessing the shared file. In emails, <i>{username}</i> is encrypted in the file share link.</li> <li>■ <i>{password}</i> is the temporary password to use when accessing the shared file. In emails, <i>{password}</i> is encrypted in the file share link.</li> </ul>
<b>Permissions</b>	Select the default file share permissions from the following options: <ul style="list-style-type: none"> <li>■ <b>View (read-only)</b></li> <li>■ <b>Download</b></li> <li>■ <b>Upload</b></li> <li>■ <b>Delete</b></li> <li>■ <b>Rename</b></li> <li>■ <b>Create folder</b></li> <li>■ <b>Delete folder</b></li> </ul>
<b>Security</b>	Type any value between 4 and 15 for the <b>Temporary password length</b> that ActiveTransfer must use when auto-generating a password for recipients to access the shared file. The default value is 8.

4. Click **Save**.

The default settings for file sharing is configured.

## Configuring Server Properties

You can configure ActiveTransfer Server properties using the **Properties** screen. The Properties screen allows you manage all the server configuration properties such as add, delete, and update the property. The modifications you make on any of the properties in this screen will get updated in the properties file (properties.cnf). This file is located in the *Integration Server\_directory* \instances\instance\_name\packages\WmMFT\config directory on ActiveTransfer Server. The updated properties are available to ActiveTransfer Server at runtime.

When you are updating the property, the other remote server aliases of ActiveTransfer Server nodes will correspond to the updated properties and runtime.

### > To configure properties

1. On the navigation pane, select **Settings > Properties**.
2. On the Properties page, click the  button and select the properties from the list of properties in the **Add new property** window.
3. Click  button to add the properties and save the changes.

You can delete a property by selecting it and clicking the  button. However, this action only deletes the value of the property from the properties.cnf file.

## Configuring ActiveTransfer to Send Emails

Configure ActiveTransfer to send emails in the following scenarios:

- As an email task for post-processing and scheduled actions
- When a new user is created

### Note:

- To send emails when a new user is created, you must enable **Activate email alerts for user creation/update** option under **User email settings** in **Settings > General settings**.
- If you have configured ActiveTransfer to send emails in the properties.cnf file, ActiveTransfer will continue to use this configuration unless you update the fields in **User email settings**. For more information, see [“Configuring Default Email Settings in properties.cnf” on page 193](#).

- When a user password is changed
- When a user shares a file manually using the web client

Before you configure ActiveTransfer to send emails, you must configure the SMTP server and the default email settings.

For more information about configuring the SMTP server, see [“Configuring the SMTP Server” on page 191](#).

For more information about configuring the default email settings, see [“Configuring Default Email Settings in the User Interface” on page 192](#) or [“Configuring Default Email Settings in properties.cnf” on page 193](#).

## Configuring the SMTP Server

Configure the SMTP server to send emails using one of the following methods:

- Edit the resource settings on the **Settings > Resources** page in Integration Server Administrator.
- Set the server configurations for SMTP server and SMTP server port.

For more information about these methods, see the "Server Configuration Parameters" chapter in *webMethods Integration Server Administrator's Guide*.

## Configuring Default Email Settings in the User Interface

### ➤ To configure the default email settings in the user interface (UI)

1. On the navigation pane, go to **Settings > General Settings**.
2. In **User email settings**, check **Activate email alerts for user creation/update** option.
3. Specify the email details in **User email settings**. The following table lists the supported email fields:

Field	Description
<b>From</b>	Send email on behalf of the user.
<b>Subject</b>	Subject of the email.

**Template for user email** Email template for the user creation alert.

You can configure the following server variables in your user email template:

- *{firstName}*: First name of the user.
- *{lastName}*: Last name of the user.
- *{username}*: User ID for the user.
- *{password}*: Password for the user.
- *{serverList}*: Listener URLs for the user.

**Template for password email** Email template for the password creation alert.

You can configure the following server variables in your password email template:

- *{firstName}*: First name of the user.
- *{lastName}*: Last name of the user.
- *{password}*: Password for the user.

Field	Description
<b>Subject for forgot password email</b>	Subject of the forgot password email.
<b>Template for forgot password email</b>	<p>Email template for the forgot password email.</p> <p>You can configure the following server variables in your forgot password email template:</p> <ul style="list-style-type: none"> <li>■ <i>{firstName}</i>: First name of the user.</li> <li>■ <i>{lastName}</i>: Last name of the user.</li> <li>■ <i>{username}</i>: User ID for the user.</li> <li>■ <i>{expiryTimeStamp}</i>: Password expiry timestamp for the user.</li> <li>■ <i>{passwordResetLink}</i>: Password reset link for the user.</li> </ul>

4. Click **Save**.

**Note:**

- The following two email alerts will be sent to the user when the user password is changed:
  - Email with the user ID and server details.
  - Email with the new password details.
- If you save the changes after entering the details in the UI, the email templates configured in `\WmMFT\config` directory will not be used.

## Configuring Default Email Settings in `properties.cnf`

### ➤ To configure default email settings in `properties.cnf` file

1. Open the ActiveTransfer configuration properties file (`properties.cnf`), located in the `Integration Server_directory \instances \instance_name \packages \WmMFT \config` directory, and set the default sender, external ActiveTransfer Server URL, and email subject line in the following parameters:
  - `mft.user.email.from`
  - `mft.user.email.public.ip`
  - `mft.user.email.subject`

For more information about these parameters, see [“Server Configuration Parameters and Variables” on page 221](#).

**Note:**

If you are specifying email settings as part of defining a “send email” action for a post-processing or scheduled event, you can override the sender and subject line parameters,

as well as provide required information such as the email recipient and email body, as part of defining the event. For details, see [“Configuring Additional Settings for a Listener” on page 40](#).

2. Configure the body of the emails sent when user profiles are created or modified by editing the following files located in the *Integration Server\_directory* \instances\*instance\_name*\packages\WmMFT\config directory in a text editor:
  - For emails that will be sent to new users, edit the `NewUserEmailContent.txt` file.
  - For emails that will be sent to existing users whose profile you have changed, edit the `ExistingUserEmailContent.txt` file.

You can include user variables in the body of the email that is sent when user profiles are created or modified.
3. Ensure that at least one server port is configured with the **Share this information with the user through email** option.
4. Reload the WmMFT package. For more information about reloading packages, see the "Reloading a Package" section in *webMethods Integration Server Administrator's Guide*.

## Disabling Email Alerts

### Note:

You must be an administrator to disable the email alerts.

➤ **To disable the automatic email alerts when you create a new user or update a user password**

1. On the navigation pane, go to **Settings > General Settings**.
2. In **User email settings**, clear the **Activate email alerts for user creation/update** checkbox.
3. Click **Ok**.

## Configuring Password Complexity for Users

---

Configure ActiveTransfer allows users to configure the complexity of passwords for their partner users. The configuration is available at **Settings > General settings > Password settings**, where following aspects can be set:

- Minimum number of lower-case letters
- Minimum number of upper-case letters
- Minimum number of special characters
- Minimum number of numeric characters

- Minimum length of the password

These aspects are applied to all the instances and the restrictions apply to the following scenarios:

- The password restrictions are honored while creating new partner users with **Generate random password** and **Create new password** options.
- The password restrictions do not impact the already existing partner users passwords.



# 13 Managing User Interface Permissions for Users, Roles, and Groups

- Overview ..... 198
- Configuring UI Permissions to Users, Roles, or Groups ..... 198
- Searching UI Permissions for Users, Roles, or Groups ..... 199

## Overview

---

Delegated administration access enables administrators to provide restricted access to users, Common Directory Service roles, and Integration Server groups with granular permissions to specific ActiveTransfer screens. With controlled access to ActiveTransfer screens; users, Common Directory Service role, or Integration Server groups can edit and view only the specified set of assets they are assigned permissions to and not the entire data. Also, administrators can configure the users to manage the assets of all partners or specific partners. The transactional data and ActiveTransfer assets such as, virtual folders and users that are accessible by the logged-in partner user is filtered based on the partners associated to them.

## Configuring UI Permissions to Users, Roles, or Groups

---

The ActiveTransfer user interface can be accessed by:

- Administrator users
- Users with UI permissions to specific ActiveTransfer screens
- Users who are part of the MFTAdministrators, MFTMonitoringUsers, Common Directory Service roles, MFTMonitoringUsers, or Integration Server groups

### Note:

- Users who are added to the ActiveTransfer UI permissions page but are not given access to any of the assets will not be able to log into ActiveTransfer. You must provide users with access to ActiveTransfer screens and functional actions to enable users to log into ActiveTransfer.
- Changes to the UI permissions for users are reflected in the next successful login into ActiveTransfer administration user interface by the users.

### > To configure UI permissions

1. In the navigation pane, select **UI permissions**.
2. On the UI permissions page, click  **+ Add**.
3. In the Add Users, Roles, Groups dialog box:
  - a. Select **Users**, **Roles**, or **Groups** tab.
  - b. Select the users, Common Directory Service roles, or Integration Server groups either from the list under each tab or perform a search.
  - c. Click **Add**.
4. Select a user, role, or group.

