

Managing File Transfers with webMethods ActiveTransfer

Version 10.11

October 2021

This document applies to webMethods ActiveTransfer Server 10.11 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: MAT-MANAGING-FILE-TRANSFERS-WITH-ACTIVE-TRANSFER-1011-20240223

Table of Contents

About this Guide	9
Document Conventions.....	10
Online Information and Support.....	11
Data Protection.....	12
1 Understanding ActiveTransfer	13
Overview of Managed File Transfer.....	14
What Is webMethods ActiveTransfer?.....	14
Features of webMethods ActiveTransfer.....	15
Typical Usage Scenarios.....	17
ActiveTransfer Architecture.....	17
How does ActiveTransfer work with Trading Networks?.....	19
Failover Support for File Transfer Operations.....	21
Session Reuse.....	25
Use of Special Characters in Search.....	25
2 Configuring webMethods ActiveTransfer	27
Before Configuring ActiveTransfer.....	29
Summary of Configuration Steps.....	29
ActiveTransfer License File.....	30
Configuring Database Settings.....	31
Configuring a MySQL Community Server Version 5.7 Database.....	32
Adding an ActiveTransfer Server Instance to My webMethods.....	32
Configuring Timeout for ActiveTransfer Server Web Service Responses.....	33
Configuring Session Replication in ActiveTransfer Servers.....	34
Replacing the Default SSL Certificate.....	34
User Certificate Mapping.....	35
Verifying the Location of Keystore Files for ActiveTransfer.....	36
Managing Proxy Server Aliases.....	37
Connecting to HTTP(S) Servers.....	40
Configuring ActiveTransfer to Send Emails.....	41
Configuring the Maximum Number Actions in an Event.....	42
Configuring and Managing Acceleration.....	42
Configuring MashZone NextGen.....	47
Starting and Stopping ActiveTransfer.....	51
Configuring Single Sign-On for ActiveTransfer User Interface.....	51
Configuring Single Sign-On for ActiveTransfer through SAML 2.0.....	53
Configuring Single Sign-On in the Configuration File.....	53
Configuring Single Sign-On for ActiveTransfer Web Client.....	54
3 Granting Access to ActiveTransfer Pages in My webMethods	57
Overview.....	58
Defining Roles.....	58

Adding My webMethods Users to the MFT Administrators Role.....	59
Granting a Role the Ability to Access an ActiveTransfer Server Instance.....	59
Associating an Existing My webMethods Server Role with ActiveTransfer.....	59
Granting or Denying Access to Specific ActiveTransfer Pages in My webMethods.....	60
Granting the Authority to Execute ActiveTransfer Services.....	61
4 Preparing to Manage and Monitor ActiveTransfer Server in My webMethods.....	63
Overview.....	64
Selecting the Instance to Work With.....	64
Searching for Items and Managing Search Results.....	64
5 Managing ActiveTransfer Server.....	67
Managing ActiveTransfer Ports.....	68
Setting Passive FTP Mode for ActiveTransfer Server.....	72
Configuring a FTP Port to Support Implicit and Explicit SSL.....	73
Configuring an HTTPS Port to Support Single Sign-On.....	74
Configuring the Certificate Revocation List for secure ports.....	74
Setting the Command Delay Interval.....	75
Setting the Encryption Method for ActiveTransfer Server.....	75
Setting SSH Encryption Algorithm, Ciphers, and Connection Options.....	76
Setting Throttling Options.....	80
Setting Server Restrictions.....	80
Banning IP Addresses.....	82
Specifying Encryption Settings.....	84
Accelerating Data Transfer.....	88
Configuring Miscellaneous Settings.....	89
6 Working with Templates.....	93
Overview.....	94
Adding a Template.....	94
Specifying a Default Template.....	94
Specifying Throttling Options at the Template Level.....	95
Specifying Restrictions at the Template Level.....	96
Specifying Encryption and Decryption Options at the Template Level.....	100
Specifying Acceleration Options at the Template Level.....	101
7 Managing Users, User Groups, and User Roles.....	103
Overview.....	104
Associating an Existing My webMethods Server User with ActiveTransfer.....	104
Associating an Existing My webMethods Server User Group with ActiveTransfer.....	106
Creating a New User.....	107
Viewing and Editing User Details.....	108
Associating a User with a Partner or with Your Enterprise.....	109
Editing Server Access Details for a User.....	109
Emailing Change of Password and Server Port Details.....	110
Specifying Throttling Options for a User.....	111
Specifying Restrictions for a User.....	112
Specifying Encryption and Decryption Options for a User.....	117

Specifying Acceleration Options for a User.....	118
8 Managing Virtual Folders in a Virtual File System.....	121
Overview.....	122
Managing the Virtual File System in ActiveTransfer.....	122
Creating a Virtual Folder.....	123
Associating Virtual Folders with a Proxy Server Alias.....	124
Searching for Folders, Associated Users, and Associated Partners.....	124
Filtering the Virtual Folder List.....	125
Deleting a Virtual Folder.....	125
Organizing Virtual Folders.....	126
Associating a Virtual Folder with a Physical Folder Location.....	127
Configuring ActiveTransfer Server for SSL Communication with Remote Servers.....	128
Specifying Encryption and Decryption Options for a Virtual Folder.....	129
Specifying User Permissions for a Subfolder.....	130
User, Group, and Role Permission Propagation in VFS.....	131
Specifying User Access Privileges for a Virtual Folder.....	132
Specifying User Permissions for a Subfolder.....	134
Specifying User Access Privileges in the Parent Folder.....	135
9 Managing Events.....	137
About Events.....	139
Adding an Event.....	139
Defining Conditions that Trigger an Event.....	141
Defining Actions to Execute when an Event Is Triggered.....	144
File Processing in Event Actions.....	144
Executing File Operations.....	145
Executing an Integration Server Service.....	169
Executing a Script.....	171
Executing a Trading Networks Service.....	173
Sending Universal Messaging or Broker Notification.....	176
Sending an Email Message.....	178
Writing File Content to the Database.....	180
Jumping to a Designated Action.....	182
Excluding Files from an Action.....	184
Defining an Error Action.....	185
Activating an Event.....	186
Activating, Deactivating, and Deleting Multiple Events.....	187
Parameterizing Scheduled Event Actions.....	188
Parameterizing Scheduled Events to Poll Source URLs and Transfer Files to Destination URLs.....	191
Examples for Configuring an Event.....	193
10 Monitoring ActiveTransfer.....	197
Overview.....	198
Monitoring File Transaction Activity.....	198
Monitoring Events.....	201
Viewing ActiveTransfer Analytical Information.....	202

11 Managing and Viewing Log Information.....	205
Managing Log Files.....	206
Configuring Logging in the Installation Directory.....	206
Setting Up Audit Logging from the My webMethods User Interface.....	209
Viewing ActiveTransfer Server Logs in My webMethods.....	209
Viewing Server Information in My webMethods.....	210
Searching for Keywords in ActiveTransfer Server Log.....	211
Filtering ActiveTransfer Server Logs for Keywords.....	211
Viewing User Information in My webMethods.....	212
Viewing Audit Logs in My webMethods.....	213
12 Partitioning the Database.....	215
Partitioning the ActiveTransfer Database.....	216
13 Migrating Assets.....	217
Overview.....	218
ActiveTransfer Assets You Can Migrate.....	218
Migration Methods.....	219
ActiveTransfer Asset Dependencies.....	219
How ActiveTransfer Server Detects Assets on the Target System Before Importing Them.....	221
14 Removing User Data from ActiveTransfer.....	223
Removing User Data.....	224
Removing PII from the ActiveTransfer Log Files.....	224
Removing PII from the ActiveTransfer Database.....	225
Removing PII from the My webMethods Server Database.....	225
15 Administering ActiveTransfer with Command Central.....	227
Overview.....	228
Managing ActiveTransfer Licenses in Command Central.....	228
Lifecycle Actions and Statuses of The WmMFT Package.....	228
16 Working with the New User Interface.....	229
Understanding ActiveTransfer.....	231
Configuring ActiveTransfer.....	237
Managing Listeners.....	247
Managing Gateways.....	261
Managing Virtual Folders.....	267
Managing Actions.....	279
Managing Users and Templates.....	331
Viewing and Downloading Logs.....	347
Managing Proxy Servers.....	359
Managing Certificates.....	365
Managing ActiveTransfer Settings.....	367
Managing User Interface Permissions for Users, Roles, and Groups.....	385
Archiving Data.....	387

Managing ActiveTransfer Account Settings.....	393
Removing User Data from ActiveTransfer.....	395
A Server Configuration Parameters and Variables.....	399
Server Configuration Parameters.....	400
Security Configuration Parameters.....	410
Server Variables.....	411
B Calendar and Processing Options for Scheduled Events.....	419
Scheduled Event Options.....	420
C Working with Jump Conditions.....	423
Overview.....	424
Jump Condition Elements.....	424
Defining a Jump Condition.....	426
D ActiveTransfer Access Points.....	429
Overview.....	430
Ports that ActiveTransfer Uses.....	430
IP Addresses and Host Names that ActiveTransfer Uses.....	431
Products to Which ActiveTransfer Connects.....	431
File Paths.....	432
E Limitations.....	433
Limitations.....	434

About this Guide

■ Document Conventions	10
■ Online Information and Support	11
■ Data Protection	12

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. For complete information, see [“Working with the New User Interface” on page 229](#).

Document Conventions

Convention	Description
Bold	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

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at <https://documentation.softwareag.com>.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at <https://empower.softwareag.com/>.

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>.

To submit feature/enhancement requests, get information about product availability, and download products, go to [Products](#).

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the [Knowledge Center](#).

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at https://empower.softwareag.com/public_directory.aspx and give us a call.

Software AG Tech Community

You can find documentation and other technical information on the Software AG Tech Community website at <https://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.
- Go to our public GitHub and Docker repositories at <https://github.com/softwareag> and <https://hub.docker.com/u/softwareag> and discover additional Software AG resources.

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 Managed File Transfer	14
■ What Is webMethods ActiveTransfer?	14
■ Features of webMethods ActiveTransfer	15
■ Typical Usage Scenarios	17
■ ActiveTransfer Architecture	17
■ How does ActiveTransfer work with Trading Networks?	19
■ Failover Support for File Transfer Operations	21
■ Session Reuse	25
■ Use of Special Characters in Search	25

Overview of Managed File Transfer

Managed file transfer (MFT) is a process 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. MFT uses a combination of advanced software and secure communications protocols to provide the following:

- Reliable, secure data transfer
- Automated data transfers based on specific policies, partners, and permissions
- Better 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:

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

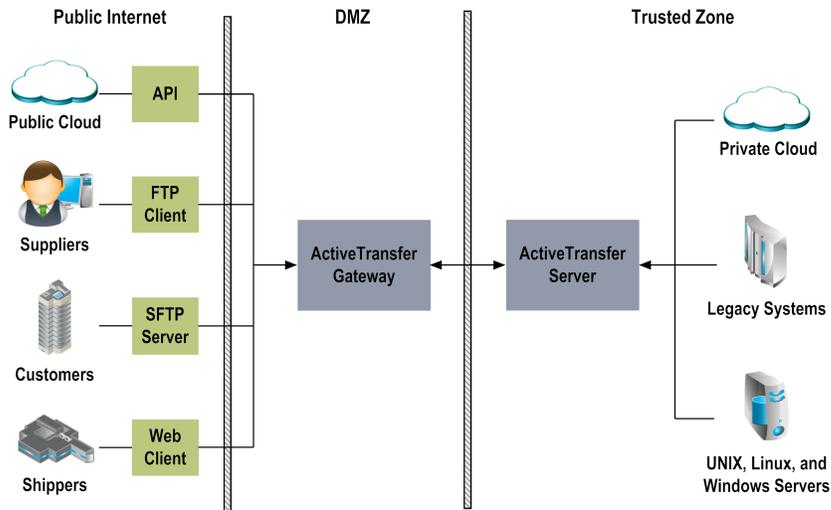
MFT offers a number of security, administration, and scalability advantages over non-secure file transfer protocols such as FTP. With MFT, there is no need to develop custom code for routine functions such as delivery confirmation, reporting, audit, security provisioning, and trading partner/community 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 activity, 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 at a high level how ActiveTransfer components fit into an MFT scenario.



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.

Features of webMethods ActiveTransfer

ActiveTransfer offers the following features:

- 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 showing metrics, making comparisons, and summarizing key activity.
- Business event triggers:** Provides the ability to trigger scheduled or post-processing actions based on file transfer criteria that you specify. For example, an action can be configured 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, 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 the file to the database.
- Multi-protocol support:** Provides full support for HTTP, HTTPS, FTP, FTPS (SSL), SFTP (SSH), SCP (server only), SMB (client only), WebDAV, WebDAVs protocols.
- Cloud file storage support:** Provides support for Amazon-S3 service, Azure Containers and Azure File shares.
- Proxy server support:** Provides full 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 specific days of the week and time of day.
- **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. ActiveTransfer also supports third-party clients such as those for FTP, FTPS, and SSH, enabling partners to transfer files using their existing technologies.
- **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, events, and files.
- **Acceleration:** Accelerated file transfers use a server's full 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 transfer.
- **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 events that fail when an ActiveTransfer Server goes down or for post-processing events that have not started after a file transfer is complete because the 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 event threads:** Provides you the option of selecting parallel processing of files in multiple threads instead of single-thread, sequential processing of files in an event. 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 events. 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 ports; 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

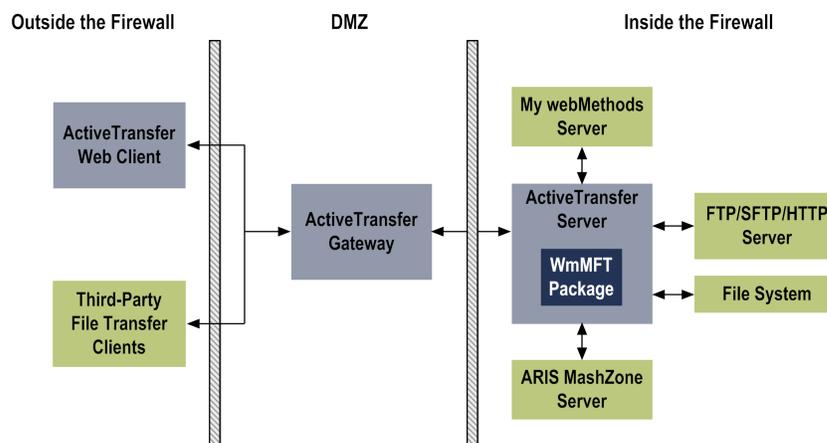
ActiveTransfer Architecture

ActiveTransfer consists of the following components, which interact with your internal FTP clients and with other applications and systems:

- ActiveTransfer Server, which resides behind a firewall.
- ActiveTransfer Gateway, which acts as an intermediary between the Internet and the internal ActiveTransfer Server.
- ActiveTransfer web client, which provides access to ActiveTransfer Server to perform file transfers.

ActiveTransfer Server includes an Integration Server package called `WmMFT`, which enables ActiveTransfer Server to communicate with Integration Server and My webMethods Server.

The following diagram illustrates how these components typically interact:



For a summary of access points to configure for the components that ActiveTransfer connects to, see “ [ActiveTransfer Access Points](#)” on page 429.

The WmMFT Package

The WmMFT package is a standard Integration Server package that performs the following functions:

- Facilitates the interaction between Integration Server and ActiveTransfer Server. When the WmMFT package is enabled in Integration Server, the package starts automatically when you start Integration Server.
- Facilitates the interaction between My webMethods Server, which hosts the ActiveTransfer administration interface, and ActiveTransfer Server. My webMethods Server uses SAML authentication and web service calls to invoke WmMFT functionality to monitor file transactions and manage ActiveTransfer Server, ActiveTransfer Gateway, users, post-processing events, scheduled actions, and data files and folders in the virtual file system.
- Contains built-in services for executing predefined events and for configuring ActiveTransfer Server.

The ActiveTransfer OSGi Bundles

ActiveTransfer Server is implemented as a set of OSGi bundles within the Integration Server profile, which contain the implementation of the core features of ActiveTransfer. ActiveTransfer comprises the following OSGi bundles, typically available in the *Integration Server_directory \common\runtime\bundles\mft\eclipse* directory:

- com.softwareag.mft.launcher
- com.softwareag.mft.common
- com.softwareag.mft.proxy
- com.softwareag.mft.server
- com.softwareag.mft.service
- com.softwareag.mft.tunnel

Note:

The *Integration Server_directory \common\runtime\bundles\mft\eclipse* location might change depending on the product or fix installation process.

The ActiveTransfer Interfaces

ActiveTransfer offers the following interfaces:

- **My webMethods:** My webMethods Server hosts the administration interface for ActiveTransfer. Using the My webMethods interface, administrators can manage users, grant access permissions, configure the ActiveTransfer environment, and perform other administrative tasks.

webMethods ActiveTransfer is also accessible through a new user interface now. For complete information, see [“Working with the New User Interface” on page 229](#).

- **API:** Built-in services enable administrators to execute predefined events and configure ActiveTransfer Server.
- **Web client:** The ActiveTransfer web client enables users to access the ActiveTransfer Server to download, upload, and share files.

How does ActiveTransfer work with Trading Networks?

In the Software AG business-to-business (B2B) platform that includes webMethods Trading Networks, ActiveTransfer provides the managed file transfer facility while Trading Networks provides you the B2B capabilities of file (referred to as *documents* in Trading Networks) management and partner management, transaction monitoring, and so on.

Whether you have installed the ActiveTransfer and Trading Networks instances on the same Integration Server host (local installation) or different Integration Server hosts (remote installation), you can control B2B transactions end to end by using ActiveTransfer and Trading Networks as follows:

- **Configure partners only once and then synchronize.**

Configure partners only once—either in ActiveTransfer or Trading Networks. If Trading Networks is not installed, you can define your own partners when you edit virtual folders or user profiles in ActiveTransfer. If Trading Networks is installed, ActiveTransfer Server can retrieve the list of partners from Trading Networks. However, you must define the partner-user and partner-virtual folder associations separately in the two products.

Synchronization of partner information between the two products depends on the following parameter settings. For detailed information about these parameters, see [“Server Configuration Parameters and Variables” on page 399](#).

- `mft.partners.useTNPartners`. This parameter enables the use of Trading Networks partners configured in Trading Networks instead of ActiveTransfer partners.

Note:

To make any new Trading Networks partner available in ActiveTransfer, reload the `wmMFT` package or run the Integration Server service `wm.mft.assets.partner.syncPartnerProfiles`.

- `mft.aliases.tn`. When connecting to remote Trading Networks instances, this parameter lists all the remote Trading Networks server aliases. Local installations of ActiveTransfer and Trading Networks do not require this parameter to share partner information.
- `mft.group.aliases`. This parameter specifies the remote server aliases of ActiveTransfer nodes that are part of a group. The remote server aliases are defined in the Integration Server Administrator portal. ActiveTransfer instance shares asset information with other ActiveTransfer nodes in the group.

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.

■ Send files to Trading Networks.

Local installations of ActiveTransfer and Trading Networks instances do not require any specific configuration for file transfers to Trading Networks. In case of remote installations, ActiveTransfer requires the parameter `mft.aliases.tn` to send files to remote Trading Networks instances. In this parameter, specify the remote server aliases defined in Integration Server for the remote Trading Networks instances. For detailed information on `mft.aliases.tn`, see [“mft.aliases.tn” on page 400](#).