- a. Under **UI permissions**, select the assets and the respective functional actions.
- b. (Optional) To allow users to access and manage assets of only specific partners, select **Partner user (Restricted access)**.
  - a. Under **Partners**, select **All partners** or type the partner name in the **Select partners** text box
  - b. Under **UI permissions**, select the assets and the respective functional actions.
  - c. To allow users to access the folders and files of partners on the local machine, under **Virtual folders**, select **Allow access to the server's local file system**.

**Note:**

When **Allow access to the server's local file system** is disabled, users without local file access will not be able to edit existing virtual folders.

5. Click **Save**.

The users, roles, or groups are configured with access to specific ActiveTransfer assets and functional actions.

## Searching UI Permissions for Users, Roles, or Groups

Search the UI permissions list to view the ActiveTransfer asset permissions assigned to users, roles, or groups.

➤ **To search for asset permissions assigned to users, roles, or groups**

1. In the navigation pane, select **UI permissions**.
2. On the UI permissions page, type a user, role, group name in the search field.
3. Click **Reset** and **Apply** for the changes to take effect.

The UI permissions list is populated with details matching your search criteria.



# 14 Archiving Data

■ Overview .....	202
■ Configuring the Schema/Database for Data Archive .....	202
■ Configuring the ActiveTransferArchive Database Pool .....	204
■ Configuring the ActiveTransfer User Interface for Data Archive .....	204
■ Archiving Data from the ActiveTransfer User Interface .....	205
■ Scheduling Data Archive .....	205
■ Searching for Archived Data .....	205
■ Executing the Stored Procedure for Data Archive .....	206

## Overview

---

ActiveTransfer stores file transaction, action execution, agent file transfer, and activity logs in the schema (Oracle, PostgreSQL) or database (Microsoft SQL Server, MySQL). You can archive data available in the ActiveTransfer production schema or database to an archive schema or database.

You can archive data through any of the following approaches:

- Through the ActiveTransfer user interface. See [“Archiving Data from the ActiveTransfer User Interface” on page 205](#).
- By executing the stored procedure scripts in the database. See [“Executing the Stored Procedure for Data Archive” on page 206](#).
- By executing the `wm.mft.admin:archiveData` service. For details, see *webMethods ActiveTransfer Built-In Services Reference*.

## Configuring the Schema/Database for Data Archive

---

For data archival, you must create a separate schema (Oracle, PostgreSQL) or database (Microsoft SQL Server, MySQL).

**Note:**

The archive schema created for Oracle or PostgreSQL should be in the same database that hosts the production schema.

Install the ActiveTransferArchive component in the archive schema or database using Database Component Configurator (DCC). The ActiveTransferArchive component contains stored procedures required for the archival process. The component also creates a table for logging the execution history of the archival process. The ActiveTransferArchive component automatically installs the ActiveTransfer database component as well. The table structure in the archive schema or database is a mirror of the production schema or database.

The archive schema or database should have SELECT and DELETE permissions for the following tables that store runtime or transaction data in the production schema or database:

- MFTTRANSACTION
- MFTEVENTLOG
- MFTACTIVITYLOG
- MFTACTIVITYLOGMESSAGE
- MFTACTIVITYDETAILS
- MFTAGENTEVENTLOG
- MFTAGENTACTIVITY
- MFTAGENTACTIVITYDETAILS

The archive schema or database should have SELECT permissions for the following tables that store asset information such as actions, agents, and so on in the production schema or database:

- SCHEDULEDACTIONS
- POSTPROCESSEVENTS
- MONITORFOLDERACTION
- INSTANCECONFIG
- SERVERCONFIG
- PARTNERMAPPING
- MFTAGENT
- MFTAGENTEVENTS

The PostgreSQL archive and production schema should have the following list of GRANT, ALTER permissions:

- GRANT CONNECT ON DATABASE *postgres\_db* TO *archive\_user*;
- GRANT USAGE, CREATE ON SCHEMA *archive\_schema\_name* TO *archive\_user*;
- GRANT USAGE, CREATE ON SCHEMA *production\_schema\_name* TO *archive\_user*;
- GRANT ALL ON SCHEMA *archive\_schema\_name* TO *archive\_user*;
- GRANT ALL ON SCHEMA *production\_schema\_name* TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *archive\_schema\_name* GRANT ALL ON TABLES TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *archive\_schema\_name* GRANT ALL ON SEQUENCES TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *archive\_schema\_name* GRANT ALL ON FUNCTIONS TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *archive\_schema\_name* GRANT ALL ON TYPES TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *production\_schema\_name* GRANT ALL ON TABLES TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *production\_schema\_name* GRANT ALL ON SEQUENCES TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *production\_schema\_name* GRANT ALL ON FUNCTIONS TO *archive\_user*;
- ALTER DEFAULT PRIVILEGES IN SCHEMA *production\_schema\_name* GRANT ALL ON TYPES TO *archive\_user*;

- GRANT ALL ON ALL TABLES IN SCHEMA *production\_schema\_name* TO *archive\_user*;
- GRANT ALL ON ALL SEQUENCES IN SCHEMA *production\_schema\_name* TO *archive\_user*;
- GRANT ALL ON ALL FUNCTIONS IN SCHEMA *production\_schema\_name* TO *archive\_user*;

## Configuring the ActiveTransferArchive Database Pool

You must configure the ActiveTransferArchive database pool in Integration Server to perform any of the following tasks:

- Execute the services in the WmMFT package for archiving data.
- Archive data through the ActiveTransfer user interface. For details, see [“Archiving Data from the ActiveTransfer User Interface” on page 205](#).
- View the execution logs of the data archive process in ActiveTransfer user interface.

The ActiveTransferArchive database pool should be configured to the same schema or database where the ActiveTransferArchive database component is installed. For more details, see *Installing Software AG Products*.

## Configuring the ActiveTransfer User Interface for Data Archive

To archive data for production schemas or databases, you must first configure the archive criteria for the production schema or database.

### ➤ To configure ActiveTransfer for data archive

1. In the navigation pane, select **Database archival**.
2. On the Database archival page, click .
3. In the Database archive settings dialog box, specify:

Field	Description
<b>Archive schema name</b>	Type the name of the production schema (Oracle, PostgreSQL) or database (Microsoft SQL Server, MySQL).
<b>Retention period (days)</b>	Type the number of days to retain data in the production schema or database before archive.

4. Click **Ok**.

## Archiving Data from the ActiveTransfer User Interface

---

After you configure the archive settings in ActiveTransfer, archive data on the production schema or database.

### ➤ To archive data from the ActiveTransfer user interface

1. In the navigation pane, select **Database archival**.
2. On the Database archival page, click **Archive Now**.
3. Read the confirmation message and click **Ok** to proceed.

The execution log of the archive process appears in the database archival list.

## Scheduling Data Archive

---

To archive data at regular intervals, use the Integration Server scheduler to configure the schedule settings for the `wm.mft.admin:archiveData` service.

Execute the `wm.mft.admin:archiveData` service to start the archive process.

## Searching for Archived Data

---

Search the archive list to view the details about archived data based on date and time, status, and user ID.

### ➤ To search for archived data

1. In the navigation pane, select **Database archival**.
2. On the Database archival page, specify all or one of the following search criteria:

Field	Description
<b>Date and time</b>	Select a time period from the list or specify a custom date range, and click <b>Ok</b> .
<b>Status</b>	Select one of the following: <ul style="list-style-type: none"> <li>■ <b>All:</b> To list all the archived data in ActiveTransfer.</li> <li>■ <b>Success:</b> To list data that have been archived successfully.</li> <li>■ <b>Failed:</b> To list data that have failed to be archived.</li> <li>■ <b>Warning:</b> To list data that have been archived with warnings.</li> </ul>

Field	Description
User ID	Type the user ID of the user who executed data archival.

---

3. Click **Reset** and **Apply** for the changes to take effect.

The archive list is populated with the archived data details matching your search criteria.

4. Click on any record to view the complete archive process details.

## Executing the Stored Procedure for Data Archive

You can start the archive process by executing the ARCHIVE\_MFT\_DATA stored procedure in the archive schema or database.

The parameters required to execute the stored procedure are as follows:

- p\_retain\_days
- p\_runtime\_schema\_name
- p\_archive\_schema\_name
- p\_batch\_size
- p\_user\_id

The stored procedure execution logs appear in the ARCHIVE\_MFT\_LOG database table. For more information about how to execute stored procedures, see the stored procedure execution instructions specific to your database.

# 15 Managing ActiveTransfer Account Settings

■	Configuring ActiveTransfer Account Settings .....	208
---	---	-----

## Configuring ActiveTransfer Account Settings

You can configure account settings for the user interface screens such as landing page, page size, page depth, date format, time format, and time zone in ActiveTransfer using the following two options:

- **My settings:** To configure settings for specific users.
- **Default settings:** To configure settings that are default to all users.

**Note:**

Only the Administrator user or a user who is part of the *MFTAdministrators* group in Integration Server.

1. Log on to webMethods ActiveTransfer Server.
2. Click  on the top-right corner and click **Account settings**.
3. You can configure or modify the following application settings under **My settings** and **Default settings** respectively:

**Note:**

- The configurations under **My settings** overrides the configurations under **Default settings**.
- The **Default settings** are displayed by default to the monitoring users.
- In Chrome and Firefox web browsers, the language settings on the web browser dictates the preferred language on the login page and the language settings on the computer where ActiveTransfer Server is installed dictates the preferred language in the user interfaces after you log in.
- In Internet Explorer web browser, the language settings on your computer dictates the preferred language on the login page and the language settings on the computer where ActiveTransfer Server is installed dictates the preferred language in the user interfaces after you log in.