After configuring the required parameters, you can use the **Execute Trading Networks Service** event action to send files to Trading Networks for document processing. For details on the **Execute Trading Networks Service** event action, see [“Executing a Trading Networks Service” on page 173](#).

■ Receive files from Trading Networks.

Similar to file transfers Trading Networks, only remote installations of Trading Networks instances require a specific configuration—in Trading Networks, you must specify the remote server aliases defined in Integration Server for the remote ActiveTransfer instances. For details on how to configure remote ActiveTransfer server aliases in Trading Networks, see the Trading Networks documentation.

In Trading Networks, ActiveTransfer is available as a delivery method for file transfer (or *document delivery* in Trading Networks). For the ActiveTransfer delivery method, the Trading Networks partner must have a virtual folder. Then, when Trading Networks triggers a file transfer, ActiveTransfer sends the file to the target location in the virtual folder without creating a local copy.

For each file sent, Trading Networks and ActiveTransfer maintain different IDs by which to identify the file transfer. To help you identify Trading Networks file transactions, ActiveTransfer logs include the Trading Networks document ID as well as the ActiveTransfer transaction ID. However, the My webMethods Server user interface only displays the ActiveTransfer transaction ID. Also, in the My webMethods Server user interface, you can identify file transactions triggered in Trading Networks by using Trading Networks (**TN**) as the trigger source or the Trading Networks file name. For details on how to filter and find file transaction details, see [“Monitoring ActiveTransfer” on page 197](#).

Failover Support for File Transfer Operations

Failover support enables you to avoid a single point of failure in your file transfer operations. ActiveTransfer Server provides failover support in the following scenarios:

- Inbound File Transfer
- Outbound File Transfer

Inbound File Transfer

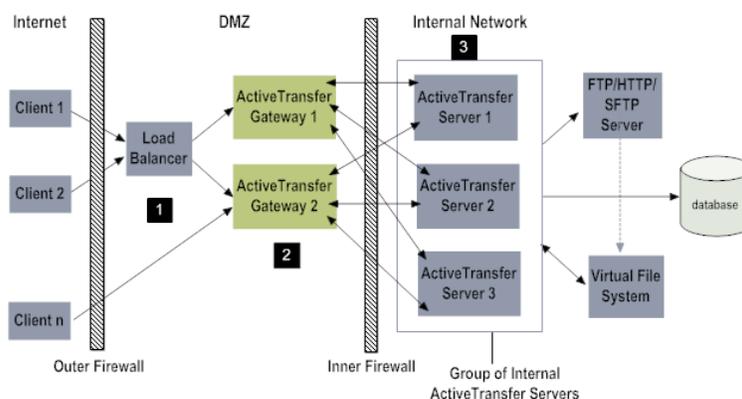
If an ActiveTransfer Server cannot handle a request, or becomes unavailable, the request is automatically redirected to another ActiveTransfer Server that is connected to the same ActiveTransfer Gateway.

Prerequisites to Configuring Failover Support for Inbound File Transfer

- All ActiveTransfer Server and Gateway nodes in the ActiveTransfer installation must run the same webMethods ActiveTransfer version, with the same fixes applied.
- All the ActiveTransfer Server nodes that are part of the *group* that will support failover of file transfer operations must connect to the same ActiveTransfer Gateway in the DMZ.
- All the ActiveTransfer Server nodes that are part of the group that will support failover of file transfer operations must connect to the same ActiveTransfer database.
- All the ActiveTransfer Server nodes that are part of the group that will support failover of file transfer operations must be able to access a common virtual folder location configured in the VFS.

How does Failover for an ActiveTransfer Server Work?

The following diagram illustrates how an ActiveTransfer client request is handled in failover mode:



Step	Description
1	External clients send file transfer requests to the ActiveTransfer Gateway, directly or through a load balancer.
2	ActiveTransfer Gateway then passes on the requests to the ActiveTransfer Server.
3	The ActiveTransfer Server processes the requests and sends responses to the ActiveTransfer Gateway. If one ActiveTransfer Server in a group fails during a file transfer operation, another ActiveTransfer Server takes over and completes the file transfer operation.

Note: ActiveTransfer does not support failover for post-processing events. If an ActiveTransfer Server goes down after the file transfer operation is completed, the post-processing event configured for the file transfer will not be executed by any other ActiveTransfer Server connected to the ActiveTransfer Gateway. If an ActiveTransfer Server goes down during the execution of a post-processing event, another ActiveTransfer Server connected to the ActiveTransfer Gateway will not resume the post-processing event.

ActiveTransfer Server Group

You can set up a group of ActiveTransfer Servers that share the same database to provide failover support for file transfers when one ActiveTransfer Server node in the group goes down. An ActiveTransfer Server group enables load balancing for incoming file transfer requests from clients. This setup, which is referred to as the *ActiveTransfer Server group*, is independent of Integration Server clustering. An ActiveTransfer Server group does not make use of the capabilities of an Integration Server cluster, except in the case of the Integration Server scheduler used for scheduled events. For an illustration of a setup that includes an ActiveTransfer Server group and a third-party load balancer, see [“How does Failover for an ActiveTransfer Server Work?” on page 21](#).

The ActiveTransfer Server group provides the following capabilities:

- Failover support for file transactions
- Session replication of ActiveTransfer client sessions using local cache
- Load balancing

The following information is stored in the database and shared between the ActiveTransfer Server nodes in a group:

- User details
- User authentication details (CDS database)
- Virtual folder definitions
- Post-processing and scheduled event configurations
- Server port details
- Transaction details

Session Replication

Session replication is useful when a client directly connects to a load balancer which in turn connects to ActiveTransfer Server. Session replication enables you to configure replication of an ActiveTransfer client session that is in progress on one node, across all other ActiveTransfer Server nodes in the group. A client connected to one ActiveTransfer Server in a group is valid on all other ActiveTransfer Servers in the group. So, if one ActiveTransfer Server goes down, the client is directed to another ActiveTransfer Server in the group and any in-progress file transfers can continue without the need for a client re-login. For configuration details, see [“Configuring Session Replication in ActiveTransfer Servers” on page 34](#).

Note that session replication is not required if the client connects directly to the ActiveTransfer Gateway which routes the requests to ActiveTransfer Server. In this case, ActiveTransfer Gateway automatically handles session replication between ActiveTransfer Servers.

Note: ActiveTransfer Server’s session replication only replicates data from client sessions. Changes to configuration data (for example: server preferences, user configuration) and runtime data (for example: list of IP addresses banned because of invalid logins) will not be replicated across the ActiveTransfer Server nodes.

Outbound File Transfer

An outbound file transfer is triggered by a scheduled event configured in the ActiveTransfer Server or when the ActiveTransfer Server directly invokes the `wm.mft.schedule:executeEventservice` service.

To configure failover support for outbound file transfers:

- In the copy or move action configuration on the Event Management page, select **Retry failed copies** and **Resume transfer from the point of interruption** options.

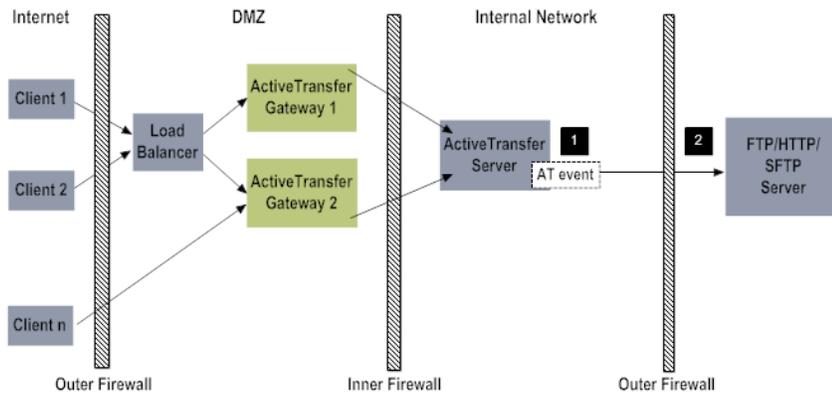
Select this option...	To...
Retry failed copies	Retry a failed copy or move operation for the specified number of times.
Resume transfer from the point of interruption	Resume an interrupted copy or move operation from the point of interruption.

For additional details, see [“Copying or Moving Files” on page 151](#).

- If you are transferring files by way of a virtual folder instead of directly connecting to an external server, configure the following additional options for the virtual folder in the **Administration > Integration > Managed File Transfer > Virtual Folder Management** page before you use the virtual folder in a move or copy action:
 - **High Availability Download Recovery**, if you want ActiveTransfer Server to recover from a download that was not completed.
 - **High Availability Upload Recovery**, if you want ActiveTransfer Server to recover from an upload that was not completed.

The High Availability Upload/Download Recovery options provide recovery from short drops in connections (30 to 60 seconds) during file transfers. ActiveTransfer Server maintains an internal buffer for the transfer-in-progress which is used for automatic retries to re-connect to the external server if the connection goes down. And, when the connection is re-established, ActiveTransfer Server resumes the file transfer from the point of failure. This automatic resume is triggered by ActiveTransfer Server without the intervention of the requestor ensuring uninterrupted file transfer. For additional details on configuring these options, see [“Associating a Virtual Folder with a Physical Folder Location”](#) on page 127.

The outbound file transfer scenario is shown in the following illustration:



Label	Description
1	A scheduled event configured in ActiveTransfer Server triggers a file transfer request to an external server.
2	The file transfer request is configured to transfer files to or from an external server, or transfer files to a virtual folder pointing to an external server configured in ActiveTransfer Server and pointing to an external server.

If the connection between an ActiveTransfer Server and a remote server goes down when a file transfer is in progress, ActiveTransfer provides failover support as follows:

- You can configure ActiveTransfer Server to try to re-establish the connection with the remote server. You can set the number of retries when you configure a copy or move action in a post-processing or scheduled event. The default value for the number of retries is `unlimited`. Once the connection with the remote server is established, you can configure the to resume file transfer from the point of failure or from the beginning.
- You can configure the High Availability Upload/Download Recovery options in a virtual folder. If selected, these settings provide automatic resume of interrupted file transfer requests from the point of failure. This process is triggered by in without the requestor’s knowledge or intervention.

Session Reuse

ActiveTransfer Server events reuse existing client sessions for remote server operations in their actions instead of creating new sessions for each remote operation. For example, a client session created by ActiveTransfer for a find action to fetch files from a remote server can be used later on by a copy or rename action for the same operation. This is achieved by caching the client sessions in ActiveTransfer Server. Session reuse reduces the load on the remote servers caused by multiple client logins. Session reuse improves the performance and scalability of ActiveTransfer Server. This capability is only available with ActiveTransfer Server 9.7 Fix 7 and higher.

Use of Special Characters in Search

My webMethods Server, which hosts the ActiveTransfer administration interface, 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.

2 Configuring webMethods ActiveTransfer

■ Before Configuring ActiveTransfer	29
■ Summary of Configuration Steps	29
■ ActiveTransfer License File	30
■ Configuring Database Settings	31
■ Configuring a MySQL Community Server Version 5.7 Database	32
■ Adding an ActiveTransfer Server Instance to My webMethods	32
■ Configuring Timeout for ActiveTransfer Server Web Service Responses	33
■ Configuring Session Replication in ActiveTransfer Servers	34
■ Replacing the Default SSL Certificate	34
■ User Certificate Mapping	35
■ Verifying the Location of Keystore Files for ActiveTransfer	36
■ Managing Proxy Server Aliases	37
■ Connecting to HTTP(S) Servers	40
■ Configuring ActiveTransfer to Send Emails	41
■ Configuring the Maximum Number Actions in an Event	42
■ Configuring and Managing Acceleration	42
■ Configuring MashZone NextGen	47
■ Starting and Stopping ActiveTransfer	51
■ Configuring Single Sign-On for ActiveTransfer User Interface	51

- Configuring Single Sign-On for ActiveTransfer through SAML 2.0 53
- Configuring Single Sign-On in the Configuration File 53
- Configuring Single Sign-On for ActiveTransfer Web Client 54

Before Configuring ActiveTransfer

Before you start performing the configuration tasks described in this chapter, make sure the following tasks are completed:

- Ensure that you have a valid license file for ActiveTransfer Server or ActiveTransfer Gateway. For details, see “ActiveTransfer License File” on page 30.
- Ensure that “[Administering ActiveTransfer with Command Central](#)” on page 227 and, optionally, ActiveTransfer Gateway are installed. For details, see *Installing Software AG Products*.
- Ensure that all ActiveTransfer Server and Gateway nodes in the ActiveTransfer installation run the same webMethods ActiveTransfer version, with the same fixes applied.
- Ensure that a database component for ActiveTransfer Server is created. For details, see the chapter on creating and dropping database components in *Installing Software AG Products*.

Note:

This step does not apply to ActiveTransfer Gateway.

- Ensure that central user management is configured in Integration Server to provide My webMethods users with access to ActiveTransfer. For details, see the chapter on configuring a central user directory or LDAP in *webMethods Integration Server Administrator's Guide*.
- Ensure that the correct SAML resolver location is specified for every Integration Server instance that communicates with My webMethods Server through the WmMFT package.

The default SAML resolver URL is `https://localhost:8585/services/SAML`. Integration Server stores this URL in the `watt.server.auth.samlResolver` server configuration parameter. For information about changing the SAML resolver URL, see *webMethods Integration Server Administrator's Guide*.

- If you want to use MySQL Community Server as your database, ensure that you install MySQL Community Server version 5.7 and complete the required configurations. For details, see “[Configuring a MySQL Community Server Version 5.7 Database](#)” on page 32.
- Ensure that My webMethods Server and Integration Server are started, in that order.

Summary of Configuration Steps

After you install ActiveTransfer, you must perform the following high-level steps to configure ActiveTransfer.

Note: Command Central also allows you to manage ports. For details on how to use Command Central to manage Active transfer, see “[Administering ActiveTransfer with Command Central](#)” on page 227.

1. Add an ActiveTransfer Server instance to My webMethods Server if the Integration Server that hosts ActiveTransfer Server is running on a machine other than “localhost” on port 5555. For details, see “Adding an ActiveTransfer Server Instance to My webMethods” on page 32.

2. Replace the default SSL certificate for ActiveTransfer instances used in production environments. For details, see “Replacing the Default SSL Certificate” on page 34.
3. Configure ActiveTransfer to send emails by editing the ActiveTransfer configuration properties file. For details, see “Configuring ActiveTransfer to Send Emails” on page 41.
4. Create server ports and configure settings for specific ActiveTransfer Server and ActiveTransfer Gateway instances. For details, see “[Managing ActiveTransfer Server](#)” on page 67 and *Managing File Transfers with webMethods ActiveTransfer Gateway*.
5. Create the users who will use ActiveTransfer to transfer files. For details, see “Working with Templates” on page 93 and “Managing Users, User Groups, and User Roles” on page 103.
6. Create a virtual file system (VFS) and grant access permissions and functional privileges to the folders within the VFS. For details, see “Managing Virtual Folders in a Virtual File System” on page 121.
7. Verify that the appropriate keystore files reside on the machines that host the ActiveTransfer Server or ActiveTransfer Gateway on which you are performing configuration tasks. For details, see “Verifying the Location of Keystore Files for ActiveTransfer” on page 36.
8. Include the IP addresses of the machines that run trusted applications in the unbanned list if these applications will send frequent requests to ActiveTransfer Server or ActiveTransfer Gateway. This is to ensure that these IP addresses are not automatically banned by the default banning settings of ActiveTransfer Server or Gateway. For details, see “mft.query.maxrows” on page 405
9. Configure and manage acceleration using My webMethods. For details, see “Configuring Tunnels for Acceleration” on page 43.
10. Define events that, when triggered, cause ActiveTransfer Server to perform a specified set of actions. For details, see “Managing Events” on page 137.
11. Set up the Software AG MashZone environment and connect the MashZone NextGen server to My webMethods Server. For details, see “Configuring MashZone NextGen” on page 47.
12. Grant non-administrator users the ability to access specific ActiveTransfer screens in My webMethods as necessary. For details, see “Granting Access to ActiveTransfer Pages in My webMethods ” on page 57.

For a summary of the ports and host names or IP addresses that ActiveTransfer uses, the products to which ActiveTransfer Server and ActiveTransfer Gateway connect, and the file paths used for virtual folders and file operations, see “ActiveTransfer Access Points” on page 429.

ActiveTransfer License File

You require a valid license file to install ActiveTransfer. During installation of ActiveTransfer, you are prompted to specify the location of the license file. Therefore, ensure that the license file is in a location that will be accessible during the installation, such as on the local file system. There are three types of ActiveTransfer license files:

- ActiveTransfer Server

- ActiveTransfer Gateway
- ActiveTransfer Agent

You will receive the license in the form of a XML file (for example, MAT97.xml). You can identify the ActiveTransfer license type by the viewing the product information in the license file.

ActiveTransfer Server:

```
<ProductCode>MAT</ProductCode>
...
<ProductName>ActiveTransfer Server</ProductName>
<ProductVersion>9.7</ProductVersion>
```

ActiveTransfer Gateway:

```
<ProductCode>MAP</ProductCode>
...
<ProductName>ActiveTransfer Gateway</ProductName>
<ProductVersion>9.7</ProductVersion>
```

For details of the ActiveTransfer Agent license, see *Managing File Transfers with webMethods ActiveTransfer Gateway*.

The license file (licenseKey.xml) is installed in the *Integration Server_directory* \instances\instance_name\packages\WmMFT\config folder when you install ActiveTransfer using Software AG Installer. ActiveTransfer checks the license file on startup and depending on the license file type installed, starts up as an ActiveTransfer Server or as an ActiveTransfer Gateway.

➤ To change the ActiveTransfer license file

1. Stop the ActiveTransfer instance.
2. Rename the new license file as licenseKey.xml. For example, rename MAT97.xml to licenseKey.xml.
3. Browse to *Integration Server_directory* \instances\instance_name\packages\WmMFT\config folder and replace the existing license file with the new file.
4. Start ActiveTransfer.

Configuring Database Settings

ActiveTransfer requires a database to store configuration and monitoring data.

When you install ActiveTransfer, you can specify database connection parameters. ActiveTransfer creates a JDBC Pool Alias as during installation and associates this to "ActiveTransfer" JDBC Functional Alias. The connection parameters (JDBC Pool Definition) can be modified after installation. For details on how to install ActiveTransfer, see *Installing Software AG Products*.

If you want to use MySQL Community Server version 5.7 as your database, you would need to perform a few additional steps as described in [“Configuring a MySQL Community Server Version 5.7 Database” on page 32](#).

Configuring a MySQL Community Server Version 5.7 Database

You can use MySQL Community Server version 5.7 as the database for JDBC connection pools.

➤ **To configure MySQL Community Server version 5.7**

1. Install MySQL Community Server version 5.7.
2. Configure the database driver for MySQL Community Server version 5.7 as described in *webMethods Integration Server Administrator’s Guide*.
3. If your ActiveTransfer Server and MySQL databases are in different time zones, set the following parameters when you configure the MySQL JDBC pools for ActiveTransfer:

- `useLegacyDatetimeTypeCode=false`
- `serverTimezone=MySQL Server Time Zone`

For example, if your ActiveTransfer time zone is Eastern Standard Time (EST) and your MySQL Server time zone is Central Standard Time(CST), the JDBC Pool URL should be:

```
jdbc:mysql://<myhost>:3306/<my  
database?useLegacyDatetimeTypeCode=false&serverTimezone=IST
```

For a list of supported time zones, see the MySQL JDBC connector documentation.

Adding an ActiveTransfer Server Instance to My webMethods

Note:

My webMethods Server is deprecated in versions 10.7 and 10.11 of ActiveTransfer Server. Beginning with 10.15, support for My webMethods Server is completely removed.

My webMethods Server, or a cluster of My webMethods Server instances, can connect to one or more instances of ActiveTransfer Server. Use this procedure to do the following:

- If the Integration Server that hosts ActiveTransfer Server is running on a machine other than “localhost” on port 5555, change the default host name or port of the Integration Server instance definition added to My webMethods.
- Add another ActiveTransfer Server instance to My webMethods, if necessary.

After you complete this procedure, a My webMethods user with access to multiple ActiveTransfer Server instances can select this ActiveTransfer Server instance on ActiveTransfer administration and monitoring pages.

Note:

For every user who logs on to My webMethods Server, My webMethods Server creates a session that expires only after the user logs off. Changes to ActiveTransfer instance configurations are not applied until the user logs off and the session ends.

➤ **To add an ActiveTransfer Server instance to My webMethods**

1. In My webMethods: **Administration > My webMethods > System Settings > ActiveTransfer Instances**.
2. In the ActiveTransfer **Instance Settings** panel, click .
3. Specify the following settings:

Field	Description
Instance Name	Name of the ActiveTransfer Server instance to connect to.
Host	Host name or IP address of the Integration Server that hosts the ActiveTransfer Server instance.
Integration Server Port	Port number of the Integration Server that hosts the ActiveTransfer Server instance.
Use SSL	Whether to use the Secure Sockets Layer protocol to secure communication between My webMethods and the ActiveTransfer Server instance.

4. Click **OK**.

Configuring Timeout for ActiveTransfer Server Web Service Responses

When a My webMethods Server user issues a request that requires access to ActiveTransfer Server data, My webMethods Server executes an ActiveTransfer Server web service on Integration Server for the purpose. On specific ActiveTransfer Server instances, use this procedure to configure how long My webMethods Server should wait for a response from ActiveTransfer Server web services before timing out the requested action.

1. In My webMethods: **Administration > My webMethods > System Settings > ActiveTransfer Instances**.
2. For the ActiveTransfer Server instance, click the **Edit ActiveTransfer Instance** icon.
3. In **Web Service Timeout**, type the number of seconds My webMethods Server should wait for a response from ActiveTransfer web services before timing out the requested action.

Configuring Session Replication in ActiveTransfer Servers

Use this procedure to enable session replication in a group of ActiveTransfer Server nodes.

1. Open the ActiveTransfer configuration properties file (properties.cnf), located in the *Integration Server_directory \instances \instance_name \packages \WmMFT \config* directory of one ActiveTransfer Server node.
2. Set the following server configuration parameters:
 - **mft.session.replication.enable:** Set this property to true to enable session replication in this ActiveTransfer Server node.
 - **mft.session.replication.address:** Provide the details of this ActiveTransfer Server node.
 - **mft.session.replication.other.nodes:** Provide the list of the ActiveTransfer Server nodes that will form a group with this ActiveTransfer Server node.

For more information about these parameters, see “Server Configuration Parameters” on page 400.

3. Save and close the properties.cnf file.
4. Repeat steps 1 to 3 for each ActiveTransfer Server node in the group.

Replacing the Default SSL Certificate

ActiveTransfer uses a default SSL certificate, installed with ActiveTransfer, for the following purposes:

- To facilitate communication between ActiveTransfer Server and ActiveTransfer Gateway
- To facilitate communication through SSL ports when specific SSL certificates are not configured for those ports

The default SSL certificate is adequate for demo or testing purposes. However, in production environments, Software AG strongly recommends replacing this default certificate with your own certificate.

1. Obtain an SSL certificate for your organization in JKS format. Save this certificate in the following directory on ActiveTransfer Server and, if you are using a gateway, ActiveTransfer Gateway:

Integration Server_directory \instances \instance_name \packages \WmMFT \resources

2. Open the ActiveTransfer security configuration file (security.cnf), located in the *Integration Server_directory \instances \instance_name \packages \WmMFT \config* directory, and update the following properties:

- **mft.ssl.privatekey.password:** Provide the private key password for the replacement default certificate.
- **mft.ssl.keystore.password:** Provide the keystore password for the replacement default certificate.
- **mft.ssl.certificate.file.name:** Provide the file name of the replacement default certificate.

3. Restart Integration Server.

Important:

Software AG strongly recommends restarting Integration Server now. Doing so deletes the password text strings from the security configuration file and enables you to restart Integration Server in the future without being prompted to supply the certificate passwords.

User Certificate Mapping

The *Certificate Mapping* feature in ActiveTransfer allows you to use the user-certificate mapping configured in Integration Server or in My webMethods to validate a client login based on the client certificate, and to fetch the user details associated with the certificate. This capability is only available with ActiveTransfer Server 9.7 Fix1 and higher.

Note:

If you configure the user-certificate mapping for a user both in Integration Server and My webMethods, the configuration in Integration Server takes precedence.

For additional details on certificate mapping, see *webMethods Integration Server Administrator's Guide* and *Administering My webMethods Server*.

Enabling ActiveTransfer Server to Use the User-Certificate Mapping in Integration Server or My webMethods

By default, ActiveTransfer Server uses the CN value in the client certificate as the user name for the client who logs in. To enable ActiveTransfer to use the user mapped to the certificate in Integration Server or My webMethods as the username, you must set the ActiveTransfer property, `mft.server.ssl.useSCertMap` in the `\packages\WmMFT\config\properties.cnf` file to `true`. This property can take the following values:

- `False` (default) ActiveTransfer Server considers the CN value in the certificate as the username.
- `True` ActiveTransfer Server looks for the user mapped to the client certificate in Integration Server or My webMethods and considers the same as the username.

ActiveTransfer Server needs the user corresponding to the certificate to fetch the virtual folders configured for the user. If the CN value in the certificate is used as the user, the administrator has the additional responsibility of creating users with the exact name as the CN value for the entire set of client certificates.

Note:

Ensure that the user to certificate mapping has been configured in Integration Server or My webMethods for the users who will log on to the ActiveTransfer Server configured as an SSL server. Use one of the following methods to configure the user to certificate mapping:

1. In Integration Server, **Security > Certificates > Configure Client Certificates**.
 - a. Specify the *Certificate Path* and *User*.
 - b. Click **Import Certificate**.
2. Alternatively, in My webMethods, **Administration > System-Wide > User Management > Certificates**.
 - a. Click **Add New Certificate**.
 - b. Browse to the *Certificate File*.
 - c. Specify the *Certificate Type*.
 - d. Click **Upload**.

Verifying the Location of Keystore Files for ActiveTransfer

A keystore file contains one or more pairs of a private key and signed certificate for its corresponding public key. Keystores provide added layers of security and are easier to use than maintaining keys and certificates in separate files. Keystore files should be strongly protected with a password and stored, either on the file system or elsewhere, so that they are accessible only to administrators.

You will be prompted to specify a keystore location when you configure the following settings:

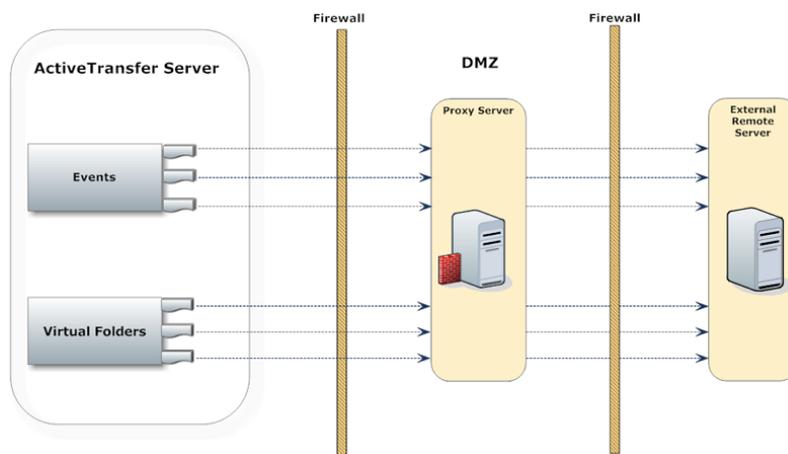
- SSL settings for an ActiveTransfer Server or ActiveTransfer Gateway port that uses the HTTPS or FTPS protocol, as described in “Specifying a Keystore File for a Port” on page 71.
- SSL settings for an ActiveTransfer Server or ActiveTransfer Gateway instance rather than for a specific port, as described in “Activating SSL Settings” on page 85.
- File-based encryption and decryption settings for an ActiveTransfer Server or ActiveTransfer Gateway instance, as described in “Activating File-Based Encryption and Decryption” on page 86.
- SSH settings for an ActiveTransfer Server port that uses the SFTP protocol, as described in “Setting RSA and DSA Encryption” on page 77.
- File-based encryption and decryption settings when configuring templates and users on ActiveTransfer Server, as described in “Specifying Encryption and Decryption Options at the Template Level” on page 100 and “Specifying Encryption and Decryption Options for a User” on page 117.

- The “encrypt” or “decrypt” file operation for an event configured on ActiveTransfer Server, as described in “Encrypting and Decrypting Files” on page 157.

Verify that the appropriate keystore files reside on the machines that host the ActiveTransfer Server or ActiveTransfer Gateway on which you are performing these configuration tasks.

Managing Proxy Server Aliases

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 full support for HTTP, HTTPS, and SOCKS proxy servers for protocols that support these proxy server types. The following diagram illustrates a typical proxy server setup in which ActiveTransfer transfers files to an external remote server.



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

File Transfer Protocol	Supported Proxy Server Type	ActiveTransfer Proxy Server Alias Type
FTP	SOCKS	SOCKS
SFTP	HTTPS	HTTPS
	SOCKS	SOCKS
HTTP	HTTP	HTTP
	SOCKS	SOCKS
HTTPS	HTTPS	HTTPS
	SOCKS	SOCKS

Set up proxy server aliases in the **My webMethods: Administration > Integration > Managed File Transfer > Proxy Management > Proxy Management** page. Each time you add, delete, or

modify proxy server aliases in the Proxy Management page, ActiveTransfer shares the changes with Integration Server, and the changes appear in **Integration Server Administrator > Settings > Proxy Servers**. Similarly, Integration Server shares proxy server aliases set up in Integration Server with ActiveTransfer. In ActiveTransfer, you can then associate virtual folders and configure event actions with the proxy server aliases. 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 file transaction details in the File Transaction page and event logs. For details on viewing file transaction details, see [“Viewing File Transaction Details” on page 199](#) and [“Monitoring Events” on page 201](#).

How to Use Proxy Server Aliases

ActiveTransfer supports proxy server alias in the following two scenarios.

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

In both these scenarios, you can either configure the VFS or event 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*.

You can set up single or multiple proxy server aliases for each file transfer protocol. However, you can designate only one proxy server alias as the default proxy server alias for a particular file transfer protocol. If you do not designate a default proxy server alias for a protocol, ActiveTransfer uses the Integration Server parameters, `watt.net.proxy.useNonDefaultProxies` and `watt.net.proxy.fallbackToDirectConnection`, to select the appropriate proxy server alias. The parameters which decide the proxy server aliases to use at run time are:

Parameter Location in...	Parameter Required and Description
--------------------------	------------------------------------

Integration Server	<code>watt.net.proxy.fallbackToDirectConnection</code>
--------------------	--

Set this parameter in *Integration Server_directory \ instances\instance_name\config directory\ cnfserver.cnf*.

The parameter determines how ActiveTransfer handles connections through proxy servers:

- *true*: ActiveTransfer establishes a direct connection to the remote server.
- *false*: ActiveTransfer treats the connection attempt as failed.

For information on the parameter, see *webMethods Integration Server Administrator's Guide*.

Parameter Location in...	Parameter Required and Description
Integration Server	<p><code>watt.net.proxySkipList</code></p> <p>Set this parameter in <i>Integration Server_directory \ instances\instance_name\config directory\ cnfserver.cnf</i>.</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> <p>For information on the parameter, see <i>webMethods Integration Server Administrator's Guide</i>.</p>
Integration Server	<p><code>watt.net.proxy.useNonDefaultProxies</code></p> <p>Set this parameter in <i>Integration Server_directory \ instances\instance_name\config directory\ cnfserver.cnf</i>.</p> <p>For information on the parameter, see <i>webMethods Integration Server Administrator's Guide</i>.</p> <p>The parameter determines how ActiveTransfer must handle the absence of default proxy sever aliases.</p> <ul style="list-style-type: none"> ■ <i>true</i>: ActiveTransfer selects any proxy server alias enabled for the protocol. ■ <i>false</i>: ActiveTransfer treats the connection attempt as failed.
ActiveTransfer	<p><code>mft.client.outbound.useProxy</code></p> <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. For more information on the parameter, see “mft.client.outbound.useProxy” on page 401.</p>

Adding a Proxy Server Alias

Use this procedure to add a proxy server alias for file transfers from and to remote servers through proxy servers. The proxy server alias you add here also appears in Integration Server Administrator > **Settings** > **Proxy Servers**.

For information on the use of proxy server aliases, see [“Managing Proxy Server Aliases” on page 37](#).

1. In **My webMethods: Administration > Integration > Managed File Transfer > Proxy Management**.
2. Above the proxy server alias list, click  at the top right corner.
3. In the Add Proxy Server Alias dialog box, provide the following details:

Field	Do this...
Alias	Type a suitable name for the proxy server alias.
Protocol	Select the file transfer protocol to which this proxy server alias applies.
Host IP Address	Type the host IP address for the proxy server..
Port Number	Type the port number to use for the proxy server alias.

4. Click **Add**.

The proxy server alias appears at the top of the proxy server alias list.

5. Select the proxy server alias in the list, and specify the following details:

Field	Do this...
User Name	Type the user name to connect to the proxy server.
Password	Type the password to connect to the proxy server.
Enable	Select this option to enable the proxy server alias.
Is Default	Select this option if you want ActiveTransfer to use this alias as the default proxy server alias for the particular file transfer protocol.

Note:

You can designate only one proxy server alias as the default proxy server alias for a particular file transfer protocol.

6. Click **Save**.

Connecting to HTTP(S) Servers

You can configure HTTP(S) servers in events and virtual folders. When connecting to remote HTTP(S) servers, ActiveTransfer works differently if the HTTP(S) server is an ActiveTransfer Server or a third-party HTTP(S) server as follows:

- **Third-party HTTP(S) server.** When connecting to third-party HTTP(S) servers, ActiveTransfer supports only upload and download file operations. Typically, third party HTTP(S) servers

do not support operations like file listing, renaming, moving, and so on. Due to this limitation, you cannot specify a third-party HTTP(S) servers in the virtual folder configuration, since virtual folders require support for all file operations.

However, you can specify a third party HTTP(S) server in an event for find and copy actions. If you use a third-party HTTP(S) server in an event action, the HTTP(S) URL specified in the action relates to a single file. Therefore, the event action works on a single file at a time.

- **ActiveTransfer HTTP(S) Server.** ActiveTransfer uses a custom method to communicate between each other using an agreed set of HTTP requests and response. Therefore, when ActiveTransfer connects to an ActiveTransfer HTTP(S) Server, all file operations are supported.

Connections to remote HTTP(S) servers also support the following features:

- **Streaming of data (chunking).** ActiveTransfer supports chunked transfer encoding in HTTP. In chunked transfer encoding, the data is sent as a series of "chunks". This enables ActiveTransfer to stream the data to an HTTP(S) server rather than sending the data in a single HTTP request, which is particularly helpful when handling large files. The Active transfer client streams the data to the server as soon as the data is available without waiting for the complete data to be available.

For upload or download, there is no limitation on the file size. However, the chunk size is determined by the Integration Server property `watt.net.httpChunkSize` and the default value is 8192. For more information about the property, see the "Server Configuration Parameters" chapter in *webMethods Integration Server Administrator's Guide*.

If the remote HTTP(S) server streams the file data that ActiveTransfer must download, ActiveTransfer downloads the file as chunks. File uploads presume that the HTTP(S) servers support chunking. ActiveTransfer sends the file data as chunks if you include the upload header `Transfer-Encoding` with the value `chunked` in the event configuration.

- **Multipart messages.** HTTP(S) servers expect data formatted as multipart messages. ActiveTransfer supports multipart messages out of the box for file upload to remote HTTP(S) servers. To send files formatted as multipart messages, include the upload header `Content-Type` with the value `multipart/form-data` in the event configuration.
- **Resuming file transfer from point of interruption.** When an upload or download operation fails while ActiveTransfer connects to an HTTP(S) server, ActiveTransfer resumes the operation from the point where the failure occurred. ActiveTransfer transfers (upload or download) only the remaining data (bytes) and skips the data that is already transferred.

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 381](#).

- 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 on configuring ActiveTransfer to send emails, see:

- [“Configuring the SMTP Server” on page 380](#)
- [“Configuring Default Email Settings in the User Interface” on page 380](#)
- [“Configuring Default Email Settings in properties.cnf” on page 381](#)
- [“Disabling Email Alerts” on page 382](#)

Configuring the Maximum Number Actions in an Event

By default, ActiveTransfer allows users to add a maximum of 20 actions in an event. You can increase this default limit to 50 actions using this procedure.

1. Navigate to the following location:

Integration Server_directory \MWS\server\default\deploy\portal.war\WEB-INF\

2. Using an XML editor, open the file `jetty8-web.xml`.
3. Locate the line `<Configure class="org.eclipse.jetty.webapp.WebAppContext">`.
4. Make the following edits:

- a. Change the default value 2000 for the property `maxFormKeys` as follows:

```
<Set name="maxFormKeys">4000</Set>
```

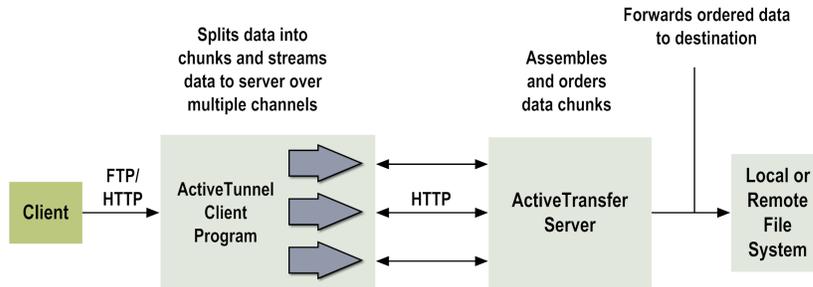
- b. In the next line, add the property `maxFormContentSize`:

```
<Set name="maxFormContentSize">2000000</Set>
```

Configuring and Managing Acceleration

Through the use of tunnels, ActiveTransfer provides the ability to conduct high-speed file transfer by dividing a single connection into many connections. Data is delivered in parallel through these tunnel connections and then reassembled and delivered to the intended destination.