Field	Description
<b>General</b>	
<b>Landing page</b>	Select an option from the list. This will be the landing page when you log on to ActiveTransfer.
<b>Page size</b>	Select a value from the list. The number of entries on each page (where pagination is applicable) appears based on the value you select.
<b>Language</b>	Select your preferred language from the list.
<b>Virtual folder</b>	

Field	Description
<b>Note:</b>	The virtual folder configuration is applicable only to the administrator.
<b>Page size</b>	Type the number of folders for display in the Virtual folders page.
<b>Page depth</b>	Type the folder depth upto which you want to apply the folder count. The folder depth value is 1 for root folder and 2, 3, and so on for subfolders depth levels.  For example, if <b>Number of folders to display</b> is 100 and <b>Count folder depth up to</b> is 3, then each page in the folder frame displays 100 folders with a depth of 1, 2, or 3. All sub folders after depth level 4 appear but not be considered for pagination.
<b>Date and time</b>	
<b>Date format</b>	Select a date format from the list. This setting is applicable for all ActiveTransfer logs and scheduled actions.
<b>Time format</b>	Select a time format from the list. This setting is applicable for all ActiveTransfer logs and scheduled actions.
<b>Time zone</b>	Select a time zone from the list. This setting is applicable for all ActiveTransfer logs and scheduled actions.

- Click **Save**.

The configured settings are updated under **My settings** or **Default settings** respectively.



# 16 Removing User Data from ActiveTransfer

■ Overview .....	212
■ Removing PII from the ActiveTransfer Log Files .....	212
■ Removing PII from the ActiveTransfer Database .....	213

## Overview

---

Data protection laws and regulations, such as the General Data Protection Regulation (GDPR) might require specific handling of user data, even after a user profile is removed from ActiveTransfer. This user data might be personally identifiable information (PII), such as user names, email addresses, or client IP addresses of employees or clients stored in ActiveTransfer and the central user directory or LDAP. When a user is removed from ActiveTransfer, the user information is still available in the central user directory or LDAP as the information might be used by other products. To comply with data protection requirements and user requests, in addition to deleting the user account, you should delete or mask the user data.

## Removing PII from the ActiveTransfer Log Files

---

The `ActiveTransfer.log` contains information about user name, ID, email address, and user's client IP address.

The default location of the `ActiveTransfer.log` is `Integration Server_directory\profiles\IS_default\logs\` or if configured as a log appender in the `Integration Server_directory\IS_default\configuration\logging\log4j2.properties\org.eclipse.equinox.simpleconfigurator` file.

Upon request, you may need to remove PII for a user from the ActiveTransfer log files.

If you enable back up of `ActiveTransfer.log`, then after this file reaches its maximum limit, the information is logged in consecutive files in the following format: `ActiveTransfer.log.<number>`

The following table identifies the type of user data that might be written to `ActiveTransfer.log`, how to locate the data, and how to delete the data:

PII data in log	How to find and remove
User ID of the user logged into ActiveTransfer Server	<p>Use a text editor to perform a search and replace for the user ID in <code>ActiveTransfer.log</code>. For example, you could search the <code>ActiveTransfer.log</code> files for the user ID and replace the user ID with an anonymous string or a blank string.</p> <p>You can also avoid logging this information by setting <code>&lt;level value="info"/&gt;</code> to off.</p>
Client IP Address from which the user logged into ActiveTransfer Server	<p>ActiveTransfer rarely stores client IP addresses in log messages. If stored, use a text editor perform a search and remove or replace the client IP address in <code>ActiveTransfer.log</code>.</p>
Email address of external user logged into the Web client	<p>ActiveTransfer rarely stores email addresses of external users in log messages. If stored, use a text editor to perform a search and remove or replace the email address in <code>ActiveTransfer.log</code>.</p> <p>Additionally, this information is also available in the <code>info.xml</code> file under your temporary shared directory, as configured in the <code>mft.sharing.account.tempdir</code> property in the <code>\packages\</code></p>

**PII data in log****How to find and remove**

WmMFT\config\properties.cnf file. The default location of the shared directory is \packages\WmMFT\resources\TempAccounts. The files in the shared folder are accessed by the user with who the file is shared. You can search for the email address in this shared folder and delete the corresponding file. However, this shared file is deleted after the expiry of the shared folder.

## Removing PII from the ActiveTransfer Database

---

The ActiveTransfer database contains information about user ID, email address, and client IP address.

The following table identifies the type of user data that might be written to the ActiveTransfer database, how to locate the data, and how to delete the data:

**PII data in database****How to find and remove**

User ID of the user logged into ActiveTransfer Server and performed file transfers	Search for the user ID in the MFTActivityLog.UserID table in the database, and delete the records for a particular user or replace it with an anonymous string or a blank string.
--	---

Client IP Address from which the user logged into ActiveTransfer Server and performed file transfers	Search for the client IP address in the MFTTransaction.USERIP table in the database, and delete the records for a particular user or replace it with an anonymous string or a blank string.
--	---



# 17 Migrating Assets

■ Overview .....	216
■ ActiveTransfer Assets You Can Migrate .....	216
■ Migration Methods .....	217
■ ActiveTransfer Asset Dependencies .....	217
■ How ActiveTransfer Server Detects Assets on the Target System Before Importing Them .....	219
■ Importing Assets .....	219
■ Exporting Assets .....	219

## Overview

---

You can migrate ActiveTransfer assets from one ActiveTransfer environment to another. Migrate assets when:

- You want to deploy assets from a development environment to a production environment.
- You have multiple ActiveTransfer Server instances and you want each instance to have identical assets. You can create the assets on one ActiveTransfer Server instance and then migrate the assets to the other instances.

In this context, a *server instance* is the ActiveTransfer Server instance that you are exporting assets from, or importing assets to, as well as the ActiveTransfer Gateway instances defined for the particular ActiveTransfer Server instance.

- You want to change the type of database you use for ActiveTransfer. For example, you were using an Oracle database and now want to use a SQL Server database.

### Important:

Only use the procedures in this chapter to migrate ActiveTransfer assets between ActiveTransfer Server instances of the same release. If you need to migrate assets from one release of ActiveTransfer Server to another, follow the instructions in *Upgrading Software AG Products*.

## ActiveTransfer Assets You Can Migrate

---

You can migrate the following ActiveTransfer assets:

- **ActiveTransfer Server instances:** You can migrate the ActiveTransfer Server instances that are configured on the source ActiveTransfer Server.
- **ActiveTransfer Gateway instances:** You can migrate the ActiveTransfer Gateway instances that are configured on the source ActiveTransfer Server.
- **ActiveTransfer Server ports:** You can migrate the configuration for FTP, FTPS, SFTP, HTTP, and HTTPS ports. You can also migration the configuration for server ports associated with ActiveTransfer Gateway instances defined on the source server.
- **ActiveTransfer Server preferences:** You can migrate general ActiveTransfer Server preferences, such as throttling, restrictions, banning, encryption, acceleration, and miscellaneous settings. You can also migrate preferences for the ActiveTransfer Gateway instances defined on the source server.
- **User templates:** You can migrate templates that are created for user configuration.
- **User configuration:** You can migrate ActiveTransfer users, groups, and roles, as well as their and configuration settings such as, throttling, restrictions, encryption, acceleration, and partner associations.
- **Virtual file system:** You can migrate VFS definitions and configuration settings such as location, partner association, and user access.

- **Partner mapping:** You can migrate the mappings between partners and the users and virtual folders with which those partners are associated. If Trading Networks is installed, ActiveTransfer performs the mapping using the partners available in Trading Networks. If Trading Networks is not installed, ActiveTransfer manages partner information separately.
- **Post-processing actions:** You can migrate post-processing action configuration, including actions to execute when the action is triggered.
- **Scheduled actions:** You can migrate scheduled action configuration, including actions to execute when the action is triggered.

ActiveTransfer assets are available for migration even if they are disabled. The state of the assets on the source system is maintained on the target system. The migration process does not include deleted assets.

You cannot migrate ActiveTransfer Server or MashZone NextGen instance settings defined on the ActiveTransfer Instances page. These settings are used to connect the ActiveTransfer Server and the MashZone NextGen server, and are not specific to any ActiveTransfer Server instance.

When an asset includes a certificate or keystore definition, you can only migrate the file path location of that certificate or keystore. You must manually deploy the actual certificate or keystore file separately.

## Migration Methods

---

You can migrate all ActiveTransfer assets, all assets of a certain type, or selected assets within an asset type. Use any one of the following methods to migrate ActiveTransfer assets:

- The `wm.mft.admin:exportData` and `wm.mft.admin:importData` built-in services. For details on the built-in services, see *webMethods ActiveTransfer Built-In Services Reference*.
- Repository-based deployment in Deployer. For details on how to use Deployer to migrate ActiveTransfer assets, see *webMethods Deployer User's Guide*.
- Importing and exporting assets within ActiveTransfer. For details on how to import or export assets, see [“Importing Assets” on page 219](#) and [“Exporting Assets” on page 219](#)

## ActiveTransfer Asset Dependencies

---

Some assets require other assets. For example, users use assets such as templates and partners, and virtual file systems use assets such as users. For migrated assets to work properly, these required assets must also exist on the target system.