The following diagram illustrates this process:



Any TCP connection that pushes data as fast as possible without internal verification of received amounts can be accelerated. Users connect to their own local host IP address, and the tunnel then routes the data over HTTP to ActiveTransfer Server, which forwards the data to the destination.

ActiveTransfer Server performs accelerated transfers by using a multiplier in the HTTP acceleration. As network latency increases, the maximum theoretical bandwidth of a connection decreases significantly. You can offset this decrease in bandwidth by configuring the HTTP tunnel multiplier needed to reach your maximum speed. For example, if the speed is 3 MB/sec and your bandwidth maximum is 50 MB/sec, entering a multiplier of 17 will give you the maximum acceleration. Entering a multiplier higher than 17 in this case is not beneficial because your Internet Service Provider still limits your maximum speed.

Configuring Tunnels for Acceleration

➤ To configure tunnels for acceleration

1. Define an ActiveTransfer Server tunnel. For details, see “Accelerating Data Transfer” on page 88.

Note:

If you are using an ActiveTransfer Gateway to accept client connections, you must define the tunnel on ActiveTransfer Server, not on the Gateway.

2. Add the following ports for ActiveTransfer Server to use internally as part of the tunneling process:
 - a. If you are using the FTP protocol for accelerated file transfers, add an FTP port numbered 55521 with an IP address of 127.0.0.1.
 - b. If you are using the HTTP protocol or the ActiveTransfer web client for accelerated file transfers, add an HTTP port numbered 55580 with an IP address of 127.0.0.1. The IP address and port number of the HTTP port are the same as the IP address and port number used in the tunnel definition for the server port.

If you are using an ActiveTransfer Gateway to route client requests to ActiveTransfer Server, configure these ports in the gateway. For details about adding ports, see “Adding a Port” on page 68.

3. Map the tunnel to one or more users to grant access to the tunnel. For details, see “Specifying Acceleration Options at the Template Level” on page 101 and “Specifying Acceleration Options for a User” on page 118.

If you do not map a tunnel to a user, and the user uses the advanced upload/download feature in the web client, the server will upload or download the files or folders at a normal, not an accelerated, rate of speed.

Using Acceleration

After you configure acceleration, users can accelerate their file transfers using one of three methods:

- **Web client.** For more information, see *webMethods ActiveTransfer Web Client User’s Guide*.
- **ActiveTunnel.jar file.** For more information, see “Accelerating File Transfers Using the ActiveTunnel.jar File” on page 44.
- **Java Network Launch Protocol (JNLP).** For more information, see “Accelerating File Transfers Using JNLP” on page 45.

Accelerating File Transfers Using the ActiveTunnel.jar File

Use this method if you are using the FTP protocol for accelerated file transfers.

You can integrate the ActiveTunnel process into an existing workflow using a standalone machine that acts as the tunnel provider using the ActiveTunnel.jar file. You can download this jar file from the WebInterface folder of ActiveTransfer Server using the following URL:

`http://host:port/WebInterface/ActiveTunnel.jar`

For example:

```
java -cp ActiveTunnel.jar com.softwareag.mft.tunnel2.Tunnel2 protocol=https  
host=localhost port=443 username=sag password=sag
```

Where:

- `protocol` is the either HTTP or HTTPS.
- `host` is the host (local or remote) to which to connect.
- `port` is the port to use to connect to the host.
- `username` is the user name to log on to the host.
- `password` is the user name to log on to the host.

The command starts the tunnel and defines it as a server that can handle both FTP and HTTP requests. The tunnel then passes the request to ActiveTransfer Server or ActiveTransfer Gateway.

You can also start a tunnel programmatically through your own code by including the ActiveTunnel.jar file in the code.

Accelerating File Transfers Using JNLP

Use this method if you are using the HTTP protocol for accelerated file transfers.

You can launch a specific tunnel from the command line using Java WebStart by way of the ActiveTunnel.jnlp file. You can download this JNLP file from the WebInterface folder of ActiveTransfer Server using the following URL:

`http://host:port/WebInterface/ActiveTunnel.jnlp`

Limitations of File Acceleration

The following limitations are observed with respect to file acceleration:

- If you enable the HTTP only security configuration by setting `HTTPOnly=true` in the `config.properties` file, file acceleration does not work. File acceleration in ActiveTransfer web client uses an applet which is blocked because you have enabled the `HTTPOnly` setting.
- If you enable CSRF security configuration by setting `csrf=true` in the `config.properties` file, file acceleration does not work.

Achieving Maximum Throughput for File Transfers using Acceleration

You can achieve maximum throughput using file acceleration when transferring large files on high latency connections such as the ones between inter-continental and cross-continental locations with the following techniques:

- Utilizing the network bandwidth to the maximum by varying the number of channels.
- Adjusting the **Minimum Fast Speed** and the **Minimum Slow speed** based on the one channel test.
- Adjusting the **Channels Ramp Up** value based on the **IN/OUT channels** set, and the performance of file acceleration.

Note:

These guidelines are applicable (have been tested) only for the inbound file transfer scenario in ActiveTransfer Server and in the case of file download using ActiveTransfer web client.

The acceleration parameters and their roles are listed in the table below:

Acceleration Parameter	Description
Basic Settings:	
IN Channels	Indicates the maximum number of inbound channels that can be opened in parallel to transfer one file.
OUT Channels	Indicates the maximum number of outbound channels that can be opened in parallel to transfer one file.

Acceleration Parameter	Description
Advanced Settings:	
Stability Interval	The time to monitor a stable average speed before adding new channels. By default, 1 channel is added after the speed is stable for 5 seconds.
Channels Ramp Up	Number of incremental channels added at one shot. Default is 1.
Minimum Fast Speed	Minimum speed that each channel should reach before a new channel can be added. Default value is 100Kb/sec.
Minimum Slow speed	Speed below which the channels are removed. By default, one channel at a time is removed at every interval 50Kb/sec.
Speed Threshold	Threshold speed to be reached before a new channel is added. Default value is 60%.

Setting Up the Channel Count

The IN and OUT channel counts are tuned based on the utilization of the hardware resources on the server machine. For example, in a network with 100 Mbps bandwidth and 150 ms latency, if we see a transfer rate of 48 Kbps with one channel, the network utilization is 0.5% of 100 Mbps. In this case, you will take around 400 minutes to transfer a 1 GB file. One solution to this issue is to set the **IN channels** to 200. This will increase the combined transfer rate to 9.37 Mbps (48 Kbps x 200 channels). With this new setting for **IN channels**, you will be able to transfer a 1 GB file in about 1 minute 49 seconds.

Increasing/decreasing the Minimum Fast Speed

You should make a note of the average transfer speed per channel and use that information to set the **Minimum Fast Speed**.

Increasing/Decreasing the Minimum Slow Speed

You should make a note of the minimum transfer speed per channel and use that information to set the **Minimum Slow Speed**.

Setting the Channels Ramp Up

You should decide on the **Channels Ramp Up** setting based on the number of IN/OUT channels. For example, if you set the **IN Channels** count to 100 channels and the **Channels Ramp Up** count to 10 for a file transfer, the channel count is ramped up in multiples of 10 which will help in achieving the required speed quickly. On the other hand, if for a **IN Channels** count of 20, if you set the **Channels Ramp Up** count to 10, you may not get the required speed. This setting might slow down the file transfer instead. A **Channel Ramp Up** value between 2- 4 channels will provide better results here.

Configuring MashZone NextGen

Before you can display ActiveTransfer analytical information in My webMethods, you must configure MashZone NextGen by performing the following high-level steps:

1. Configure MashZone NextGen and set up the dashboard for ActiveTransfer. For details, see “Setting Up the MashZone NextGen Environment” on page 47.
2. Connect the MashZone NextGen server to My webMethods Server so that analytical information can be viewed in My webMethods. For details, see “Connecting MashZone NextGen Server to My webMethods Server” on page 50.

For additional information about configuring MashZone NextGen and managing MashZone NextGen dashboards, see the MashZone NextGen documentation.

Setting Up the MashZone NextGen Environment

When you install ActiveTransfer using the Software AG Installer, the monitoring MashApps for ActiveTransfer Server are downloaded but are not installed on the MashZone NextGen server. Use this procedure to complete the configuration of MashZone NextGen.

> To set up the MashZone NextGen environment

1. Copy the necessary files to the MashZone NextGen installation as follows:
 - a. Copy the corresponding JDBC driver for your database to the directory:
MashZone_Installation_directory\MashZoneNG\mashzone\data\jdbcdrivers.
 - b. Copy the Red.less file from the directory *Integration Server_directory* \IntegrationServer\instances*instance_name*\packages\WmMFT\mashzone\columnchart to the directory: .

MashZone_Installation_directory\MashZoneNG\apache-tomcat\webapps\mashzone\hub\dashboard\assets\custom-look-and-feel\dashboard\default\columnchart
2. Update the XFrame-Options filters and content security policies in the MashZone NextGen directory using the contents of the ActiveTransfer file as follows:
 - a. Navigate to the directory *Integration Server_directory* \IntegrationServer\instances*instance_name*\packages\WmMFT\mashzone\security-filter
 - b. Using an XML editor, open the file applicationContext-security-filters.xml.
 - c. Copy the complete header content (all content within the open and close tags) for the following to a temporary file like a text file.

■ http pattern="/**/*.*.jsp" use-expressions="false"

- `http pattern="/hub/(login|reset_password)\.html.*" request-matcher="regex"`
 - `http pattern="/**/*.html" use-expressions="false"`
- d. In the copied header content, locate each instance of `otherServerHost:otherServerPort` and replace:
- `otherServerHost` with your My webMethods Server host name.
 - `otherServerPort` with your My webMethods Server Server port number.
- e. Close the `applicationContext-security-filters.xml` file.
- f. Navigate to the directory
`MashZone_Installation_directory\MashZoneNG\apache-tomcat\webapps\mashzone\WEB-INF\classes.`
- g. Open the file `applicationContext-security-filters.xml`.
- h. Replace the following header content (all content within the open and close tags) with the corresponding header content that you copied and edited earlier:
- `http pattern="/**/*.jsp" use-expressions="false"`
 - `http pattern="/hub/(login|reset_password)\.html.*" request-matcher="regex"`
 - `http pattern="/**/*.html" use-expressions="false"`
- i. Save and close the `applicationContext-security-filters.xml` file.
3. Start the MashZone NextGen server.
4. Browse to the MashZone NextGen welcome page `http://host:8080/mashzone`, and log on as a system user.

The default system user name and password are `Administrator` and `manage`, respectively.

5. Depending on the system directory you use to store user credentials, do the following
- By default, ActiveTransfer uses the My webMethods Server system directory. If you use the My webMethods Server system directory to store user profiles, create a matching user profile in MashZone NextGen for each user who has the permission to view or manage ActiveTransfer analytical information as follows:
 1. In the MashZone NextGen welcome page, click **Administrator > Admin Console**.
 2. On the Admin Console page, click **Users & Groups > Users**.
 3. Click **Add new user**.
 4. Specify the login ID defined for the user in My webMethods Server and other relevant details.

5. Click **Add this user**.

- Instead of the My webMethods Server system directory, if you use LDAP as your central user profile repository, integrate your LDAP directory with Software AG MashZone NextGen.

For details on how to integrate your LDAP repository with MashZone NextGen, see the MashZone NextGen documentation.

6. In the MashZone NextGen, Admin Console page, add user groups and associate users with the user groups, as required.

For details on how to add user groups and associate users to user groups, see MashZone NextGen documentation.

Tip:

Instead of specifying privileges for each user individually, define privileges for multiple users at a time by creating a user group, and then associating users with the group.

7. Import the ActiveTransfer analytics dashboard into MashZone NextGen by using the following command at the command prompt:

- a. Navigate to the directory *Integration Server_directory* \IntegrationServer\instances\default\packages\WmMFT\mashzone\dashboard.
- b. Copy the file *ActiveTransfer_Analytics_Dashboard.zip* to any location on your local machine.
- c. Navigate to the directory *MashZone_Installation_directory* \MashZoneNG\prestocli\bin.
- d. Open the command prompt and run the following command:

```
padmin importDashboard -l http://host:port/mashzone -f Location of
ActiveTransfer_Analytics_Dashboard.zip -u Administrator -w manage -o
```

8. Define a data source in MashZone NextGen to the ActiveTransfer database as follows:

- a. On the Admin Console page, click **JDBC Configuration > Data Sources**.
- b. Click **Add data source**.
- c. In **Data Source Name**, type MFTDB, the name of the ActiveTransfer database.

For the ActiveTransfer analytics dashboard to work, the MFTDB database is mandatory.

d. Specify other relevant details for the ActiveTransfer database component.

Provide a normal JDBC URL in the **JDBC URL** field instead of providing the URL in the webMethods format.

- e. Click **Save Changes**.
 - f. To test the database connection, click .
9. Share the dashboard with the users or groups you defined previously as follows:
- a. On the MashZone NextGen welcome page, open the **ActiveTransfer Analytics** dashboard.
 - b. In the menu, click  > **Manage > Permissions**.
 - c. In the Manage dashboard permissions dialog box, select view or edit permissions for the user or group.
 - d. Click **Save**.
10. Add the following parameter in the *Integration Server_directory* \profiles\MWS_default\configuration\custom_wrapper.conf file:
- ```
wrapper.java.additional.n =
-Dcom.webmethods.content.security.hosts="MashZone_host:MashZone_port"
```
11. Restart My webMethods Server.

**Postrequisite:**

[“Connecting MashZone NextGen Server to My webMethods Server” on page 50](#)

## Connecting MashZone NextGen Server to My webMethods Server

MashZone NextGen dashboards for ActiveTransfer only work with My webMethods Server. Before you can view analytical information in My webMethods, you must connect the MashZone NextGen server to My webMethods Server.

➤ **To connect MashZone NextGen server to My webMethods Server**

ActiveTransfer

1. In My webMethods: **My webMethods > System Settings > ActiveTransfer Instances**.
2. In the **MashZone Server Settings** window, click the  button to add a MashZone NextGen server.
3. In the **Add MashZone Server Configuration** dialog box, type the following in the respective field text boxes:

- The name of the MashZone NextGen server.
- The host name and port of the machine on which MashZone NextGen is installed.

If you want to use the SSL port specified during MashZone installation, select the **Use Secure Connection** check box.

4. In the **ActiveTransfer Instance** list, select the appropriate ActiveTransfer Server.
5. Click **Save**.

Navigate to My webMethods: **Monitoring > Integration > Managed File Transfer > Analytics** to view the MashZone NextGen page for ActiveTransfer.

## Starting and Stopping ActiveTransfer

ActiveTransfer has several components hosted in Integration Server runtime, including the WmMFT package and ActiveTransfer OSGi bundles. By default, when Integration Server starts and stops, ActiveTransfer also starts and stops. However, you can also start and stop ActiveTransfer separately.

From the **Packages** menu in the Integration Server, you can perform the following operations:

- Disable the WmMFT package to control ActiveTransfer separately from the Integration Server startup and stop processes.
- Start or stop the WmMFT package to start or stop ActiveTransfer. This ensures that all the ActiveTransfer OSGi bundles in the correct sequence.

For details on how to use Integration Server Administrator, see the *webMethods Integration Server Administrator's Guide*.

You can also use Command Central to start and stop the WmMFT package. For details, see [“Administering ActiveTransfer with Command Central” on page 227](#) and *Software AG Command Central Help*.

## 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/<br>TestSAML/protocol/saml/descriptor/<br><br>Or<br><br>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.

## Configuring Single Sign-On for ActiveTransfer through SAML 2.0

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.

You can configure Single Sign-On for ActiveTransfer using:

### Configuring Single Sign-On in the Configuration File

➤ To enable SSO for ActiveTransfer Web Client in `properties.cnf` configuration file

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 Single Sign-On checkbox in the Server Management page for the port.
3. Create a WebSSO configuration file in the Integration Server\ *instances* \default\packages\WmMFT\config\sso

**Note:**

You can also provide the configuration filename that represents the port number. For example, *websso\_2343.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   | 2343                                                                  |
| SSO_SP_ENDPOINT_URL  | https://localhost:2343                                                |
| SSO_IDP_METADATA_URL | https://localhost:8443/auth/realms/TestSAML/protocol/saml/descriptor/ |

Or

| Key                        | Key value                                 |
|----------------------------|-------------------------------------------|
|                            | 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 Single Sign-On for IDP initiated login, then add the property, SSO\_IDP\_INITIATED\_REDIRECT\_URI for the file (*websso\_2343.properties*.) with the IDP initiated URL. For example, SSO\_IDP\_INITIATED\_REDIRECT\_URI= https://idp.machine/adfs/ls/idpinitiatedsignon.aspx.
- When you configure 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, then copy the content of the hosted IDPMetadata XML 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.

## Configuring Single Sign-On for ActiveTransfer Web Client

### ➤ To enable SSO for ActiveTransfer Web Client

1. Enable the system property, `mft.server.https.auth.samlto true` in the *Integration Server\_directory* \instances\ *instance\_name* \packages\WmMFT\config\properties.cnf file.
2. Configure the redirection URI, the ActiveTransfer Server URL that you provided when registering with the identity provider in the `mft.server.https.auth.saml.redirecturi` property. For example, `https://idp.machine/adfs/ls/idpinitiatedsignon.aspx`.
3. The public key from the IDP server must be configured to the web client. Configure the profiles for SAML under the Security Infrastructure (SIN). You can configure the security properties that are set during server startup. The configuration file `com.softwareag.sso.pid.properties`

is located in the *Software AG\_directory/profiles/profile/configuration/com.softwareag.platform.config.propsloader* directory. The default configuration is as shown below:

```
com.softwareag.security.idp.keystore.keyalias=ssos
com.softwareag.security.idp.SSOassertion.lifetime=5
com.softwareag.security.idp.keystore.type=JKS
com.softwareag.security.idp.assertion.skew=30
com.softwareag.security.idp.truststore.location=/common/conf/
platform_truststore.jks
com.softwareag.security.idp.truststore.password=manage
com.softwareag.security.idp.keystore.location=/common/conf/keystore.jks
enabled=false
com.softwareag.security.idp.keystore.password=manage
com.softwareag.security.idp.truststore.keyalias=ssos
com.softwareag.security.idp.assertion.lifetime=300
com.softwareag.security.idp.truststore.type=JKS
```

The downloaded key from the IDP server must be included in the location, `com.softwareag.security.idp.truststore.location`

**Note:**

SIN searches for `com.softwareag.security.idp.truststore.keyalias` to load the alias. If a user wants to configure more than one alias, then do not set any value to this property.

4. Verify the configured SSO truststore and add the public key from the identity provider to the truststore and restart ActiveTransfer Server.
5. In the Server Management page, **Ports** tab, select an HTTPS listener for which you want to enable SSO.

**Note:**

SSO is supported only for HTTPS protocol.

- a. In the **SSO Options** section of the **Advanced** tab, select the **Support Single Sign-On login** option.

The HTTPS host name and port (for example: `https://localhost:234`) is now enabled for SSO in ActiveTransfer Web Client.



# 3 Granting Access to ActiveTransfer Pages in My webMethods

---

- Overview ..... 58
- Defining Roles ..... 58
- Adding My webMethods Users to the MFT Administrators Role ..... 59
- Granting a Role the Ability to Access an ActiveTransfer Server Instance ..... 59
- Associating an Existing My webMethods Server Role with ActiveTransfer ..... 59
- Granting or Denying Access to Specific ActiveTransfer Pages in My webMethods ..... 60
- Granting the Authority to Execute ActiveTransfer Services ..... 61

## Overview

---

My webMethods Server provides control of access permissions at both the user and the role level. You can specify which parts of the ActiveTransfer interface are available to specific users, user groups, or roles, and the functions that each user, user group, or role is allowed to execute.

Using these permissions, you grant access to ActiveTransfer pages in My webMethods, typically based on the role membership of My webMethods users. By default, My webMethods users have no access to ActiveTransfer pages.

To grant access, you must:

1. Create a My webMethods user account.
2. Define any custom roles you want to create for the user.
3. Grant permissions to any custom roles you have created.
4. Add the user or user group as a member of one or more ActiveTransfer roles.

The default My webMethods role for ActiveTransfer is as follows:

| <b>My webMethods Server Role</b> | <b>Corresponding ACL</b> | <b>Description</b>                                                                                                                       |
|----------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| MFT Administrators               | MFTAdmins                | These users can view all ActiveTransfer pages and perform all ActiveTransfer actions. You manually add My webMethods users to this role. |

When you first start Integration Server and ActiveTransfer Server after configuring central user management, ActiveTransfer automatically adds the MFT Administrators role to the Allowed list of the MFTAdmins ACL.

## Defining Roles

---

Defining roles for users consists of the following tasks:

- Creating a My webMethods user account for the user
- Defining roles to which you will grant access to ActiveTransfer pages
- Adding My webMethods users or user groups to the roles

### **Important:**

A user configured with the MFT Administrators role has the same privileges as a system user. The ActiveTransfer system owner should set appropriate file access rights for the user with the MFT Administrators role.

## Adding My webMethods Users to the MFT Administrators Role

To grant a My webMethods user the authority to access ActiveTransfer pages, you must add the user to the MFT Administrators role. You can accomplish this by doing either of the following:

- Add the user to the MFT Administrators role.
- Add the group to which the user belongs to the MFT Administrators role.

## Granting a Role the Ability to Access an ActiveTransfer Server Instance

Users can connect to multiple ActiveTransfer Servers in My webMethods. On every My webMethods page that requires access to ActiveTransfer data, users can select the ActiveTransfer Server instance on which they would like to perform the requested action. You grant this access to a role by adding the role to the list of allowed roles for an ActiveTransfer Server instance.

### ➤ To grant a role the ability to access an ActiveTransfer Server instance

1. In My webMethods: **Administration > My webMethods > System Settings > ActiveTransfer Instances**.
2. Click the **Permissions** icon for the ActiveTransfer Server instance you want to work with.

**Note:**

If no ActiveTransfer Server instances are listed, you can add one. For details, see [“Adding an ActiveTransfer Server Instance to My webMethods” on page 32](#).

3. In the **Select Roles** dialog box, type text that exists in the names of the roles you want, and then click **Search**.
4. Move the roles to which you want to grant access from the **Available** list to the **Selected** list.
5. Click **Apply**.

## Associating an Existing My webMethods Server Role with ActiveTransfer

Use this procedure to associate user role already defined in My webMethods Server withActiveTransfer. Similar to user association, once associated with ActiveTransfer, you can perform any of following operations on roles:

- Specify throttling options.
- Specify restrictions for server access, file actions, login volume, and so on.
- Specify encryption and decryption options.

- Specify acceleration options.

For details on inheritance of permissions, see [“Inheritance of Permissions and Settings in Groups and Roles” on page 104.](#)

➤ **To associate an existing My webMethods Server role with ActiveTransfer**

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users.**
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64.](#)
3. Click **Role.**
4. Click the  button above the list of roles.
5. In the **Add Role** dialog box, enter the search criteria in the **Search Role** box and click **Search.**
6. In the search results, select the check box next to the role that you want to associate with ActiveTransfer and click **Select Role.**

**Note:**

You can continue to add more user groups to the selected roles' list.

7. Click **Add.**

ActiveTransfer Server lists the roles in the Role page. and lists the user on the Users page.

**Tip:**

To delete a role, select the role and click . This action does not delete the role from the system directory or from the external directory service. Rather, it removes the association between the role and ActiveTransfer.

## Granting or Denying Access to Specific ActiveTransfer Pages in My webMethods

---

You can grant or deny access to specific My webMethods pages that a user or role can access. Examples include the following:

- You might want to grant another user selected administrative privileges. For example, you might want that user to be able to manage ActiveTransfer and Software AG MashZone servers and their settings. To do so, you must grant access to the **Administration > My webMethods > System Settings > ActiveTransfer Instances** page.
- Users in an operations analyst role would be interested in examining file transaction details and viewing analytics information. Users in this role would not be performing ActiveTransfer

administrative tasks. Therefore, you would grant the role access to the File Transactions and Analytics pages, and you would deny access to the ActiveTransfer administration pages.

### ➤ To grant or deny access to specific ActiveTransfer pages in My webMethods

1. In My webMethods:**Administration > System-Wide > Permissions Management**.
2. On the **Advanced** tab on the Search panel, select **webMethods Applications** from the **Resource Type** list and click **Search**.
3. Move **webMethods Applications** from the **Found** list to the **Selected** list and click **Next**.
4. In the Manage Permissions panel, click **Add**.
5. In the **Add Principals** dialog box, search for and select one or more My webMethods users or roles to which you want to grant access.
6. Click **Add**.
7. In the Permissions panel, click the **Grant** check box for the ActiveTransfer pages you want the user or role to access, and click the **Deny** check box for the pages you do not want the user or role to access.
8. In the Manage Permissions panel, click **Apply**.

#### **Important:**

Be sure to perform this step to assure that the permission is granted.

## Granting the Authority to Execute ActiveTransfer Services

When a My webMethods user issues a request that requires access to ActiveTransfer data, My webMethods Server executes an ActiveTransfer service on Integration Server to perform the requested action, and then displays the results in My webMethods. To execute the service, My webMethods Server uses the credentials of the user. The My webMethods user must, therefore, have the authority in Integration Server to execute the service.

In Integration Server, ActiveTransfer services are protected by the MFTAdmins ACL. For My webMethods users to be able to execute the services, the users must belong to the MFT Administrators role. However, you must still grant the user's role the appropriate permissions to My webMethods pages, as described in [“Granting or Denying Access to Specific ActiveTransfer Pages in My webMethods ” on page 60](#).

#### **Note:**

If you want users to be able to execute ActiveTransfer services from Software AG Designer, the users must be a member of the MFTAdmins ACL in Integration Server.



# 4 Preparing to Manage and Monitor ActiveTransfer Server in My webMethods

---

- Overview ..... 64
- Selecting the Instance to Work With ..... 64
- Searching for Items and Managing Search Results ..... 64

- “Overview” on page 64
- “Selecting the Instance to Work With” on page 64
- “Searching for Items and Managing Search Results” on page 64

## Overview

---

Many of the My webMethods pages on which you perform ActiveTransfer administrative and monitoring tasks share a common way of selecting server instances to work with and displaying and managing search results. This chapter describes the steps to perform these common tasks.

For additional information about the My webMethods user interface, see *Working with My webMethods*.

## Selecting the Instance to Work With

---

The ActiveTransfer administrative and monitoring tasks you perform in My webMethods require you to first select the ActiveTransfer Server, ActiveTransfer Gateway, or Software AG MashZone server instance you want to work with.

### > To select the instance to work with

1. At the top left of the ActiveTransfer **Server Management** page in My webMethods, click the name of the current instance.
2. If you are working with the Analytics page to view ActiveTransfer analytical information, select the Software AG MashZone server instance you want to work with.
3. If you are working with the Server Management page to change the configuration of an ActiveTransfer Server or ActiveTransfer Gateway instance, do the following:
  - a. From the **ActiveTransfer Instances** list, select the ActiveTransfer Server instance you want to work with.
  - b. If you are working with an ActiveTransfer Gateway instance defined for the selected ActiveTransfer Server, select the instance from the **ActiveTransfer Gateway Instances** list.
  - c. Click **OK**.
4. If you are working with any other ActiveTransfer administration or monitoring page, select the ActiveTransfer Server instance you want to work with.

## Searching for Items and Managing Search Results

---

The following ActiveTransfer pages display search results in a table at the top of the page.

|                                                                                |                                                                                                           |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>ActiveTransfer Page</b>                                                     | <b>Navigation Path in My webMethods</b>                                                                   |
| Server Management<br>( <b>Ports, Acceleration,</b><br>and <b>Gateway</b> tabs) | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; Server Management</b>                  |
| Templates                                                                      | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; User Management &gt; Templates</b>     |
| Users                                                                          | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; User Management &gt; Users</b>         |
| Event Management                                                               | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; Event Management</b>                   |
| File Transactions                                                              | <b>Monitoring &gt; Integration &gt; Managed File Transfer &gt; File Transactions</b>                      |
| Agents                                                                         | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; Agent Management &gt; Agents</b>       |
| Agent Groups                                                                   | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; Agent Management &gt; Agent Groups</b> |
| Agent Events                                                                   | <b>Administration &gt; Integration &gt; Managed File Transfer &gt; Agent Management &gt; Agent Events</b> |
| Agent Event Log                                                                | <b>Monitoring &gt; Integration &gt; Managed File Transfer &gt; Agent Event Log</b>                        |
| Agent Activity Log                                                             | <b>Monitoring &gt; Integration &gt; Managed File Transfer &gt; Agent Activity Log</b>                     |

You can search for a specific port, template, user, event, or file transaction. You can also set the number of rows to display in the search results list, select the columns to display in the table, and export the list details to a CSV file.

**Note:**

Not all of the features described in the following procedure are available for all items.

➤ **To search for items and manage search results**

1. If you want to search for a port, template, user, or event, type the first few letters of the item name in the **Search** box. The search results lists dynamically populates with the items that match your search criteria.

**Tip:**

For users, you can type the first few letters of the user's first name, last name, or user ID. Alternatively, you can click the arrow to the right of the search box and enter the search criteria in the appropriate box.

**Note:**

This step does not apply to file transactions. For file transactions, you must populate the search results table by specifying filter criteria. For details, see [“Monitoring File Transaction Activity” on page 198](#).

2. If you want to set the number of rows to display in the search results list, click  and select the appropriate number of rows in the **Table Options** dialog box.
3. If you want to select the columns to display in the table, click  and do the following:
  - a. Select the **Configure Table** option from the list.
  - b. Select the columns to display or hide.
  - c. Click **OK**.
4. If you want to export the list details to a CSV file, click , select the **Export Table** option in the **Table Options** dialog box, and do the following:
  - a. From the **Character Encoding** list, select the appropriate character encoding for the exported data.
  - b. Click **Export**.
  - c. Specify where to save the file. The exact method depends on the browser you are using.

**Note:**

In case of file transactions, change the search criteria to limit the search results to a reasonable number. If the number of file transactions is extremely large, export fails.

5. If you want to refresh the list, click .

# 5 Managing ActiveTransfer Server

---

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| ■ Managing ActiveTransfer Ports .....                                     | 68 |
| ■ Setting Passive FTP Mode for ActiveTransfer Server .....                | 72 |
| ■ Configuring a FTP Port to Support Implicit and Explicit SSL .....       | 73 |
| ■ Configuring an HTTPS Port to Support Single Sign-On .....               | 74 |
| ■ Configuring the Certificate Revocation List for secure ports .....      | 74 |
| ■ Setting the Command Delay Interval .....                                | 75 |
| ■ Setting the Encryption Method for ActiveTransfer Server .....           | 75 |
| ■ Setting SSH Encryption Algorithm, Ciphers, and Connection Options ..... | 76 |
| ■ Setting Throttling Options .....                                        | 80 |
| ■ Setting Server Restrictions .....                                       | 80 |
| ■ Banning IP Addresses .....                                              | 82 |
| ■ Specifying Encryption Settings .....                                    | 84 |
| ■ Accelerating Data Transfer .....                                        | 88 |
| ■ Configuring Miscellaneous Settings .....                                | 89 |

## Managing ActiveTransfer Ports

---

You can configure ActiveTransfer Server to listen on one or more ports. Each port is associated with a protocol. Clients can connect to ActiveTransfer Server using configured ports to transfer files and to execute other commands, such as obtain a directory listing. For example, if you create port 21 with the FTP protocol, clients can connect to ActiveTransfer Server through port 21 using any standard FTP client, and then transfer files or execute FTP commands.

You can create any number of ports for a protocol. Each port you create will start a listener in ActiveTransfer Server that waits for client connections.

You create and manage ports on the Server Management page in My webMethods. On this page, the settings on the **Ports** tab are specific to each port associated with the ActiveTransfer Server instance, whereas the settings on the **Throttling, Restrictions, Banning, Encryption, and Miscellaneous** tabs are general and apply to all ports associated with the server instance.

**Note:**

ActiveTransfer Server does not share ports with ActiveTransfer Gateway. If you want a Gateway instance to listen to any ports, add the ports to the gateway instance.

## Adding a Port

➤ **To add a port**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance.  
  
For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, click the **+** button to add a new port to the instance.
4. In the **Add a Port** dialog box, type the **Name** you want to give the port.
5. From the **Protocol** list, select the appropriate protocol (for example, HTTP).
6. Type the **Host IP Address** and **Port** values.

**Note:**

Make sure that the port you specify is not being used by any application, including the default ports used for ActiveTransfer Server and ActiveTransfer Gateway (2080 and 8500, respectively).

7. Click **OK**.

8. To refresh the server listing page, click the **Refresh** button in the upper right of the Server Management page.

The port information appears in the table on the **Ports** tab.

## Starting, Stopping, or Restarting a Port

### > To start, stop, or restart a port

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select the port from the list of ports.
4. To start, stop, or restart the port, in the **Status** section of the **Basic** tab, click the appropriate button.

## Checking the Status of a Port

### > To check the status of a port

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select the port from the list of ports.
4. In the **Status** section of the **Basic** tab, click **Check Status**.

#### Note:

It is possible that a client cannot connect to ActiveTransfer Server or transfer files even when a port 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. In such a situation, enable the **Router/Firewall Aware** option. For details, see [“Setting Passive FTP Mode for ActiveTransfer Server ” on page 72](#).

## Activating or Deactivating a Port

### > To activate or deactivate a port

**Note:**

When you start or stop a port, the port is started or stopped only on that ActiveTransfer Server or ActiveTransfer Gateway instance. However, when you activate or deactivate a port, the port is started or stopped on all ActiveTransfer Server instances or that specific ActiveTransfer Gateway instance.

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select the port from the list of ports.
4. In the **Settings** section of the **Basic** tab, select or deselect the **Activate port** check box to activate or deactivate the port respectively.

When you activate or deactivate a port, ActiveTransfer starts or stops the port in all the ActiveTransfer Server instances and or this specific ActiveTransfer Gateway instance.

5. Click **Save**.

## Deleting a Port

### ➤ To delete a port

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select the port from the list of ports.
4. Click the  button.
5. Click **OK** in the confirmation dialog box to delete the port.

## Including Port Information in User Emails

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

### ➤ To include port information in user emails

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select the port from the list of ports.
4. In the **Settings** sections below the port list, select the **Include this information in the user credentials email** check box.
5. Click **Save**.

## Specifying a Keystore File for a Port

Use this procedure to specify a keystore file for a port that uses the FTP, FTPS, HTTP, or HTTPS protocol. This keystore file overrides any global SSL encryption settings that apply to all ports on the server. For information about specifying global SSL encryption settings, see [“Specifying Encryption Settings” on page 84](#).

### ➤ To specify a keystore file for a port

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select an FTP, FTPS, HTTP, or HTTPS port from the list of ports.
4. Click the **Advanced** tab.

**Note:**

The remaining steps in this procedure pertain to the **SSL Options** section.

5. For **Keystore Location**, specify the path to the keystore file.

**Note:**

For an ActiveTransfer Gateway, specify the path of the server on which ActiveTransfer Gateway is running.

6. In the **Keystore Password** box, type the keystore password.
7. In the **Private Key Password** box, type the private key password.
8. If you want to allow connections only for clients with a valid client certificate, select **Require valid client certificate**.

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.

For details on how to map client certificates to users, see [“User Certificate Mapping” on page 35](#).

When establishing a connection with the server, ActiveTransfer validates only the client certificate but not the password.

**Tip:**

To store valid certificates:

- a. Create a truststore file in the same location as the keystore file named *keystoreName\_trust*. For example, if the keystore file name is *server\_ks.jks*, the truststore file name should be *server\_ks.jks\_trust*.
  - b. Add the valid client certificates to this truststore.
9. If you want ActiveTransfer to validate both the client certificate and the password when establishing a connection with the server, select **Require valid client certificate and password**.

Additionally, when you select this option for an HTTPS port, ActiveTransfer clears the selection of **Support Single Sign-On**.

For details on the single sign-on option for HTTPS ports, see [“Configuring an HTTPS Port to Support Single Sign-On” on page 74](#).

10. Click **Save**.

## Setting Passive FTP Mode for ActiveTransfer Server

---

ActiveTransfer Server can work in both active and passive FTP modes.

In active mode, the server creates an outgoing connection through the specified port to the client machine for data transfer as specified in the FTP commands issued by the client.

In some cases, such as when firewall impose restrictions on connections, it is not possible to create an outgoing connection to a client machine. In such cases, passive FTP mode is used, and the client initiates the connection to the server specified from the range of port numbers that can be used for such a data connection.

### > To set passive FTP mode for ActiveTransfer Server

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select an FTP port from the list of ports.

- In the **Access** section, for the **Passive Port Range** in the **From** and **To** boxes, specify the range of port numbers that can be used for passive port connections.

**Note:**

Be sure to provide proper access for the ports in your firewall settings. Otherwise, connections between the client machine and ActiveTransfer Server might be blocked.

- If your firewall or router is FTP-aware, select the **Router/Firewall Aware** check box.

**Note:**

FTP-aware routers and firewalls will inspect the FTP command and response, and might modify the response. Check your firewall configuration before selecting this option.

- In the **Passive IP Address** box, do one of the following:
  - If you want ActiveTransfer Server to automatically assign the IP address or host name of the server based on the listener configuration, type `Auto`. Ensure that you specify the IP address or host name while creating data connections in passive mode.
  - If you want to enter an IP address manually, type the IP address to use for the passive IP address.
- In the **Welcome Message** box, type an optional welcome message. If specified, this message appears in the FTP, FTPS, and SFTP client console when a user connects to the server.
- Click **Save**.

## Configuring a FTP Port to Support Implicit and Explicit SSL

To configure a FTP Port to support implicit SSL (FTPS) or explicit SSL (FTPES), you must configure additional settings on a FTP port in ActiveTransfer Server.

### ➤ To configure a FTP port to support FTPS or FTPES

- In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
- Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
- On the **Ports** tab, select an FTP port from the list of ports.
- In the **Encryption** section of the **Advanced** tab, enable **Implicit SSL** or **Explicit SSL**.
- In the **SSL Options** section of the **Advanced** tab, specify the following:

| Parameter                   | Details                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Keystore Location</b>    | <i>Mandatory</i> ActiveTransfer Server loads the truststore file from the keystore file path, <Keystore-File-Path>_trust |
| <b>Keystore Password</b>    | <i>Mandatory</i> The password for the keystore file                                                                      |
| <b>Private Key Password</b> | <i>Mandatory</i> The private key password                                                                                |

6. Click **Save**.

---

## Configuring an HTTPS Port to Support Single Sign-On

---

To configure an HTTPS port to support single sign-on (SSO) using Security Assertion Markup Language for ActiveTransfer web client.