When a dependency exists, ActiveTransfer automatically exports or imports the dependent assets.

The following table lists all possible dependencies an asset might have, as well as specific instructions for migration where appropriate. The name you use for an asset on the target system must match the name on the source system, with the same capitalization.

Asset	Dependency
ActiveTransfer Server ports	ActiveTransfer Server ports have a dependency on the server instance to which they are configured.
ActiveTransfer Server preferences	ActiveTransfer Server preferences have a dependency on the server instance for which they are configured.
User profiles	<p>User profiles have a dependency on user templates, partners, and server instances that define tunnels for the users.</p> <p><b>Note:</b> If Trading Networks is installed, migrate partner profiles defined in Trading Networks separately.</p>
Virtual file system folders	<p>VFS folders have a dependency on users and partners who have been granted access to the folders.</p> <p><b>Note:</b> If Trading Networks is installed, migrate partner profiles defined in Trading Networks separately.</p>
Post-processing actions and associated actions	Post-processing actions have a dependency on users, associated VFS folders, and partners who have been granted access to the folders.
Partner mapping	<p>Partner mappings have a dependency on Trading Networks partner profiles.</p> <p><b>Note:</b> If Trading Networks is installed, migrate partner profiles defined in Trading Networks separately.</p>
Scheduled actions and associated actions	<p>Scheduled actions have a dependency on associated VFS folders and partners who have been granted access to the folders.</p> <p><b>Note:</b> If Trading Networks is installed, migrate partner profiles defined in Trading Networks separately.</p>

If a dependent asset is not present in the file being imported or is not present on the target server, ActiveTransfer Server does not import the asset. ActiveTransfer Server logs an error message and continues importing the remaining assets.

If the export file contains the dependent assets for any asset, the `wm.mft.admin:importData` service ensures that the required assets are migrated first so that no error occurs.

## How ActiveTransfer Server Detects Assets on the Target System Before Importing Them

---

When you import an asset, ActiveTransfer Server checks whether an asset with the same asset name already exists on the target system. For user assets, ActiveTransfer Server checks the authentication ID (user ID).

The *force* parameter in the `wm.mft.admin:importData` service specifies whether to update an asset when ActiveTransfer Server finds a matching asset on the target system. If *force* is set to `true` and ActiveTransfer Server finds a match, the server overwrites the asset on the target system. The *force* parameter does not apply when mapping partner assets. If the partner information already exists on the target server, ActiveTransfer Server ignores the imported partner asset.

## Importing Assets

---

1. In ActiveTransfer, go to **Asset movement > Import Assets**.
2. On the **Import Assets** page, select the ZIP that you want to import.
3. After importing the ZIP file, you can use the **Filters** menu to filter the assets by the asset name or you can manually select the assets that you want to import.
4. Resolve the errors in the analysis report to import assets successfully. The three categories of severities are **Error**, **Warning**, and **Skip**.
5. Click **Import**. To overwrite assets that might already exist in the target audience, select **Force import**. On the Import Assets page, review the asset list that you have imported.
6. If you have more assets to import, click **Start new import**.

**Note:**

ActiveTransfer does not support the export or import of Tunnels as an asset.

## Exporting Assets

---

To export ActiveTransfer assets

1. In ActiveTransfer, go to **Asset movement > Export Assets**.
2. On the **Export Assets** page, select the assets to export from the tabs that mention the types of assets. The **Include dependencies** option is selected by default. Clear this option if you do not want the dependent assets to be included in the export file. Each asset specifies the number of dependencies it has. To view all the dependent assets, click the number against each asset.
3. After you select the assets, click **Add to export list** and click **Next**. When selecting a virtual folder, all the child virtual folders are selected by default, but not the parent virtual folder.

4. On the Export assets page, the assets are mentioned under their own respective tabs. Verify the final export set. Assets can be removed while verifying the final export set.
5. Click **Next**.
6. On the **Export Assets** page, select the export action **Export as a .zip file** and specify a name for the export file.

**Note:**

ActiveTransfer downloads the exported assets in the form of a ZIP file. The location of the downloaded file depends on your browser configuration.

7. Click **Finish**.
8. ActiveTransfer has an option to export all assets. Click on the check box **Export all** and follow the instructions from step 4 to complete export of all assets.

**Note:**

ActiveTransfer does not export or import tunnels configured for Users, Roles, Groups, and Templates

**Note:**

You need to migrate all assets to certificate IDs using ActiveTransfer built-in service `wm.mft.admin:updateFileBasedCertToDB` before exporting and importing to higher environments, if these assets have any configurations pointing to a filepath as created by using Software AG Designer. Run the `wm.mft.admin:updateFileBasedCertToDB` service, to scan all the assets for certificates and store them into a database linking them to the assets using certificate IDs. If you later want to revert this behavior, run the `wm.mft.admin:updateCertFromDBToFile` service.

# A Server Configuration Parameters and Variables

---

■ Server Configuration Parameters .....	222
■ Security Configuration Parameters .....	232
■ Server Variables .....	233

## Server Configuration Parameters

---

This section contains a description of the parameters you can specify in the ActiveTransfer Server properties configuration file, `properties.cnf`. This file is located in the `Integration Server_directory\instances\instance_name\packages\WmMFT\config` directory on ActiveTransfer Server. To update the files, you should first shut down ActiveTransfer Server and, if you are using ActiveTransfer Gateway, and then edit the file using a text editor. After you make the changes, restart the ActiveTransfer Server and Gateway.

ActiveTransfer Server uses default values for many of the parameters. If a parameter has a default, it is listed with the description of the parameter.

You can also use the `wm.mft.admin:manageProperties` service to view and change the current values of some of these parameters. For details, see *webMethods ActiveTransfer Built-In Services Reference*.

### mft.aliases.tn

Specifies the remote server aliases for Trading Networks instances hosted on remote Integration Server hosts. These remote server aliases are defined in the Integration Server Administrator portal. When synchronizing partner details and transferring files to remote Trading Networks instances, ActiveTransfer checks this parameter in order to determine to which remote Trading Networks instances it must connect. Use commas to separate the remote server aliases.

For example: `mft.aliases.tn=remote server alias 1,remote alias 2,remote alias 3`

**Note:**

This parameter is applicable only if you have webMethods Product Suite version 9.12 and later.

If you do not specify any value in this parameter, ActiveTransfer only connects to local Trading Networks instances (that is, Trading Networks instances hosted on the same Integration Server host as ActiveTransfer).

### mft.client.file.optimizeListing

Specifies if ActiveTransfer's optimized or normal file listing functionality must be used on Microsoft Windows Server directories.

When you have an extremely large number of files for ActiveTransfer to list, set this parameter to `true` to enable the optimized file listing functionality. If you retain the default value of `false`, ActiveTransfer uses its normal file listing functionality.

### mft.client.ftp.list.command

Specifies the list command to use on remote FTP servers. The value for this parameter is not case-sensitive. The possible values are:

- `LIST`. ActiveTransfer executes the `LIST` command to list the file directories on the remote FTP servers. `LIST` is the default value if you have not specified a value for the parameter, or if the value you specified is invalid.

- **MLST.** If the remote FTP servers support the MLST command, ActiveTransfer executes the MLST command to list the file directories on the remote servers. If the remote FTP servers do not support the MLST command, LIST command is used.

## **mft.client.http.maxUploadSize**

Specifies the maximum file size for non-chunked data in upload operations to HTTP(S) servers. The default value is 10 MB.

## **mft.client.networkDiscovery.timeout**

Specifies the number of milliseconds ActiveTransfer Server should wait to establish an outgoing connection before ending it. By default, this property has no value, in which case, ActiveTransfer Server uses the JVM network connection's timeout setting.

For example: `mft.client.networkDiscovery.timeout=250`

## **mft.client.outbound.useProxy**

Specifies if you want to enable the use of proxy server settings for file transfers. The possible values are:

- `true`. Supports outbound connections through proxy servers.
- `false`. Default value. ActiveTransfer ignores all proxy server alias configurations, and creates a direct connection to the remote server.

## **mft.client.session**

This section describes the parameters that you can configure in the ActiveTransfer Server cache for client sessions. These parameters are only available with ActiveTransfer Server 9.7 fix 7 and higher.

### **Note:**

These parameters are provided for advanced configuration settings which are not expected to change unless there is a specific requirement in your ActiveTransfer Server.

### **mft.client.session.cache.ttl**

Specifies the time in seconds for clients sessions to be stored in cache. This is used only for event execution. A client session is logged out and removed from the cache when this parameter is exceeded. The default value is 120 seconds. This property is used only when `session.reuse` is set to `true`.

### **mft.client.session.cache.pingInterval**

This parameter relates to the caching of client sessions created to connect to remote servers when ActiveTransfer executes an event. Specifies the idle time in seconds for a client session stored in the cache after which a test command is run to verify if the client session is valid, before the session is used again. The default value is 30 seconds. If the value of this property is

set to 0, ActiveTransfer runs a test command to verify the validity of the session each time, prior to executing a remote operation. Set the value of this property to a higher value (> 0) to reduce the number of test commands that have to be run in scenarios which involve transfer of a large number of files, and frequent use of remote operations.

### **mft.log.sessionlog.disable**

Specifies if logging of session information should be disabled for individual user sessions.