### > To configure an HTTPS port to support SSO

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select an HTTPS port from the list of ports.
4. In the **SSO Options** section of the **Advanced** tab, select the **Support Single Sign-On** option.
5. Click **Save**.

---

## Configuring the Certificate Revocation List for secure ports

---

ActiveTransfer supports the validation of Certificate Revocation List (CRL) for the secure ports such as HTTPS and FTPS.

You can configure ActiveTransfer to validate CRL for secure ports using the property `mft.server.crlUrl`. ActiveTransfer validates the client certificate against the CRL specified in `mft.server.crlUrl` to permit or block client access to secure ports. The 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.

### > To configure ActiveTransfer Server to validate CRL with secure ports

1. Browse to the `Integration Server_directory \instances \instance_name \packages \WmMFT \config` directory on ActiveTransfer Server.

2. Open the properties configuration file (properties.cnf).
3. Set the `mft.server.crlUrl` property as one of the following:
  - a. A file stored in an accessible directory. For example:  
`mft.server.crlUrl=C:/MFT/CRL/mftCRL.crl`.
  - b. A file that can be downloaded from a URL. For example: `mft.server.crlUrl=http://softwareag.com/crls/mftCRL.crl`

**Note:**

Configuration of CRL check is not mandatory. If you leave the `mft.server.crlUrl` property blank, then ActiveTransfer does not perform the CRL check.

## Setting the Command Delay Interval

---

You can add a pause between each command to slow down clients that continually access the server.

➤ **To set the command delay interval**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select the port from the list of ports.
4. Click the **Advanced** tab.
5. In the **Priority Options** section, type a command delay interval in milliseconds.
6. Click **Save**.

## Setting the Encryption Method for ActiveTransfer Server

---

Use this procedure to set the encryption methods for ActiveTransfer Server ports that use FTP protocol.

ActiveTransfer supports Transport Layer Security (TLSv1) and Secure Sockets Layer (SSLv3), cryptographic protocols that provide Internet communication security. The 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.

➤ **To set the encryption method for ActiveTransfer Server**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management.**
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64.](#)
3. On the **Ports** tab, select an FTP port from the list of ports.
4. Click the **Advanced** tab.
5. In the **Encryption** section, set the encryption method from these options:

| Option                                  | Description                                                                                                                                                                                                                                          |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Implicit SSL</b>                     | Use implicit SSL as the encryption mode. SSL is used on all the clients in each session.                                                                                                                                                             |
| <b>Explicit SSL: Require encryption</b> | Require the client to use the data transfer encryption mode while connecting to the FTP server. In this mode, the client has the option to switch off the channel encryption.                                                                        |
| <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><li>■ <b>SSLv3</b></li></ul> |

**Note:**

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.

6. Click **Save**.

## Setting SSH Encryption Algorithm, Ciphers, and Connection Options

---

For SFTP ports, you can specify SSH settings such as an encryption algorithm and associated host keys, the ciphers used to encrypt or decrypt data, and connection settings.

## Setting RSA and DSA Encryption

ActiveTransfer supports both RSA and DSA encryption.

### Note:

The following procedure applies only to ports that use the SFTP protocol. When you create a default SFTP port in ActiveTransfer Server or ActiveTransfer Gateway, 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.

### > To set RSA or DSA encryption

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select an SFTP port from the list of ports.
4. Click the **Advanced** tab.
5. In the **SSH - Server Host Keys** section, do either or both of the following:

### Note:

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, *Installation\_directory\IntegrationServer\instances\default*.

- To enable RSA, click the **Activate** link and then specify the full path of the file that contains the key for the RSA algorithm.
- To enable DSA, click the **Activate** link and then specify the full path of the file that contains the key for the DSA algorithm.

### Note:

For an ActiveTransfer Gateway, specify the path of the server on which ActiveTransfer Gateway is running.

6. Click **Save**.

### Tip:

To deactivate RSA or DSA, click the relevant **Deactivate** link.

## Setting the Supported Ciphers for SSH

Use this procedure to set ciphers for ports that use the SFTP protocol.

Ciphers are algorithms that are used to encrypt or decrypt data. In ActiveTransfer, you can set the supported ciphers for SSH.

### ➤ To set the supported ciphers for SSH

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select an SFTP port from the list of ports.
4. Click the **Advanced** tab.
5. In the **SSH - Supported Ciphers** section, do the following:

- a. Click **+**.
- b. In the **Add Ciphers** dialog box, enable or disable the supported ciphers and click **OK**.

The enabled ciphers appear in the **SSH - Supported Ciphers** section.

**Note:**

The ciphers, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr, and arcfour256 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. Do not add ciphers that require a key strength of more than 128 bytes as default when you configure a new SFTP server.

6. In the **SSH - Supported MAC** section, do the following:
  - a. Click **+**.
  - b. In the **Add MAC** dialog box, enable or disable the supported keyed-hash message authentication codes (HMACs) for verification of data integrity and click **OK**.

The enabled HMACs appear in the **SSH - Supported MAC** section.
7. Click **Save**.

## Configuring SSH Connection Settings

Use this procedure to configure SSH connection settings for SFTP ports.

SSH connection settings include the following:

- Default character encoding that controls how ASCII characters are encoded when being sent to a client.
- Whether to use asynchronous threading to enable tasks to run in parallel. Asynchronous threading is useful to transfer a file to multiple external locations at the same time 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.

### > To set SSH connection settings

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. On the **Ports** tab, select an SFTP port from the list of ports.
4. Click the **Advanced** tab.
5. In the **SSH Connection Settings** section, click the **Text Encoding** list and select the encoding format you want to work with. In general, most clients use the UTF-8 encoding.
6. If you want to use asynchronous threading, select the **Use Asynchronous Threading** check box.
7. If you want to specify a timeout value for disconnecting an idle connection, type the number of seconds in the **Idle Timeout** box.
8. Select either or both of the handshake options to use when you establish a secure connection with a partner:
  - If you want to make the password mandatory when the certificate handshake is passed, select **Require Password Authentication**.
  - If you require a certificate or public key, select **Require Public Key Authentication**. Whether password-based authentication is mandatory or not, authentication is done with the public key alone.
9. Click **Save**.

## Setting Throttling Options

---

Throttling enables you to control the percentage of the bandwidth that should be made available for 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 ports in the ActiveTransfer instance
- IP patterns that define a range of IP addresses that are immune to the speed settings, for internal IP addresses for which bandwidth is not a concern

### ➤ To set throttling options

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Throttling** tab.
4. In the **Maximum Simultaneous User Connections** box, type the maximum number of connections allowed for the server at any given time.
5. In the **Maximum Outgoing Speed** box, type the maximum allowable speed for outbound transfers, in kilobytes per second.
6. In the **Maximum Incoming Speed** box, type the maximum allowable speed for inbound transfers, in kilobytes per second.
7. In the **IP Patterns Immune to Speed** section, click . In the new row that appears in the section, type the pattern representing a range of IP addresses. For example, 168.21.\* indicates that all addresses that begin with 168.21 are immune to speed settings.

You can delete an IP address pattern by selecting it and clicking the  button.

8. Click **Save**.

## Setting Server Restrictions

---

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 the virtual file system that match a specified pattern.

➤ **To set server restrictions**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Restrictions** tab.
4. If you want to allow connections to the server only on particular days, select the appropriate check box next to the days of the week in the **Active Time Window** section.

**Note:**

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

5. If you want to restrict particular operations for certain files, do the following in the **Patterns** list in the **File Name Filters** section:
  - a. Click the  button.
  - b. From the **Command** list, select an operation to restrict (**Rename, Listing, Download, or Upload**).
  - c. From the **Filter Type** list, select a filter type (**Ends with, Starts with, or Contains**).
  - d. In the **File Name** box, type the portion of the file name that the **Filter Type** criterion should evaluate (for example, “exe”).

**Note:**

Any characters except wildcard characters or regular expressions are permitted. ActiveTransfer Server treats those characters as part of the file name.

- e. To add more file name filters, click the  button. To delete a file name filter, select the filter and click the  button.
6. If you want to restrict access to specific folders in the virtual file system, do the following in the **Block Paths Matching These Patterns** area of the **File Name Filters** section:
  - a. Click the  button.
  - b. Type the virtual file system path you want to block in the new row.

**Note:**

You can specify a regular expression pattern. You can also use simple pattern matching by preceding the pattern with the tilde (~) character. For example, to deny user access to the folder `/system/bin`, you would type: `~/system/bin/*`

- c. To add more block paths, click the  button. To delete a path, select the path and click the  button.

7. Click **Save**.

## Banning IP Addresses

---

ActiveTransfer enables you to restrict access to ActiveTransfer Server and ActiveTransfer Gateway for specific IP addresses.

## Specifying Hammering Settings

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 the server only in the absence of a gateway instance. If you have a 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, and then ban the user's IP address for a specified number of minutes when those 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 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 about the

service, see the "wm.mft.server:unbanIPS" section in *webMethods ActiveTransfer Built-In Services Reference*.

➤ **To specify hammering settings**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.

2. Select the server.

For details, see [“Selecting the Instance to Work With” on page 64](#).

3. Click the **Banning** tab.

**Note:**

The remaining steps in this procedure pertain to the **Hammering** section.

4. If you want to ban a user’s IP address after a certain number of connection, password, or command execution attempts, do the following in the **Ban a user’s IP address after a certain number of unsuccessful attempts** section:
  - a. Click the **Edit** button in the **Connection**, **Password**, or **Command** row as desired.
  - b. In the **Maximum of** box, enter the maximum number of attempts allowed.
  - c. In the **attempts in** box, enter the time period to be measured, in seconds.
  - d. In the **then banned for** box, enter the number of minutes to ban the IP address.
5. If you want to ban the IP address associated with a specific user after the user’s first incorrect password attempt, do the following in the **Ban the IP addresses associated with the following users after the users’ first incorrect password attempt** section:
  - a. Click the **+** button, and then enter the name of the user whose IP address you want to ban. Repeat this step for each user whose IP address you want to ban.
  - b. In **Ban these IP addresses**, select whether to ban the user’s IP address permanently or only for a certain number of minutes. If you select **If attempted, for**, enter the number of minutes to elapse before accepting another password attempt from that user’s IP address.
6. In the **Remember invalid user names for** box, enter the number of seconds to hold the names of invalid users in cache.

The temporary caching of invalid user names is useful for blocking robots that make repeated attempts to discover valid user credentials. As a robot scans ActiveTransfer Server or ActiveTransfer Gateway during the user validation process, this option blocks subsequent

login attempts made using an invalid user name for the specified number of seconds. If the user name is valid, the ActiveTransfer Server or ActiveTransfer Gateway ignores this setting.

7. To slow down responses to a client that appears to be a robot scanning for writable directories on your server by way of an FTP connection, select **Slow down hack attempt scans**. This setting doubles the server's response time 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.

8. Click **Save**.

## Allowing or Denying a Range of 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.

### ➤ To allow or deny a range of IP Addresses

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server or gateway instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Banning** tab.
4. In the **IP Restrictions** section, click **+**.
5. From the first list, select **Allow** or **Deny**.
6. Type the IP address range in the **Address from** and **To** fields.

For example, specifying from 168.21.\* to 168.23.\* indicates that all addresses within that range are affected.

7. Click **Save**.

## Specifying Encryption Settings

---

ActiveTransfer enables you to use SSL encryption and file-based encryption. SSL is configured as a two-way handshake. Clients must submit valid and trusted certificates before an SSL connection is completed.

## Activating SSL Settings

The following procedure specifies global SSL encryption settings that apply to all ports on the server. For information about specifying a keystore file for a specific FTP, FTPS, HTTP, or HTTPS port, see [“Specifying a Keystore File for a Port” on page 71](#).

### › To activate SSL settings

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Encryption** tab.
4. In the **SSL** section, click **Activate**.
5. For **Keystore Location**, specify the path to the keystore file (for example, “C:\keystore” on Windows and “/usr/keystore” on UNIX).
6. In the **Keystore Password** box, type the keystore password.
7. In the **Private Key Password** box, type the private key password.
8. If you want to allow connections only for clients with a valid client certificate, select **Require valid client certificate**.

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.

For details on how to map client certificates to users, see [“User Certificate Mapping” on page 35](#).

When establishing a connection with the server, ActiveTransfer validates only the client certificate but not the password.

#### Tip:

To store valid certificates:

- a. Create a truststore file in the same location as the keystore file named *keystoreName\_trust*. For example, if the keystore file name is *server\_ks.jks*, the truststore file name should be *server\_ks.jks\_trust*.
  - b. Add the valid client certificates to this truststore.
9. If you want to use the SSL keystore settings for file upload and download operations using acceleration, select the **Enable advanced upload/download option in web client** check box.
  10. Click **Save**.

## Managing 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 the SSL ports associated with a server instance.

### > To manage SSL ciphers

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Encryption** tab.
4. In the **SSL** section, click the  button in the **Manage Ciphers** list.
5. In the **Add Ciphers** dialog box, select the cipher(s) you want to use and click **OK**.
6. To list the ciphers in a particular order, select a cipher and do one of the following:

**Note:**

Select the **Prefer cipher list order on server** option to force the order of the ciphers as listed on the server.

- Click  to move the cipher up.
- Click  to move the cipher down.

7. Click **Save**.

**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.

## Activating File-Based Encryption and Decryption

File-based encryption enables you to store files on your 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.

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 virtual folder), ActiveTransfer enforces the following order of preference:

1. User management

2. Virtual folder management
3. Server management

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 virtual folder settings for a key. If no key is present at the VFS level, then ActiveTransfer checks the server level settings for the key.

➤ **To activate file-based encryption and decryption**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With”](#) on page 64.
3. Click the **Encryption** tab.
4. In the **File-Based Encryption** section, do the following:
  - a. Click **Activate**.
  - b. In the **Public PGP Key Location** box, specify the file path to the public PGP key (for example, “C:\keylocation\simple.key” on Windows and “/usr/keylocation/enterprise.key” on UNIX).

**Note:**

You can use the `wm.mft.security.pgp:generatePGPKeyFiles` service to generate an OpenPGP key pair. For details, see the “`wm.mft.security.pgp:generatePGPKeyFiles`” section in *webMethods ActiveTransfer Built-In Services Reference*.

5. In the **File-Based Decryption** section, do the following:
  - a. Click **Activate**.
  - b. In the **Private PGP Key Location** box, specify the file path to the private PGP key (for example, “C:\keylocation\simple.key” on Windows and “/usr/keylocation/enterprise.key” on UNIX).
  - c. In the **Private PGP Key Password** box, enter the password for the private PGP key.
6. Click **Save**.

You can deactivate file-based encryption or decryption at any time by clicking **Deactivate**.

## Accelerating Data Transfer

---

Through the use of tunnels, ActiveTransfer speeds up file transfers by using the server's full bandwidth regardless of network latency or distance. For more information about this process, see [“Configuring and Managing Acceleration” on page 42](#).

Use the following procedure to define a tunnel for an ActiveTransfer Server instance.

### ➤ To define a tunnel

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Acceleration** tab.
4. To add a new tunnel, do the following:
  - a. Click the **+** button.
  - b. In the **Tunnel Name** box on the **Add a Tunnel** dialog box, type a name for the tunnel. The new tunnel appears in the list of tunnels.
5. Select the tunnel in the tunnel list and edit the following options in the **Basic** tab:
  - a. If you want the tunnel to start as soon as it is ready without any user intervention, select the **Auto-Start** check box.
  - b. In the **Server** section, the default host and port values for the destination server are 127.0.0.1 and 55580, respectively. Do not change these values.
  - c. In the **Client** section, the default host and port values for the destination server are 127.0.0.1 and 55555, respectively. Do not change these values.
  - d. To connect the tunnel to ActiveTransfer Server, create a tunnel back to your system, and then connect to a destination from there, select the **Reverse** check box.
  - e. In the **Channels** section, specify the maximum number of inbound and outbound channels to use for file transfer. 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.
6. On the **Advanced** tab, in the **Advanced Settings** section, enter the following tunnel details:

- a. In the **Stability Interval** box, enter the number of seconds to build an average speed for a single connection. After this time is reached, channels are added.
  - b. In the **Channel Ramp Up** box, enter the number of channels to be added as the data transfer speed increases.
  - c. In the **Minimum Fast Speed** box, enter the minimum speed (in KB/s) that each channel should reach before new channels are added.
  - d. In the **Minimum Slow Speed** box, enter the speed (in KB/s) below which the channels are removed.
  - e. In the **Speed Threshold** box, enter the threshold of the speed reached (in percentage) before a new channel is added.
7. Click **Save**.
  8. Ensure that the remaining acceleration configuration tasks described in [“Configuring and Managing Acceleration” on page 42](#) are completed.

## Configuring Miscellaneous Settings

---

You can configure additional server settings, including protocol options, zip compression level, and directory listing options.

### Setting Protocol Options

You can set additional protocol options that apply to all protocols.

#### > To set protocol options

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Miscellaneous** tab.
4. In the **Protocol Options** section, set the following options:
  - a. To download files only in binary mode, select the **Download in binary** check box. This prevents ActiveTransfer from altering the ASCII text file line endings even if the FTP client requests it.

- b. To upload files only in binary mode instead of ASCII mode, select the **Upload in binary** check box.
- c. To run events in parallel, select the **Run events asynchronously** check box.
- d. To allow extended passive and port commands (EPSV/EPRT), select the **Allow extended passive and port commands** check box.

**Note:**

Before you enable this option, make sure that your client supports these commands.

- e. To prevent users from changing modified times on uploaded files, select the **Disable MTDM notifications** check box.
  - f. To delete any incomplete uploads done in ActiveTransfer, select the **Delete partial uploads** check box.
5. Click **Save**.

## Setting the Zip Compression Level

You can set the zip compression level according to your needs for file size and data transfer speed.

### > To set the zip compression level

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Miscellaneous** tab.
4. In the **Zip Compression Level** section, select one of the following options from the **Compression Level** list:

| Option      | Explanation                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>None</b> | No compression. Results in the largest file size of the three options, with the longest transfer time.                                                                                          |
| <b>Fast</b> | Fastest compression. Performs little compression, but compression time is the fastest of the three options.                                                                                     |
| <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 than the other two options. |

5. Click **Save**.

## Setting Directory Listing Options

You can have ActiveTransfer use the directory listing command `ls -la` to list the owner, user group, and permission details of the destination directory when the operating system is Mac OS X, UNIX, or Linux..

### > To set directory listing options

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Miscellaneous** tab.
4. In the **Directory Listing** section, select the **Use ls -la for Destination Directory Listing (Mac OS X, UNIX, Linux)** check box.
5. Click **Save**.