If you retain the default value of `false`, ActiveTransfer creates separate log files for each ActiveTransfer Server user session in the following directory:

*Integration Server\_directory \instances\instance\_name\packages\WmMFT\resources\logs\session\_logs*

If you set this parameter to `true`, ActiveTransfer does not create logs for ActiveTransfer Server user sessions in the given directory.

## **mft.client.zip.extract.maxFileSize**

Specifies the maximum size of zip files to be unzipped using Unzip task.

The default value for this property is 10240. By default, ActiveTransfer set a limit of 10240\*1024\*1024 bytes (10 GB) size for a zip file to unzip by Unzip task.

For example, if you want to set a 20GB limit, then you can set the value 20480 for this property. ActiveTransfer achieves this by multiplying the value for the property with 1024 \* 1024 internally.

## **mft.client.zip.extract.maxFiles**

Specifies the maximum number of files a zip file can contain to unzip using Unzip task. The default value is 1000.

## **mft.sftp.port.forward.allow**

Specifies if the port forwarding is allowed on SFTP listeners.

## **mft.client.sftp.unmask**

Specifies the default unmask used to connect to SFTP servers. The default value is 022.

## **mft.db**

This section describes the parameter you can set in ActiveTransfer to retry a database connection.

### **mft.db.connection.retry**

Specifies the number of times ActiveTransfer should retry a connection to a database when there is a broken connection caused by transient database errors. The default value is 0.

### **mft.db.connection.retryInterval**

Specifies the interval in seconds ActiveTransfer should wait between connection retries to a database. The default value is 10 seconds.

## mft.server

This section describes the parameter you can set in ActiveTransfer Server.

### **mft.server.auth.rolesGroups**

Specifies if all user login requires the Role or Group information. Set this property to `true` only when VFS has permissions to set the role or group.

### **mft.server.dmz.http.upload.confirm**

Checks the connection between your ActiveTransfer Server and ActiveTransfer Gateway. When set to `true`, ActiveTransfer Gateway verifies with ActiveTransfer Server if a file upload is successful.

### **mft.server.https.auth.redirectURI**

SSO authentication redirects the URL when `mft.server.https.auth.sml` is set to `true`. All listeners are ignored.

### **mft.server.import.size.max**

Specifies maximum file size that can be imported. Maximum file size is 10 MB.

## mft.server.commandcentral

This section describes the parameters you can use to register the Command Central instance used to install ActiveTransfer Agent instances. These parameters are available in the `CommandCentral.cnf` file. ActiveTransfer Server uses the information in these parameters to connect to the Command Central instance when synchronizing agent installation details from Command Central.

### **.commandCentral.host**

Specifies the host name or IP address of the machine that hosts the Command Central instance used to install ActiveTransfer Agent instances.

### **mft.server.commandCentral.port**

Specifies the port for the Command Central instance used to install ActiveTransfer Agent instances.

### **mft.server.commandCentral.port.secure**

Specifies if communication between the Command Central instance and ActiveTransfer Server must use SSL protocol.

### **mft.server.commandCentral.username**

Specifies the user name to use when ActiveTransfer Server connects with Command Central.

### **mft.server.commandCentral.password**

Specifies the password to use when ActiveTransfer Server connects with Command Central.

## mft.event

This section describes the parameter you can set for post-processing events configured on ActiveTransfer Server.

### **mft.event.sleep.time**

Specifies the time interval ActiveTransfer Server should wait to trigger a post-processing event. The default is 1 second. If you set the value of this property to 20 seconds, ActiveTransfer Server holds a post-processing event in a queue and triggers the event along with the other events that are queued, at 20 second intervals.

### **mft.event.scheduler.runAsUser**

Specifies the user name associated with the scheduled task whenever an Integration Server scheduled task is created by ActiveTransfer. The default is `Administrator`. However, ActiveTransfer does not change the user while updating the scheduled task.

### **mft.event.session.reuse**

#### **Important:**

Do not configure this parameter in your production environment. This parameter is provided to help solution providers debug the individual actions in an event.

ActiveTransfer reuses the connections (sessions) to remote servers that are created by ActiveTransfer event actions. This is achieved by caching the sessions for the event and reusing them later in similar actions within the same event instance. This parameter specifies if client sessions should be reused or not in ActiveTransfer events. The default value is `true`. If you set this parameter to `false`, a new session is created for each operation involving a remote server connection in the ActiveTransfer event actions. The new session is closed soon after the remote operation is completed.

### **mft.event.actions.caseSensitive**

Specifies if the action name search in action log page is case sensitive.

### **mft.event.move.skipRename**

ActiveTransfer Server attempts to rename a file when the Move operation is used and the host machine is the same for the source and destination locations. This adversely affects files located on two different drives. Set the property to `false` if files are moved across different drives to skip rename, copy, and delete the original file.

### **mft.event.manual.allowStatusChange**

The manual schedule action is deactivated, by default. This parameter allows manual scheduled action to be activated.

## mft.group.aliases

When more than one ActiveTransfer instances share the same database(ActiveTransfer Group), this property specifies the remote server alias for the other nodes. These remote server aliases are defined in the Integration Server Administrator portal. This information is used to synchronize different assets like VFS, Post Process Action, Scheduled Actions across all nodes in the group.

For example: `mft.group.aliases=remote server alias 1,remote server alias 2,remote server alias 3`

**Important:**

Do not configure this parameter with a node that points to itself.

For instance, let us assume that you have node A and node B. Now, to configure the `mft.group.aliases` for node A, you must point it as `mft.group.aliases=node B`, excluding the node A.

Configuring the node that points to itself results in a performance issue.

## mft.http

`mft.http`. This section describes the parameters you can configure for HTTP ports.

**mft.http.default.port**

Specifies the default HTTP port for ActiveTransfer Server to use for collecting data for the Logs page. The default is 2080.

**mft.http.default.port.secure**

Specifies if the default HTTP port created in MFT is made secure. By default HTTP port is not secure.

## mft.query.maxrows

Specifies the maximum number of asset records to fetch from the database and display on the ActiveTransfer Server monitoring pages. The default value for this parameter is 1000.

To avoid errors in the log details views, always set the value of this parameter in relation to the cache parameter `maxElementsInMemory` available in **Integration Server Administrator > Settings > Caching > SoftwareAG.IS.MFT > MFTQueryResults**. The value of `mft.query.maxrows` must be lesser (by five times) or equal to the value of `maxElementsInMemory`. If the value of `mft.query.maxrows` is higher than the recommended value, users might encounter the `Failed to fetch file transactions` error while navigating a large number of paginated record pages.

## mft.never.ban.list

Specifies a list of IP addresses that should be excluded from the hammering settings that you configure in ActiveTransfer Server. The IP addresses listed using this property are not banned by the ActiveTransfer Server or the ActiveTransfer Gateway. If you have an ActiveTransfer Server and an ActiveTransfer Gateway instance, apply the restriction to the ActiveTransfer Gateway. Apply the restriction to the server only in the absence of an ActiveTransfer Gateway instance.

**Note:**

If you have a load balancer, include the load balancer IP in this list.

Restart the ActiveTransfer Server and the ActiveTransfer Gateway instances associated with the server for this property to take effect.

## **mft.vfs.tree.pagination.depth**

When there is a large number of virtual folders, the Virtual Folder Management page takes longer than expected to load the virtual folders. This property along with `pageSize` will do pagination on VFS screen.

This property specifies the folder depth at which to apply the folder count provided in the property `mft.vfs.tree.pagination.pageSize`. The folder depth value is 1 for the root folder, 2, 3, and so on for the child folder depth levels.

## **mft.vfs.tree.pagination.pageSize**

When there is a large number of virtual folders, the Virtual Folder Management page takes longer than expected to load the virtual folders. This property along with `mft.vfs.tree.pagination.depth` will perform the pagination on Virtual folders screen.

This property specifies the number of virtual folders to display in the Virtual Folder Management page. Software AG recommends a value of 300 or less. Higher values for this property might result in lengthy loading time. The value `-1` displays all virtual folders.

## **mft.partners.useTNPartners**

Specifies if ActiveTransfer must synchronize with and use the partners configured in Trading Networks. You can either use ActiveTransfer partners or Trading Networks partners, not both.

The default value is `false`. Set this parameter to `false` if you want to use partners configured in ActiveTransfer.

Set this parameter to `true` to use partners configured in Trading Networks. On changing the parameter value to `true`, the ActiveTransfer partners become invalid.

### **Note:**

This parameter is applicable only if you have webMethods Product Suite version 9.12 and later.

## **mft.session.replication**

This section describes the parameters you can configure for the ActiveTransfer Servers to enable session replication in a group of ActiveTransfer Servers.

### **mft.session.replication.enable**

Enables the replication of the HTTP user sessions across all the ActiveTransfer Server nodes. Replicating session information across nodes is expensive. The default value is `false`. Set the property to `true` only if HTTP listeners in ActiveTransfer Server nodes are exposed through a load balancer. Set to `false` if ActiveTransfer Gateway does not require session replication.

### **mft.session.replication.address**

Specifies the IP address or host name, and port details of this ActiveTransfer Server node. The parameters are as follows:

`IP_address_node_1:port_node_1`

`IP_address_node_1` The IP address or host name of this ActiveTransfer Server node.

`port_node_1` The port number on which the session replicator is running for this node.

For example: `mft.session.replication.address=10.60.30.100:7800`

**Note:**

The IP addresses cannot be loopback addresses (localhost or 127.0.0.1).

**mft.session.replication.other.nodes**

Specifies the IP address or host name, and port details of the ActiveTransfer Server nodes that will form a group with this server node. The parameters are as follows:

`IP_address_node_2[port_node_2]`, `IP_address_node_3[port_node_3]`... `IP_address_node_n[port_node_n]`

`IP_address_node_n` The IP address of the nth node in the group.

`port_node_n` The port on which the session replicator is running on the nth node.

For example:

`mft.session.replication.other.nodes =10.60.27.214[7800],10.60.28.89[7800]`

## mft.server

This section describes the parameters you can configure for ActiveTransfer Server to enable SSO.

**mft.server.https.auth.saml**

The default value is `false`. Set this parameter to `true` to enable SSO for HTTPS listeners in ActiveTransfer Server for access through the ActiveTransfer web client.

**mft.server.https.auth.saml.redirecturi**

Specifies the redirection URI. Set the redirection URI, that you provided when registering with the identity provider.

## mft.server.dmz.cert.hostnames

Set the comma-separated hostnames that ActiveTransfer uses to validate the gateways SSL certificate's hostnames.

## mft.server.dmz.exclude

A comma-separated list of Gateway server names that cannot connect from this instance. This property is useful when there are multiple server and gateway and you want to avoid crisscross connections among them. Setting the accept IP list in the Gateways cannot establish the connection. However, ActiveTransfer Servers will continue trying to connect to all the Gateways. This property will help to avoid this scenario.

## **mft.server.sftp.algorithms.keyexchange.exclude**

Specifies a comma-separated list of key exchange algorithms that need to be excluded from the supported list for SFTP servers.

## **mft.server.sftp.algorithms.keyexchange.preferred**

Specifies the preferred key exchange algorithm for SFTP servers.

## **mft.server.crlUrl**

If certificate-based authentication is enforced through either the "Require valid certificate" or "Require valid certificate and password" field for FTPS (implicit or explicit) and HTTPS ports, ActiveTransfer validates the client certificate against the certificate revocation list (CRL) specified in `mft.server.crlUrl` to permit or block client access to ActiveTransfer Server.

Set the value of `mft.server.crlUrl` as either as a file stored in an accessible directory or a file that can be downloaded from a URL.

Example:

- `mft.server.crlUrl=C:/MFT/CRL/mftCRL.crl`
- `mft.server.crlUrl=http://softwareag.com/crls/mftCRL.crl`

If this property is not set, ActiveTransfer does not perform the CRL check.

## **mft.server.gateway.socket.timeout**

ActiveTransfer Gateway and ActiveTransfer Server connection break if the ActiveTransfer takes more time to respond with a timeout of 10 seconds, which causes a failure.

This parameter sets the timeout for a session in milliseconds between ActiveTransfer Server and ActiveTransfer Gateway. The default value is 10000.

Example: `mft.server.gateway.socket.timeout=10000`

## **mft.server.ftp.list.allowEmpty**

Specifies if the error code 450 is returned for LIST command for the file names that do not exist. When set to `true`, ActiveTransfer Server returns an empty list and not error code 450.

## **mft.sharing.account.tempdir**

Specifies a temporary directory location for a file share. When the ActiveTransfer group is available, this location must be a shared file location that is accessible from all the nodes. Use only forward slashes in the file path. For example, `D:/activetransfer/sharedcontent/`.

Software AG recommends that you replace the default shared file location with any local or shared directory.

## mft.ssl.client

This section describes the parameter you can configure for SSL authentication of a remote server.

### **mft.ssl.client.acceptAnyCert**

Specifies if ActiveTransfer Server should validate the SSL certificates from a remote server against the certificates in its truststore and allow communication only from trusted remote servers, or accept all SSL certificates. The default is `true`. Set the value of the property to `false` if you want ActiveTransfer Server to accept SSL certificates only from servers that have a truststore entry.

### **mft.ssh.client.preferred.publickey**

Specifies the preferred public key algorithm that ActiveTransfer Server should use to communicate with a SFTP server. The default is `ssh-dss`. Set the value of the property to `ssh-rsa` if you want ActiveTransfer Server to use the RSA key as the preferred public key algorithm. You must restart Integration Server for this change to take effect. This property is available only on the application of ActiveTransfer Server 9.7 Fix 4 and higher.

## mft.user.email

This section describes the parameters you can configure for the emails that are sent to ActiveTransfer users.

### **mft.user.email.from**

Specifies the email address of the ActiveTransfer administrator who will send messages to ActiveTransfer users when adding or editing the user's profile. If this parameter is not set, the message is sent without any "from email" address. The value you specify here is overridden by any value you set in the **File Share** settings.

### **mft.user.email.public.ip**

Specifies the ActiveTransfer Server host name to use for the external server URL that is emailed to users for logging in to the server. If this parameter is not set, the internal IP address is used in the email. This parameter also applies to the email notifications sent for shared files. The shared file link contains either the ActiveTransfer Server or ActiveTransfer Gateway if the source location of the shared file is the ActiveTransfer Server VFS or ActiveTransfer Gateway. For example, suppose the host for ActiveTransfer Server port 8080 is defined on the Server Management page as `localhost` or `127.9.1.10`. If this parameter is not set, the server URL that is emailed to users will contain the internal IP address of the server (in this example, `http://localhost:8080` or `http://128.1.10:8080`, respectively). If you set this parameter to the external host or domain name that your organization uses to represent the server's internal IP address, the server URL will reflect the external host name (for example, `http://xyz.com:8080`).

### **mft.user.email.subject**

Specifies the subject line of the email message that is sent to the user. If this parameter is not set, messages are sent without any subject.

## **mft.server.event.monitor.threads**

Specifies the thread pool size to run Monitor folder actions. The default value is 10.

## **mft.server.event.monitor.fileEvent.threads**

Specifies the thread pool size to process file events to trigger Monitor folder actions. The default value is 1000.

## **mft.server.http.header.csp.xss**

X-XSS-Protection header: This configurable property enhances the security of the application by restricting content sources and mitigating potential security vulnerabilities.

## **mft.server.http.header.csp**

Content-Security-Policy headers: This configurable property enhances the security of the application by restricting content sources and mitigating potential security vulnerabilities.

## **Security Configuration Parameters**

---

This section contains a description of the parameters you can specify in the ActiveTransfer Server security configuration file (`security.cnf`), which is located in the *Integration Server\_directory* \instances\instance\_name\packages\WmMFT\config directory. To update this file, you should first shut down ActiveTransfer Server and ActiveTransfer Gateway and then edit the file on ActiveTransfer Server and ActiveTransfer Gateway using a text editor. After you make the changes, restart Integration Server, ActiveTransfer Server, and ActiveTransfer Gateway.

## **mft.ssl**

This section describes the SSL security parameters you can configure.

### **mft.ssl.privatekey.password**

Specifies the private key password for the default SSL certificate.

### **mft.ssl.keystore.password**

Specifies the keystore password for the default SSL certificate.

### **mft.ssl.certificate.file.name**

Specifies the file name of the default SSL certificate.

## **mft.web.security**

This section describes the web security parameter that you can configure to make the ActiveTransfer web client more secure.

### **mft.web.security.httpOnly**

Specifies if the `httpOnly` header is added to all HTTP requests from ActiveTransfer Web client. The default is `false`.

#### **mft.server.http.header.verification.enable**

ActiveTransfer web client supports a set of HTTP headers which can be added to the `installation_dir\IntegrationServer\instances\default\packages\WmMFT\config\headers.txt` file. This property disables the header check by setting its value to `false`. The default value of this property is `true`.

#### **mft.web.security.sameSite**

Specifies if `sameSite` header is added to all HTTP requests from ActiveTransfer Web client. The default value is `false`.

#### **mft.web.security.csrf**

Specifies if `CSRF` header is added to all HTTP requests from ActiveTransfer Web client. The default value is `false`.

#### **Note:**

This property is available with ActiveTransfer 9.7 Fix 3 or later.

## Server Variables

By using variables, you can pass values to post-processing and scheduled actions dynamically at run time. For example, when you configure a copy action for a post-processing event, you can specify the destination URL as `{parent_path}` and the “rename file to” parameter as `{name}_processed`. When the event is triggered, ActiveTransfer Server copies the file to the parent directory and appends “\_processed” to the end of the file name.

#### **Note:**

For ActiveTransfer Web Client, enclose these variables within percent sign characters (%) instead of curly braces. For example, `{user_name}` is represented as `%userName%` in the Web Client.

ActiveTransfer supports general variables that handle special characters and error messages, variables that pertain to file references, variables that pertain to date and time formats, and user variables that pertain to the content of emails that are sent to ActiveTransfer users.

#### **Note:**

The variables are case sensitive.