# 6 Working with Templates

---

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| ■ Overview .....                                                           | 94  |
| ■ Adding a Template .....                                                  | 94  |
| ■ Specifying a Default Template .....                                      | 94  |
| ■ Specifying Throttling Options at the Template Level .....                | 95  |
| ■ Specifying Restrictions at the Template Level .....                      | 96  |
| ■ Specifying Encryption and Decryption Options at the Template Level ..... | 100 |
| ■ Specifying Acceleration Options at the Template Level .....              | 101 |

## Overview

---

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 new users when those users are created.

ActiveTransfer provides a default template, called Default Template. You can edit the settings for this template. 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 that user. For more information, see [“Managing Users, User Groups, and User Roles”](#) on page 103.

## Adding a Template

---

### > To add a template

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With”](#) on page 64.
3. Click the  button above the list of templates.
4. On the **Add Template** dialog box, enter the name and description of the template.
5. Click **OK**. The new template appears in the list of templates.

## Specifying a Default Template

---

ActiveTransfer identifies the default template with a check mark in the **Default** column in the template list at the top of the Templates page. When a new ActiveTransfer user profile is created, the user is associated with this template by default. You can specify a different template to use as the default for any new users created.

### > To specify a default template

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With”](#) on page 64.
3. In the template list, select the template you want to define as the default template.

4. On the **General** tab, select the **Default Template for New User** check box.
5. Click **Save**.

## Specifying Throttling Options at the Template Level

---

You can specify preferences for speed, file size, and data limits for upload and download operations.

### > To specify throttling options at the template level

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Throttling** tab.
5. In the **Upload Preferences** section, do the following:
  - a. If you want to specify the maximum permissible speed, in kilobytes per second, for an upload operation, enter a value in the **Maximum Speed** box.
  - b. If you want to specify the maximum permissible size, in megabytes, for an uploaded file, enter a value in the **Maximum Individual File Size** box.
  - c. If you want to specify the maximum amount of data that can be uploaded per session, enter a value, in megabytes, in the **Maximum Amount per Session** box.
  - d. If you want to specify the maximum amount of data that can be uploaded per day, enter a value, in megabytes, in the **Maximum Amount per Day** box.
  - e. If you want to specify the maximum amount of data that can be uploaded per month, enter a value, in megabytes, in the **Maximum Amount per Month** box.
6. In the **Download Preferences** section, do the following:
  - a. If you want to specify the maximum permissible speed, in kilobytes per second, for a download operation, enter a value in the **Maximum Speed** box.
  - b. If you want to specify the maximum amount of data that can be downloaded per session, enter a value, in megabytes, in the **Maximum Amount per Session** box.

- c. If you want to specify the maximum amount of data that can be downloaded per day, enter a value, in megabytes, in the **Maximum Amount per Day** box.
- d. If you want to specify the maximum amount of data that can be downloaded per month, enter a value, in megabytes, in the **Maximum Amount per Month** box.

7. Click **Save**.

## Specifying Restrictions at the Template Level

---

You can have the template define a set of restrictions that apply to all users associated with the template. Specifically, you can:

- 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 the virtual file system 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.

## Specifying Time Windows for Server Availability

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

**Note:**

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

➤ **To specify time windows for server availability**

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Restrictions** tab.
5. In the **Active Time Window** section, do the following:
  - a. If you want to restrict access to particular days of the week, select the appropriate check box next to the days you want the server to be available.

- b. If you want to restrict access to particular time slots, click . Then, select start and end times from the **From Time** and **To Time** lists, respectively.

**Tip:**

You can specify additional time slots by clicking .

6. Click **Save**.

## Specifying File Name Filters

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 virtual file system that match a specified pattern.

### > To specify file name filters

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Restrictions** tab.
5. If you want to restrict particular actions for certain files, do the following in the **Patterns** area of the **File Name Filters** section:
  - a. Click the  button.
  - b. From the **Command** list, select a command (**Rename**, **List**, **Download**, or **Upload**).
  - c. From the **Filter Type** list, select a filter type (**Starts with**, **Ends with**, or **Contains**).
  - d. In the **File Name** box, type the portion of the file name that the **Filter Type** criterion should evaluate (for example, “exe”).

**Note:**

Any characters except wildcard characters or regular expressions are permitted. ActiveTransfer Server treats those characters as part of the file name.

- e. Add more file name filters as necessary by clicking .
6. If you want to restrict access to specific folders in the virtual file system, do the following in the **Block Paths Matching These Patterns** area of the **File Name Filters** section:

- a. Click the  button.
- b. Type the virtual file system path you want to block in the new row.

**Tip:**

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 would type:

```
~/system/bin/*
```

- c. Add more block paths as necessary by clicking .
7. Click **Save**.

## Setting Authentication and Login Restrictions

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

### ➤ To set authentication and login restrictions

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Restrictions** tab.
5. In the **Authentication and Login** section, do the following:
  - a. If you want to specify the maximum number of simultaneous logins allowed for the same user, enter a value in the **Maximum Simultaneous Logins** box.
  - b. If you want ActiveTransfer Server to require the user to supply a public key and password, select the **Require public key and password** check box.
  - c. If you want to specify the maximum number of minutes a user can remain logged in per session, enter a value in the **Maximum Login Time per Session** box.
  - d. If you want to specify the maximum number of minutes a user session can remain idle, enter a value in the **Maximum Idle Time per Session** box.

- e. If you want to use trusted public SSH key files for authentication, click the  button next to **Paths to Trusted Public SSH Key Files**. Then, enter the path to a public key (for example, `/usr/var/keys/key_1`).
6. Click **Save**.

## Setting Connection Restrictions

You can restrict connections by protocol or IP address. You can also specify the default character encoding for the connection between the user and ActiveTransfer Server.

### > To set connection restrictions

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Restrictions** tab.

#### Note:

The remaining steps in this procedure pertain to the **Connection** section.

5. If you want to restrict connections to particular protocols, select the check box next to the desired protocols.
6. From the **Default Character Encoding** list, select the appropriate default character encoding. The default is **UTF-8**.
7. If you want ActiveTransfer Server to accept or deny connection requests from specific IP addresses, do the following in the **IP Restrictions** area:
  - a. Click the  button.
  - b. From the list, select **Deny** or **Accept**.
  - c. Specify a range of IP addresses in the **from** and **to** boxes.
  - d. Add more IP address ranges to accept or deny as necessary by clicking .
8. Click **Save**.

## Specifying Encryption and Decryption Options at the Template Level

---

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 for use with this feature and make sure they are stored in the correct location. For details, see [“Verifying the Location of Keystore Files for ActiveTransfer” on page 36](#).

You can override the template-level encryption and decryption options for a specific user. For more information, see [“Specifying Encryption and Decryption Options for a User” on page 117](#).

➤ **To specify encryption and decryption options at the template level**

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Encryption** tab.
5. In the **File-Based Encryption** section, specify the path to the public PGP key in the **Public PGP Key Location** box (for example, “C:\keylocation” on Windows and “/usr/keylocation” on UNIX).

**Note:**

You can use the `wm.mft.security.pgp:generatePGPKeyFiles` service to generate an OpenPGP key pair. For details, see the “`wm.mft.security.pgp:generatePGPKeyFiles`” section in *webMethods ActiveTransfer Built-In Services Reference*.

6. In the **File-Based Decryption** section, do the following:
  - a. In the **Private PGP Key Location** box, specify the path to the private PGP key (for example, “C:\keylocation” on Windows and “/usr/keylocation” on UNIX).
  - b. In the **Private PGP Key Password** box, enter the password for the private PGP key.
7. Click **Save**.

---

## Specifying Acceleration Options at the Template Level

---

ActiveTransfer allows accelerated data transfer, also known as *acceleration*. For more information about acceleration, see [“Configuring and Managing Acceleration” on page 42](#).

➤ **To specify acceleration options at the template level**

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Templates**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the template from the template list.
4. Click the **Acceleration** tab.
5. In the **Active Tunnels** section, click the **+** button.

ActiveTransfer Server displays the tunnels that were created on the Server Management page.

6. On the **Add Tunnel** dialog box, select the tunnel that you want to associate with this template.
7. Click **OK**.

**Note:**

It is only necessary to 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.

8. Click **Save**.



# 7 Managing Users, User Groups, and User Roles

---

|                                                                                     |     |
|-------------------------------------------------------------------------------------|-----|
| ■ Overview .....                                                                    | 104 |
| ■ Associating an Existing My webMethods Server User with ActiveTransfer .....       | 104 |
| ■ Associating an Existing My webMethods Server User Group with ActiveTransfer ..... | 106 |
| ■ Creating a New User .....                                                         | 107 |
| ■ Viewing and Editing User Details .....                                            | 108 |
| ■ Associating a User with a Partner or with Your Enterprise .....                   | 109 |
| ■ Editing Server Access Details for a User .....                                    | 109 |
| ■ Emailing Change of Password and Server Port Details .....                         | 110 |
| ■ Specifying Throttling Options for a User .....                                    | 111 |
| ■ Specifying Restrictions for a User .....                                          | 112 |
| ■ Specifying Encryption and Decryption Options for a User .....                     | 117 |
| ■ Specifying Acceleration Options for a User .....                                  | 118 |

## Overview

---

ActiveTransfer users are My webMethods Server users who have an ActiveTransfer profile. The ActiveTransfer profile contains all of the settings required for users to log in to ActiveTransfer Server to transfer files and perform other ActiveTransfer tasks.

You can create an ActiveTransfer profile for a user in two ways:

- If the user is already defined as a My webMethods Server user, either by way of the internal My webMethods Server system directory service or through an external directory service such as LDAP, you create an ActiveTransfer profile for the user by associating the user with ActiveTransfer. For details, see [“Associating an Existing My webMethods Server User with ActiveTransfer” on page 104](#).
- If the user is not already defined as a My webMethods Server user, you can create the user in the My webMethods Server system directory and define an ActiveTransfer profile for the user at the same time. For details, see [“Creating a New User” on page 107](#).

## Inheritance of Permissions and Settings in Groups and Roles

In My webMethods Server, 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, virtual folder management configuration, and post-processing event 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 virtual 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 user 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.

## Associating an Existing My webMethods Server User with ActiveTransfer

---

If a user is already defined as a My webMethods Server user but does not have an ActiveTransfer profile, use this procedure to associate the user with ActiveTransfer.

➤ **To associate an existing My webMethods Server user with ActiveTransfer**

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the  button above the list of users.
4. In the **Add User** dialog box, click **Search for Existing Users** and enter the search criteria in the **Existing User Search** box.
5. In the search results, select the check box next to the users that you want to associate with ActiveTransfer.
6. Click **Advanced Settings**.
7. If you want to change the user’s password, select the **Change Password** check box and then either generate a random password or create a specific password for the user.
8. Specify the ActiveTransfer Server ports to include in emails sent to users along with the user credentials:
  - To include ports that are listed as **Default in Emails** in the **Server Management** page, select **Default Ports**.
  - To include specific ports, select **Select Servers**, and then select the required ports.
9. Click **Select User**.

**Note:**

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

10. Click **Add**.

ActiveTransfer Server creates an ActiveTransfer profile for the user and lists the user on the Users page.

**Tip:**

To delete a selected user, select the user and click . This action does not delete the user from the system directory or from the external directory service. Rather, it removes the association between the user and ActiveTransfer.

11. If you want to send an email to the user containing the user’s login credentials and the URL of the ActiveTransfer Server the user will be logging in to, click **Send** at the bottom of the user’s **User Details** tab.

ActiveTransfer Server sends emails by way of the SMTP server configured in webMethods Integration Server. For information about the SMTP server configuration, see *webMethods Integration Server Administrator's Guide*.

## Associating an Existing My webMethods Server User Group with ActiveTransfer

---

Use this procedure to associate user groups already defined in My webMethods Server with ActiveTransfer. For details on how to create a group in My webMethods Server, see *Administering My webMethods Server*. Similar to user association, once associated with ActiveTransfer, you can perform any of following operations on groups:

- Associate the group with any partner or with your enterprise.
- Specify throttling options.
- Specify restrictions for server access, file actions, login volume, and so on.
- Specify encryption and decryption options.
- Specify acceleration options.

### ➤ To associate an existing My webMethods Server user group with ActiveTransfer

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click **Group**.
4. Click the  button above the list of user groups.
5. In the **Add Group** dialog box, enter the search criteria in the **Search Group** box and click **Search**.
6. In the search results, select the check box next to the user group that you want to associate with ActiveTransfer and click **Select Group**.

**Note:**

You can continue to add more user groups to the selected groups' list.

7. Click **Add**.

ActiveTransfer Server lists the user groups in the Group page. and lists the user on the Users page.

**Tip:**

To delete a user group, select the group and click . This action does not delete the group from the system directory or from the external directory service. Rather, it removes the association between the group and ActiveTransfer.

## Creating a New User

---

If a user is not already defined as a My webMethods Server user and does not have an ActiveTransfer profile, use this procedure to create the user in the My webMethods Server system directory and then define an ActiveTransfer profile for the user.

### > To create a new user

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users.**
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64.](#)
3. Click the  button above the list of users.
4. In the **Add User** dialog box, click **Create a New User.**
5. Enter the user ID, user’s first and last name, and email address in the respective boxes.
6. Click **Advanced Settings.**
7. Assign a password to the new user by either generating a random password or creating a specific password for the user.
8. Specify the ActiveTransfer Server ports to include in emails sent to users along with the user credentials:
  - To include ports that are listed as **Default in Emails** in the **Server Management** page, select **Default Ports.**
  - To include specific ports, select **Select Servers,** and then select the required ports.
9. Click **Select User.**

**Note:**

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

10. Click **OK.**

ActiveTransfer Server creates an ActiveTransfer profile for the user and lists the user on the Users page.

**Tip:**

To delete a user, select the user and click . This action does not delete the user from the system directory or from the external directory service. Rather, it removes the association between the user and ActiveTransfer.

11. Click **Add**.

ActiveTransfer Server creates an ActiveTransfer profile for the user and lists the user on the Users page.

**Tip:**

To delete a user, select the user and click . This action does not delete the user from the system directory or from the external directory service. Rather, it removes the association between the user and ActiveTransfer.

12. If you want to send an email to the user containing the user's login credentials and the URL of the ActiveTransfer Server the user will be logging in to, click **Send** at the bottom of the user's **User Details** tab.

**Note:** ActiveTransfer Server sends emails by way of the SMTP server configured in webMethods Integration Server. For information about the SMTP server configuration, see *webMethods Integration Server Administrator's Guide*.

## Viewing and Editing User Details

---

You can view and edit the details of the ActiveTransfer profile for an existing user created in the My webMethods Server system directory.

**> To view and edit user details**

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. On the **User Details** tab, in the **General** section, edit the user's name or email address as desired.

**Note:**

The **Role** box displays the role(s) assigned to the user. **Distinguished Name** uniquely identifies the user in LDAP or in the Directory Service. An example of an entry for this field is `uid=john,ou=people,o=system,o=mws`. You cannot edit these two fields.

5. If you want to change the default template assigned to a user, select the appropriate template from the **Template** list.

6. Click **Save**.

## Associating a User with a Partner or with Your Enterprise

You can associate a user with a partner or with your enterprise. Associating users with partners or with your enterprise is a way to organize virtual folders and file transactions.

### ➤ To associate a user with a partner or with your enterprise

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. On the **User Details** tab, in the **Associated Partner** section, do one of the following:
  - If you do not want to associate the user with either a partner or your enterprise, select **No Partner**.
  - If you want to associate the user with your enterprise, select **Your Enterprise**.
  - If you want to associate the user with a partner, select **The Following Partner**. Then, click the box beneath the option and select the partner name from the list.

#### Note:

You may not see the desired partner name if webMethods Trading Networks is not installed. In this case, you can type the partner name manually.

5. Click **Save**.

## Editing Server Access Details for a User

You can edit server access details such as the user’s password, or disable a user’s ID to prevent the user from logging in to the server. ActiveTransfer Server sends an email to the user when you change the user’s password and the ports selected for the user.

#### Note:

This section does not include information about sending server port details to users. For details on how to send server port details to users, see [“Emailing Change of Password and Server Port Details” on page 110](#).

### ➤ To edit server access details for a user

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. If you want to disable the user’s ID and prevent that user from logging in to the server, select the **Disable login** check box.
5. Click **Save**.

## Emailing Change of Password and Server Port Details

---

Use the **Send Email** option in the User Details page to immediately communicate the following details to existing ActiveTransfer Server users through emails:

- Change of user login password. For example:

```
Your username: Jill122
Your password: fl89&^_L09
```

- The URL for server ports where the ActiveTransfer file storage is located. For example:

```
ftp://idt56yu-97p4.sii.ad.for:1100
sftp://kpmml7-97p4.sii.ad.for:0047
```

You can choose to include details of both change of password and server ports, or only one of them. To generate the email, ActiveTransfer uses the default format in the `ExistingUserEmailContent.txt` file, available in the *Integration Server\_directory* \instances\instance\_name\packages\WmMFT\config directory. You can modify this default format as required. For details on how to modify the `ExistingUserEmailContent.txt`, see .

### ➤ To email change of password and server port details to an existing user

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the relevant user from the list of users.
4. Click **Send Email**.

**Note:**

If you do not need to change the user's password skip the next step.

5. To change the user's login password:

- a. Click **Change password**.
- b. Select the method for generating the password:
  - **Generate random password.** To allow ActiveTransfer to generate a random user password.
  - **Create a password.** To type and confirm a specific new password for the user.

**Note:**

Skip the next step if you do not want to email server port details.

6. Select the ActiveTransfer Server server ports to include the email:
  - a. Select from one these server port options:
    - **Send port server details, marked as default.** To share details of the server ports marked as default ports in the Server Management page.
    - **Select port server details, to be shared with user.** To share details only of the specific server ports.
  - b. If you selected **Select port server details, to be shared with user.**, select the required server ports from the list that appears.
  - c. Click **OK**.
7. Click **Save**.

The email is immediately sent to the user with the specified details.

## Specifying Throttling Options for a User

You can specify preferences for speed, file size, and data limits for upload and download operations for an individual user. These settings will override any throttling options set in the template associated with the user. You can apply the same settings to user groups (**User Management > Users > Group**) and (**User Management > Users > Role**) roles.

### ➤ To specify throttling options for a user

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. Click the **Throttling** tab.

5. In the **Upload Preferences** section, do the following:
  - a. If you want to specify the maximum permissible speed, in kilobytes per second, for an upload operation performed by the user, enter a value in the **Maximum Speed** box.
  - b. If you want to specify the maximum permissible size, in megabytes, for a file the user uploads, enter a value in the **Maximum Individual File Size** box.
  - c. If you want to specify the maximum amount of data that the user can upload per session, enter a value, in megabytes, in the **Maximum Amount per Session** box.
  - d. If you want to specify the maximum amount of data that the user can upload per day, enter a value, in megabytes, in the **Maximum Amount per Day** box.
  - e. If you want to specify the maximum amount of data that the user can upload per month, enter a value, in megabytes, in the **Maximum Amount per Month** box.
6. In the **Download Preferences** section, do the following:
  - a. If you want to specify the maximum permissible speed, in kilobytes per second, for a download operation performed by the user, enter a value in the **Maximum Speed** box.
  - b. If you want to specify the maximum amount of data that the user can download per session, enter a value, in megabytes, in the **Maximum Amount per Session** box.
  - c. If you want to specify the maximum amount of data that the user can download per day, enter a value, in megabytes, in the **Maximum Amount per Day** box.
  - d. If you want to specify the maximum amount of data that the user can download per month, enter a value, in megabytes, in the **Maximum Amount per Month** box.
7. The  icon to the left of each box in this section indicates a property that is inherited from the template associated with this user. If you override a template value and you want to reset it to the default value specified by the template, click the  **Reset inheritance** button to the left of the box.
8. Click **Save**.