## General Variables

Variable	Description	Supported Event Type
<code>{r}</code>	Return character.	Post-processing and scheduled actions
<code>{n}</code>	New line character.	Post-processing and scheduled actions

Variable	Description	Supported Event Type
{task_error}	Returns the last error that occurred in an action.	Post-processing and scheduled actions
{task_errors}	Returns the list of all the errors in an action.	Post-processing and scheduled actions
{error_trace}	Used to get the stack trace in case of any exception.	Post-processing and scheduled actions
{event_execution_id}	Returns the event execution ID which is unique for each event.	Post-processing and scheduled actions
{task_error_types}	Returns the type of actions where the error occurred.	Post-processing and scheduled actions
{host_name}	Host name of the ActiveTransfer Server.	Post-processing and scheduled actions
{outbound_proxy_alias}	Proxy server name that is defined for use with an action.	Post-processing and scheduled actions
{task_error_names}	Name of the action that results in an error.	Post-processing and scheduled actions
{parent_url}	Actual URL that points to the parent folder in which the file resides.	Post-processing and scheduled actions
{parent_url_decoded}	Decoded value of the variable {parent_url}	Post-processing and scheduled actions
{event_name}	Name of the action.	Post-processing and scheduled events
{ssl_protocol}	SSL/TLS version used for the HTTPS or FTPS protocol for a session.	Post-processing event
{ssl_cipher}	Cipher algorithm used for the HTTPS or FTPS protocol for a session.	Post-processing event
{random_string}	Generates a random string.	Post-processing and scheduled events

## File Reference Variables

### Note:

In event actions such as Write File to Database and Send Email that process multiple files, use the variables as per the following example:

```
<LINE>{stem}{ext}
</LINE>
```

This syntax ensures that all the files in the list are processed by these actions instead of just the first file.

Variable	Description	Supported Event Type
{command}	Command forwarded to remote FTP servers to list files.	N/A
{end}	End time for the file transfer.	Post-processing event
{error}	Error messages related to the file transfer.	Post-processing and scheduled events
{ext}	Last part of the file name, including the period.	Post-processing and scheduled events
{file_metadata}	Applicable only to FTP remote servers. Raw response from the remote server for each file while performing MLST, MLSD, LIST, or NLST commands.  Example: <pre>Type=file;Modify=20151006091701; Perm=r,w,a,d,f;Size=584; UNIX.owner=user;UNIX.group=group; properties_4.cnf</pre>	Scheduled event
{group}	Applicable only to FTP remote servers. Retrieves information from the UNIX ownership class <code>group</code> , <i>os-depend-fact</i> in MLST RFC 3659.	Scheduled event
{md5}	MD5 hash of the uploaded file.	N/A
{modified}	Applicable only to FTP remote servers. Date when the file was last modified in UNIX epoch time (milliseconds).	Scheduled event
{name}	Name of the file.	Post-processing and scheduled events
{owner}	Applicable only to FTP remote servers. Retrieves information from the UNIX ownership class <code>owner</code> , <i>os-depend-fact</i> in MLST RFC 3659.	Scheduled event
{parent_path}	Path to the parent folder.	Scheduled event

Variable	Description	Supported Event Type
{path}	Path of the file: <ul style="list-style-type: none"> <li>■ <b>Local file system.</b> Local directory path.</li> <li>■ <b>Remote file system.</b> Relative path of the file in a file system with respect to the current folder.</li> </ul>	Post-processing and scheduled events
{permissions}	Applicable only to FTP remote servers. Permission for the file on the remote server to which ActiveTransfer is connected. The format is <code>-rw-r--r--</code> . For MLST, this format is maintained only when <code>unix.mode</code> is available. If <code>unix.mode</code> is not available, the format is <code>r,w,a,d,f</code> , and is retrieved from <code>perm</code> .	Scheduled event
{real_parent_path}	Local path of the parent folder for the file on the disk.	Post-processing and scheduled events
{real_parent_path_decoded}	Decoded value of the variable {real_parent_path}	Post-processing and scheduled events
{real_path}	Complete path to the file in the local or remote file system.	Post-processing and scheduled events
{real_path_decoded}	Decoded value of the variable {real_path}	Post-processing and scheduled events
{resume_loc}	Location in the file where the transfer should resume if interrupted.	Post-processing and scheduled events
{size}	Size of the file.	Post-processing and scheduled events
{speed}	Speed of the file transfer.	Post-processing event  Note that when the actual speed is 0, this variable value might be inaccurate.
{start}	Start time for the file transfer.	Post-processing event
{stem}	First part of the file name, before the period.	Post-processing and scheduled events

Variable	Description	Supported Event Type
{the_file_error}	Any error during file transfer.	Post-processing and scheduled events
{the_file_name}	Name of the file.	Post-processing and scheduled events
{the_file_size_formatted}	Size of the file.	Post-processing and scheduled events
{the_file_speed}	Speed of the file transfer (upload/download) for post-processing events.	Post-processing event
{the_file_path}	Path of the file.	Post-processing and scheduled events
{url}	Actual URL that points to the file.	Post-processing and scheduled events
{url_decoded}	Decoded value of the variable {url}	Post-processing and scheduled events
{user_dir}	Folder that the user sees when uploading the file.	Post-processing and scheduled events
{user_session_download_count}	Total download count per user session for post-processing events.	Post-processing event
{user_session_upload_count}	Total upload count per user session for post-processing events.	Post-processing event
{user_time}	User upload/download time for post-processing events.	Post-processing event
{items_count} or {item_count}	Count of the number of files an events consists.	Post-processing and scheduled events

## Date/Time Variables

You can precede any of the date/time variables with the following symbols:

- Preceding a variable with a dot (.) results in replacing the variable with the current value. For example, {.dd} results in the current day and {.hh} results in the current hour.
- Preceding a variable with an underscore (\_) results in replacing the variable with the file's ending transfer time. For example, if a file was downloaded on Monday, and if the event triggered a "file rename" action with a value of Report\_{EEE} provided for the new file name, ActiveTransfer Server would rename the downloaded file to Report\_Mon.

Variable	Description	Supported Event Type
{MM}	Month (for example, 06 to represent June).	Post-processing and scheduled events
{dd}	Day (for example, 05 to represent the fifth day of the month).	Post-processing and scheduled events
{yy} or {yyyy}	Year, represented in two digits (for example, 13 to represent 2013) or four digits (for example, 2013).	Post-processing and scheduled events
{HH}	Hours, using the 24-hour time format (for example, 14 to represent the hour of 2 o'clock PM).	Post-processing and scheduled events
{hh}	Hours, using the 12-hour clock format (for example, 02 to represent the hour of 2 o'clock PM).	Post-processing and scheduled events
{mm}	Minutes.	Post-processing and scheduled events
{aa}	AM or PM.	Post-processing and scheduled events
{ss}	Seconds.	Post-processing and scheduled events
{S}	Milliseconds.	Post-processing and scheduled events
{EEE}	Weekday abbreviation (for example, Mon to represent Monday).	Post-processing and scheduled events
{MMM}	Month (for example, 12 to represent the month when the action is executed by ActiveTransfer Server	Post-processing and scheduled events
{d}	Date of the month.	Post-processing and scheduled events
{k}	Hour in 24-hour format.	Post-processing and scheduled events
{K}	Hour in 12-hour format.	Post-processing and scheduled events
{z}	Time zone (for example, IST).	Post-processing and scheduled events
{Z}	Time zone (for example, +5:30 in case of IST).	Post-processing and scheduled events

Variable	Description	Supported Event Type
{dd+n} or {d+n}	<p>Current date of the month plus "n" number of days. The final value is calculated based on the calendar days.</p> <p>Example</p> <ul style="list-style-type: none"> <li>■ For {dd+1} - If today's date is 30, the result is either 31 or 1, depending on whether the current month has 30 days or 31 days.</li> <li>■ For {d+n} - If today's date is 8, the result is 9.</li> </ul>	Post-processing and scheduled events
{dd-n} or {d-n}	<p>Current date of the month minus "n" number of days. The final value is calculated based on the calendar days.</p> <p>Example</p> <ul style="list-style-type: none"> <li>■ For {dd-1} - If today's date is 01, the result is either 30 or 31, depending on whether the current month has 30 days or 31 days.</li> <li>■ For {d+n} - If today's date is 8, the result is 7.</li> </ul>	Post-processing and scheduled events

## User Variables

User variables enable you to set values in the emails that ActiveTransfer Server sends to users when changes are made to a user's profile. You can also use these variables when setting a virtual folder path.

Variable	Description	Supported Event Type
{firstName}	First name of the user.	Post-processing and scheduled events
{lastName}	Last name of the user.	Post-processing and scheduled events
{user_name}	User ID of the user.	Post-processing and scheduled events
{serverList}	One or more URLs of the ActiveTransfer Server to which the user has access.	Post-processing and scheduled events
{username}	Name of the user who triggers the file operation (upload, download, or delete).	Post-processing events

<b>Variable</b>	<b>Description</b>	<b>Supported Event Type</b>
{email}	Email of the user who triggers the file operation (upload, download, or delete).	Post-processing events
{last_name}	Last name of the user who triggers the file operation (upload, download, or delete).	Post-processing events
{first_name}	First name of the user who triggers the file operation (upload, download, or delete).	Post-processing events

# **B** Calendar and Processing Options for Scheduled Events

---

■ Scheduled Event Options .....	242
---------------------------------	-----

## Scheduled Event Options

---

This section describes the calendar and processing options that are available when you specify conditions for a scheduled event.

### Date Range

The Date Range settings enable you to specify the start and end date and time for executing actions for scheduled events. These settings apply to all scheduled events except those specified to execute once.

Option	Description
<b>Date Range</b>	Populates the start and end date and time fields according to the value selected in this list. For example, selecting <b>This Week</b> populates <b>Start Date</b> with Sunday's date, <b>Start Time</b> with 12:00:00 AM, <b>End Date</b> with Saturday's date, and <b>End Time</b> with 11:59:59 PM.  Selecting <b>Custom</b> enables you to select a custom date range.
<b>Start Date</b> and <b>End Date</b>	Specifies the start date and end date. You can either type a date manually according to the default date format specified in your account setting or click the calendar icon to select a date.
<b>Start Time</b> and <b>End Time</b>	Specifies the start time and end time. You can either type the time increments manually according to the default time format specified in your account setting or click the arrow buttons to increase or decrease an individual time unit.
<b>No end date</b>	Indicates that you want the action to execute indefinitely.

### Process Actions Every *Time Period*

The Process Actions Every *Time Period* settings enable you to specify exactly when, within the specified date range, ActiveTransfer Server should execute actions for a scheduled event. These settings apply to all scheduled events except those specified to execute once, or at a fixed interval.

Option	Description
<b>Hours</b> and <b>Minutes</b>	Specifies the hour and minute portions of the time to execute an action (for example, 1:00 and 1:30, or 1:15 and 3:15).
<b>On these days</b>	Specifies the days of the week to execute a weekly action.
<b>Days of Month</b> or <b>Weekdays</b>	Specifies whether to specify days by calendar date (for example, 4 for the fourth day of the month) or by days of the week (for example, "second Tuesday of the month") to execute a monthly or yearly action.

Option	Description
<b>During these months</b>	Specifies the months to execute a yearly action.
<b>Do not overlap task</b>	Indicates that ActiveTransfer Server should complete a running action before starting the next one.

**Note:**

Selecting this check box might cause actions to start at other than specified times.

## Fixed Interval

The Fixed Interval settings enable you to specify the time interval that ActiveTransfer Server should wait (for example, 10 seconds) before executing the next action for a scheduled event. These settings apply to scheduled events that are specified to execute at fixed intervals.

Option	Description
<b>Interval</b>	Specifies the number of seconds, minutes, hours, weeks, or days that ActiveTransfer Server should wait before executing the next action in a scheduled event.
<b>Do not overlap task</b>	Indicates that ActiveTransfer Server should complete a running action before starting the next one.

**Note:**

Selecting this check box might cause actions to start at other than specified times.



# C Working with Jump Conditions

---

■ Overview .....	246
■ Jump Condition Elements .....	246
■ Defining a Jump Condition .....	248

## Overview

---

This section describes how to use server variables to define a jump condition in a Jump action.

## Jump Condition Elements

---

The jump condition has three parts: server variables, the qualifier, and the value of the server variables.

## Server Variables

The following server variables can be used in the jump condition:

Category	Server Variable	Description
File parameters	{name}	Name of the file.
	{stem}	First part of the filename before the period.
	{ext}	Last part of the filename including the period.
	{size}	Size of the file.
	{items_count}	Count of files.
Filepath parameters	{url}	Actual URL that points to the file.
	{parent_url}	Actual URL that points to the parent folder in which the file resides.
	{path}	Path to the file.
	{parent_path}	Path to the parent folder in which the file resides.
	{user_dir}	Directory the user sees when uploading a file.
	{real_path}	Local path for the file on the disk.
	{real_parent_path}	Local path of the parent folder for the file on the disk.
Transfer parameters	{speed}	Speed of the file transfer.
	{error}	Error messages related to the file transfer.

Category	Server Variable	Description
	{resume_loc}	Resume location in file.
	{md5}	MD5 hash of the uploaded file.
Transfer time window parameters	{start}	Start time for the file transfer.
	{end}	End time for the file transfer.
	{MM}	Month (for example, 06 to represent June).
	{dd}	Day (for example, 05 to represent the fifth day of the month).
	{yy} or {yyyy}	Year, represented in two digits (for example, 13 to represent 2013) or four digits (for example, 2013).
	{HH}	Hours, using the 24-hour time format (for example, 14 to represent the hour of 2 o'clock PM).
	{hh}	Hours, using the 12-hour clock format (for example, 02 to represent the hour of 2 o'clock PM).
	{mm}	Minutes.
	{aa}	AM or PM.
	{ss}	Seconds.
	{S}	Milliseconds.
	{EEE}	Weekday abbreviation (for example, Mon to represent Monday).

**Note:**

If you specify multiple server variables, separate each with a space.

## Jump Condition Qualifier

After you select the Jump task for an action, and have specified the server variables for the Jump condition, you can select a qualifier from the drop-down list in the **Jump Condition** section. The following qualifiers can be used in the jump condition:

Qualifier	Description
<b>Contains</b>	Includes items that contain a specified value.
<b>Does Not Contain</b>	Excludes items that contain a specified value.
<b>Equals</b>	Includes items that equal a specified value.
<b>Does Not Equal</b>	Excludes items that equal a specified value.
<b>Matches Pattern</b>	Uses pattern matching to include items that match a specified pattern.
<b>Does Not Match Pattern</b>	Uses pattern matching to exclude items that match a specified pattern.

## Values for the Server Variables

You can specify the values that the Jump condition should check for, in the last part of the jump condition.

**Note:**

If you specify multiple server variables values, separate each with a space.

## Defining a Jump Condition

---

### ➤ To define a jump condition

1. In the **Action** section of the **Event Management** page, select **Jump Action**.
2. Specify the **Action Name** and **Source Filter**.

For information on the use of wildcards in ActiveTransfer Server, see [“Features in Virtual Folders” on page 64](#).

3. Specify the **Jump Condition** as follows:
  - a. Enter or select server variables. For a list of server variables, see [“Server Variables” on page 233](#).
  - b. Select a qualifier for the drop-down box. For example, **Contains** to include items that contain a specific value.
  - c. Specify values for the server variables. The jump condition uses these values to search for items.
4. Configure other settings for the event and save the event.

## Examples

Some examples for jump conditions are listed below:

Example	Description
<code>{EEE} {stem} Contains FRI invoice</code>	ActiveTransfer Server triggers the Jump action if at the time of checking the Jump condition, the weekday is Friday and the file name contains <code>invoice</code> .
<code>{dd} {MM} {yyyy} Equals 12 01 2014</code>	ActiveTransfer Server triggers the Jump action if at the time of checking the Jump condition, the date of the action is <code>12.01.2014</code> .
<code>{url} Matches Pattern ^SFTP</code>	ActiveTransfer Server triggers a Jump action if the file URL starts with SFTP.
<code>{name} Matches Pattern invoice\$</code>	ActiveTransfer Server triggers a Jump action if the string <code>invoice</code> occurs at the end of the file name.



# D Limitations

---

■ Limitations .....	252
---------------------	-----

## Limitations

This appendix provides a high-level list of limitations and issues. For additional details, refer to your vendor documentation.

### Endpoint specific Constraints

Remote Path Endpoint	Operation	Limitation Description
Amazon-S3	Rename	Does not support renaming an Amazon-S3 folder.
	Preserve file modification date	Does not support setting the file modification date to an Amazon-S3 object or file.
	Append the file for Copy and Move	Does not support appending an object once an S3 object or a file is uploaded. This limits ActiveTransfer's support for resuming the transfer of the file from the point of interruption. This is applicable for Upload, Copy, and Move tasks.
	Socks proxy	ActiveTransfer supports only HTTP and HTTPs proxy for Amazon-S3 endpoints.
	Upload the batch of small files to Amazon-S3	<p>Uploading a batch of small files takes a significant amount of time. This action is time-consuming as ActiveTransfer needs to initiate and then confirm each upload irrespective of the size of the file.</p> <p>For events, it is recommended to use parallel processing for a large batch of small files which needs to be uploaded to the Amazon-S3 endpoint.</p>
	Unexpected behavior on unzip task with the compressed file in Amazon-S3	<p>If the source for an Unzip task is a ZIP file that contains a large number of files, then it can lead to unexpected behavior. This occurs in the following scenarios:</p> <ul style="list-style-type: none"> <li>■ For the compressed file which contains a larger number of files.</li> <li>■ For an unzip task which takes beyond 5 minutes to unzip the files.</li> <li>■ If S3 closes the input stream from where ActiveTransfer reads the compressed files.</li> </ul>

Remote Path Endpoint	Operation	Limitation Description
	Delete a folder	<p>Amazon-S3 does not support directory structure, hence it represents a directory using S3 keys and delimiter / symbol. If an S3 key contains a / symbol, then text till the delimiter is considered as a folder.</p> <p>However, if there are multiple S3 keys with the same folder name, then to delete a folder ActiveTransfer must delete all S3 file objects that belong to that particular folder. This process is time-consuming.</p> <p>If you attempt to delete a directory, then ActiveTransfer consumes time to list and delete the files of that particular directory.</p>
AZURE-FILE	Rename	Does not support the Rename operations.
	Preserve file modification date	Does not support setting the file modification date.
AZURE-BLOB	Rename	ActiveTransfer allows you to rename blob files below 256 MB
	Preserve file modification date	Does not support setting the file modification date.
	Create directory	If you want to place a blob within a directory, thenActiveTransfer will maintain the hierarchy. However, you will not be able to create a directory explicitly without any files in it.
Hosted-S3	Rename	Does not support renaming an Hosted-S3 folder.