## Specifying Restrictions for a User

---

You can define the following restrictions for a user, user group, or role:

- 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 the virtual file system 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.

## Specifying Time Windows for Server Availability

You can specify the days of the week and the times during which a user can connect to ActiveTransfer Server.

**Note:**

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

### ➤ To specify time windows for server availability

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. Click the **Restrictions** tab.
5. In the **Active Time Window** section, do the following:
  - a. If you want to restrict access to particular days of the week, select the appropriate check box next to the days you want the server to be available to the user.
  - b. If you want to restrict access to particular time slots, click . Then, select start and end times from the **From Time** and **To Time** lists, respectively.

**Tip:**

You can specify additional time slots by clicking .

6. The  icon to the left of each box in this section indicates a property that is inherited from the template associated with this user. If you override a template value and you want to reset it to the default value specified by the template, click the  **Reset inheritance** button to the left of the box.
7. Click **Save**.

## Specifying File Name Filters

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

### > To specify file name filters

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. Click the **Restrictions** tab.

**Note:**

The remaining steps in this procedure pertain to the **File Name Filters** section.

5. If you want to restrict particular actions for certain files, do the following in the **Patterns** area of the section:
  - a. Click the **+** button.
  - b. From the **Command** list, select a command (**Rename, List, Download, or Upload**).
  - c. From the **Filter Type** list, select a filter type (**Starts with, Contains, or Ends with**).
  - d. In the **File Name** box, type the portion of the file name that the **Filter Type** criterion should evaluate (for example, “exe”).

**Note:**

Any characters except wildcard characters or regular expressions are permitted. ActiveTransfer Server treats those characters as part of the file name.

- e. Add more file name filters as necessary by clicking **+**.
6. If you want to restrict a user’s access to specific folders in the virtual file system, do the following in the **Block Paths Matching These Patterns** area of the section:
    - a. Click the **+** button.
    - b. Type the virtual file system path you want to block in the new row.

**Note:**

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 would type:

```
~/system/bin/*
```

- c. Add more block paths as necessary by clicking .
7. The  icon to the left of each box in this section indicates a property that is inherited from the template associated with this user. If you override a template value and you want to reset it to the default value specified by the template, click the  **Reset inheritance** button to the left of the box.
8. Click **Save**.

## Setting Authentication and Login Restrictions

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

### ➤ To set authentication and login restrictions

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. Click the **Restrictions** tab.
5. In the **Authentication and Login** section, do the following:
  - a. If you want to specify the maximum number of simultaneous logins allowed for this user, enter a value in the **Maximum Simultaneous Logins** box.
  - b. If you want ActiveTransfer Server to require the user to supply a public key and password, select the **Require public key and password** check box.
  - c. If you want to specify the maximum number of minutes the user can remained logged in per session, enter a value in the **Maximum Login Time per Session** box.
  - d. If you want to specify the maximum number of minutes the user session can remain idle, enter a value in the **Maximum Idle Time per Session** box.

- e. If you want to use trusted public SSH key files for authentication, click the  button next to **Paths to Trusted Public SSH Key Files**. Then, enter the path to a public key (for example, `/usr/var/keys/key_1`).
6. The  icon to the left of each box in this section indicates a property that is inherited from the template associated with this user. If you override a template value and you want to reset it to the default value specified by the template, click the  **Reset inheritance** button to the left of the box.
7. Click **Save**.

## Setting Connection Restrictions

You can restrict connections by protocol or IP address. You can also specify the default character encoding for the connection between the user and ActiveTransfer Server.

### > To set connection restrictions

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. Click the **Restrictions** tab.

**Note:**

The remaining steps in this procedure pertain to the **Connection** section.

5. If you want to restrict connections to particular protocols, select the check box next to the desired protocols.
6. From the **Default Character Encoding** list, select the appropriate default character encoding. The default is **UTF-8**.
7. If you want ActiveTransfer Server to accept or deny connection requests from specific IP addresses, do the following in the **IP Restrictions** area:
  - a. Click the  button.
  - b. From the list, select **Deny** or **Allow**.
  - c. Specify a range of IP addresses in the **from** and **to** boxes.

- d. Add more IP address ranges to accept or deny as necessary by clicking .
8. The  icon to the left of each box in this section indicates a property that is inherited from the template associated with this user. If you override a template value and you want to reset it to the default value specified by the template, click the  **Reset inheritance** button to the left of the box.
9. Click **Save**.

## Specifying Encryption and Decryption Options for a User

You can define specific file-based encryption and decryption PGP keys for an individual user. These settings will override any encryption assignments set in the template associated with the user. 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.

You can apply the same settings to user groups (**User Management > Users > Group**) and (**User Management > Users > Role**) roles.

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

1. User management
2. Virtual folder management
3. Server management

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 virtual folder settings for a key. If no key is present at the VFS level, then ActiveTransfer checks the server level settings for the key.

### > To specify encryption and decryption options for a user

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the user from the list of users.
4. Click the **Encryption** tab.
5. In the **File-Based Encryption** section, specify the path to the public PGP key in the **Public PGP Key Location** box (for example, “C:\keylocation\simple.key” on Windows and “/usr/keylocation/enterprise.key” on UNIX).

**Note:**

You can use the `wm.mft.security.pgp:generatePGPKeyFiles` service to generate an OpenPGP key pair. For details, see the "`wm.mft.security.pgp:generatePGPKeyFiles`" section in *webMethods ActiveTransfer Built-In Services Reference*.

6. In the **File-Based Decryption** section, do the following:
  - a. In the **Private PGP Key Location** box, specify the path to the private PGP key (for example, "`C:\keylocation\simple.key`" on Windows and "`/usr/keylocation/enterprise.key`" on UNIX).
  - b. In the **Private PGP Key Password** box, enter the password for the private PGP key.
7. Click **Save**.

You can deactivate file-based encryption or decryption at any time by clicking **Deactivate**.

## Specifying Acceleration Options for a User

---

ActiveTransfer allows accelerated data transfer, also known as *acceleration*. For more information about acceleration, see "[Configuring and Managing Acceleration](#)" on page 42.

The acceleration settings you specify in the following procedure will override any acceleration settings set in the template associated with the user. You can apply the same settings to user groups (**User Management > Users > Group**) and (**User Management > Users > Role**) roles.

### > To specify acceleration options for a user

1. In My webMethods: **Administration > Integration > Managed File Transfer > User Management > Users**.
2. Select the server instance. For details, see "[Selecting the Instance to Work With](#)" on page 64.
3. Select the user from the list of users.
4. Click the **Acceleration** tab.
5. In the **Active Tunnels** section, click the  button.
6. On the **Add Tunnel** dialog box, select the tunnel that you want to associate with this user.
7. Click **OK**.

**Note:**

It is only necessary to 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.

8. The  icon to the left of each box in this section indicates a property that is inherited from the template associated with this user. If you override a template value and you want to reset it to the default value specified by the template, click the  **Reset inheritance** button to the left of the box.
9. Click **Save**.



# 8 Managing Virtual Folders in a Virtual File System

---

|                                                                                     |     |
|-------------------------------------------------------------------------------------|-----|
| ■ Overview .....                                                                    | 122 |
| ■ Managing the Virtual File System in ActiveTransfer .....                          | 122 |
| ■ Creating a Virtual Folder .....                                                   | 123 |
| ■ Associating Virtual Folders with a Proxy Server Alias .....                       | 124 |
| ■ Searching for Folders, Associated Users, and Associated Partners .....            | 124 |
| ■ Filtering the Virtual Folder List .....                                           | 125 |
| ■ Deleting a Virtual Folder .....                                                   | 125 |
| ■ Organizing Virtual Folders .....                                                  | 126 |
| ■ Associating a Virtual Folder with a Physical Folder Location .....                | 127 |
| ■ Configuring ActiveTransfer Server for SSL Communication with Remote Servers ..... | 128 |
| ■ Specifying Encryption and Decryption Options for a Virtual Folder .....           | 129 |
| ■ Specifying User Permissions for a Subfolder .....                                 | 130 |
| ■ User, Group, and Role Permission Propagation in VFS .....                         | 131 |
| ■ Specifying User Access Privileges for a Virtual Folder .....                      | 132 |
| ■ Specifying User Permissions for a Subfolder .....                                 | 134 |
| ■ Specifying User Access Privileges in the Parent Folder .....                      | 135 |

## Overview

---

ActiveTransfer enables you to create a *virtual file system* (VFS). A virtual file system provides an abstract, virtual view of resources in your physical file system or on a remote system such as another FTP server. This capability enables users and client applications to access a variety of file systems 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 create a virtual file system 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 then assign users to the folder and specify each user's access privileges for that folder. When the users log in to ActiveTransfer, they see the folders they can access and the resources within those folders. In 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 access to that data according to individual need.

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 what type of file system they are accessing.

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

## Using SMB Protocol for File Sharing

In ActiveTransfer, you can configure virtual folders to exchange files with an SMB server. The SMB protocol allows ActiveTransfer to read, create, and update files on a network file share or a remote server that supports SMB, with the option to specify the user name and password for access. ActiveTransfer supports SMB 1.0, SMB 2.0, and SMB 3.0 versions. By default, Microsoft Windows systems support the native SMB protocol. However, UNIX systems must have interoperability utilities like Samba. SMB also allows for cross-platform file access. For example, ActiveTransfer running on Microsoft Windows system can access files on a Linux system.

Typically, file operations are faster when you connect to a network file share using SMB protocol (SMB://host/Folder/) than when directly using a network file path (for example, FILE:///host/SharedFolder/). This is especially true when the operations are carried out on a large number of files.

## Managing the Virtual File System in ActiveTransfer

---

You can perform the following VFS management tasks:

- Create and delete virtual folders.
- Search for virtual folders and any associated users or partners.

- Filter the list of virtual folders.
- Organize virtual folders by partners or by your enterprise.
- Associate a virtual folder with a physical folder location.
- Specify the access privileges that ActiveTransfer users, groups, and roles have for a virtual folder.

## Creating a Virtual Folder

You create and maintain virtual folders on the Virtual Folder Management page in My webMethods. When you create a virtual folder, you have two options:

- Associate the virtual folder with a physical location. That is, the virtual folder represents an existing physical folder on a local or remote file system. Such folders are identified by an orange square in the virtual folder list.
- Create a virtual folder with no physical location. In this case, the virtual folder simply represents a collection of physical folders and files located on one or more local or remote file systems. Such folders are identified by a white rectangle in the virtual folder list.

### Important:

You cannot add a virtual folder beneath a virtual folder that is associated with a remote physical location.

### ➤ To create a virtual folder

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. In the virtual folder list, click  to the right of the **Home** folder.
4. In the **Add Virtual Folder** dialog box, type the folder name.
5. If you want the folder to be associated with a physical local or remote folder, select **This folder has a physical location**. For information about specifying the physical location, see [“Associating a Virtual Folder with a Physical Folder Location” on page 127](#).
6. To provide access My webMethods Server users, groups, or roles to the virtual folder, click **Permissions** and add users, groups, and roles.

For information on how to associate users, groups, and roles, with virtual folders, see [“Associating an Existing My webMethods Server User with ActiveTransfer” on page 104](#), [“Associating an Existing My webMethods Server User Group with ActiveTransfer” on page 106](#), and [“Associating an Existing My webMethods Server Role with ActiveTransfer” on page 59](#).

7. If you want to route file transfers through a proxy server, associate the virtual folder with a proxy server alias. For information on how to associate virtual folders, see [“Associating Virtual Folders with a Proxy Server Alias”](#) on page 124.
8. Click **Add**.

The new virtual folder appears in the list of virtual folders on the left side of the page.

## Associating Virtual Folders with a Proxy Server Alias

---

Use this procedure to associate proxy server aliases with virtual folders for file transfers to remote servers. For information on proxy server aliases in ActiveTransfer, see [“Managing Proxy Server Aliases”](#) on page 37.

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With”](#) on page 64.
3. Select the virtual folder in the virtual folder list.
4. Select **Use Proxy**.
5. If you want ActiveTransfer to use the default proxy server alias defined for a specific file transfer protocol in Integration Server or ActiveTransfer, select **Global proxy settings**.
6. If you want to use a specific proxy alias for the VFS:
  - a. Select **Select proxy alias**.
  - b. From the available list, select the appropriate proxy server alias to use.
7. Click **Save**.

## Searching for Folders, Associated Users, and Associated Partners

---

If you need to quickly locate a virtual folder or its associated users or partners, you can search the virtual folder list.

### ➤ To search for folders, users, or partners

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.

2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. In the virtual folder list, click **Expand All** .
4. By default, all folders and all partners will be searched. Depending on how complex the virtual folder structure is, the search could take some time to complete. To narrow your search, you can apply a partner-based filter to the folder display or you can manually navigate to a specific partner folder in the list.

For instructions on applying a filter to the folder display, see [“Filtering the Virtual Folder List” on page 125](#).

5. In the **Search** box, enter the search criteria. The folder list dynamically populates with the names of the items matching your search criteria.

## Filtering the Virtual Folder List

---

You can filter the virtual folders that are displayed in the virtual folder list. You can view all virtual folders, the virtual folders of a trading partner, or the virtual folders of your enterprise.

### > To filter the virtual folder list

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click **Filters** at the top of the page to show the filter options.
4. If you want to display all virtual folders, select **All Folders**.
5. If you want to display only the virtual folders for a specific partner or for your enterprise, do the following:
  - a. Select **Folders of the Partner or Your Enterprise**.
  - b. Click the box beneath the option.
  - c. Select a partner name or enterprise name.
6. Click **Apply**.

## Deleting a Virtual Folder

---

### > To delete a folder

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the virtual folder name in the virtual folder list.
4. Click  to the right of the folder name.
5. In the **Delete Folder** confirmation dialog box, click **OK**.

Deleting a virtual folder does not delete its contents in the local or remote location.

## Organizing Virtual Folders

---

You can organize the virtual folders in your VFS by associating the folders with partners or with your enterprise. If you do not associate a folder with either a partner or your enterprise, the folder appears beneath a folder called No Partner.

### ➤ To organize virtual folders

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the virtual folder in the virtual folder list. The folder details appear on the right side of the page.
4. Click the arrow to the left of **Partner** to view the partner options.
5. Do one of the following:
  - If you do not want to associate the folder with either a partner or your enterprise, select **No Partner**.
  - If you want to associate the folder with your enterprise, select **Your Enterprise**.
  - If you want to associate the folder with a partner, select **The Following Partner**. Then, click the box beneath the option and select the partner name from the list.

#### Note:

You may not see the desired partner name if webMethods Trading Networks is not installed. In this case, you can type the partner name manually.

6. Click **Save**.

After the virtual folder list refreshes, the virtual folder you modified appears under the appropriate folder.

## Associating a Virtual Folder with a Physical Folder Location

You can associate a virtual folder with a physical folder location. The location can be either local or remote.

### » To associate a virtual folder with a physical location

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the virtual folder in the virtual folder list. The virtual folder details appear on the right side of the page.
4. Click the arrow to the left of **Location** to view the folder location options.
5. Select **This folder has a physical location**.
6. If you want to specify a local physical location, do the following:
  - a. Click **Local File Path**.
  - b. Specify the path to the folder you want to use in your local file system by either typing the path or browsing your local file system to locate the folder.
7. If you want to specify a remote physical location, do the following:
  - a. Click **Remote Path**.
  - b. Select the transport mechanism from the list.

For example, **FTPES** to connect to servers that use explicit FTPS over TLS, or **FTPS** to enable communication for Implicit mode.
  - c. Enter the remote path in the format *protocol://host:port/relative path* (for example, `ftp://ftpmc:56/projectfolder/download/`).

#### **Important:**

Make sure the path ends with “/” to identify the location as a folder and not a file.

You can use user variables in the path. For information about these variables, see [“Server Configuration Parameters and Variables” on page 399](#).

**Note:**

If you do not specify a port, ActiveTransfer will use the default port for the protocol.

- d. Type a **User Name** and **Password** for the remote system.
- e. If you select the secure protocols FTPES, FTPS, and HTTPS, specify the keystore path in **Keystore**, and enter the **Keystore Password** and **Key Password**.

By default, ActiveTransfer Server accepts SSL certificates from any remote server. You can configure ActiveTransfer Server to accept certificates only from trusted remote servers. For details, see [“Configuring ActiveTransfer Server for SSL Communication with Remote Servers” on page 128](#).

- f. If you select the **SFTP** transport type and require public key authentication, enter the **Private Key Path** and the **Private Key Password**.

For SFTP transport type, if you want both basic authentication and public key authentication, select **Two-Factor Authentication**.

If either the basic authentication password or the public key authentication password is missing, the connection fails.

- g. If you want to quickly check the connection to a remote location, click **Test Connection**.
- h. If you want ActiveTransfer Server to recover from a download that was not completed, select **High Availability Download Recovery**.
- i. If you want ActiveTransfer Server to recover from an upload that was not completed, select **High Availability Upload Recovery**.
- j. For FTP, FTPS, and FTPES protocols, to enable ActiveTransfer Server to connect to a remote server using the passive mode, select **Passive**. By default, **Passive** is not selected so that ActiveTransfer Server uses the active mode.

8. Click **Save**.

## Configuring ActiveTransfer Server for SSL Communication with Remote Servers

---

By default, ActiveTransfer Server accepts SSL certificates from any remote server. You can configure ActiveTransfer Server to accept certificates only from trusted remote servers. For this configuration to work, the remote server's certificate should be listed as a trusted root in the ActiveTransfer Server's truststore. ActiveTransfer Server validates the certificate received from the remote server against the ones listed in its truststore.

➤ **To configure ActiveTransfer Server to allow SSL communication only with trusted remote servers**

1. Browse to the *Integration Server\_directory* \instances\*instance\_name*\packages\WmMFT\config directory on ActiveTransfer Server.
2. Open the properties configuration file (properties.cnf).
3. Set the `mft.ssl.client.acceptAnyCert` property to `false`. For details of `mft.ssl.client.acceptAnyCert`, see “[mft.ssl.client](#)” on page 408 and save the file.

**Note:**

When you set this property to `false`, ActiveTransfer Server validates the certificate presented by the remote server against the certificates in its truststore. You must store the truststore file with all the trusted certificates in the same location as the keystore file. The truststore file should have the name `keystoreName_trust`. For example, if the keystore file name is `remoteserver_ks.jks`, the truststore name should be `remoteserver_ks.jks_trust`.

## Specifying 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 stream. Encrypted files are decrypted only if they are transferred back through ActiveTransfer using the same 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 event. If you want to use the encryption and decryption keys in an event, create an encryption or decryption action in the event.

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

1. User management
2. Virtual folder management
3. Server management

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 virtual folder settings for a key. If no key is present at the VFS level, then ActiveTransfer checks the server level settings for the key.

### ➤ To specify file-based encryption and decryption options for a virtual folder

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.

2. Select the ActiveTransfer Server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).

3. Select the required virtual folder in the VFS tree.

The folder details appear on the right side of the page.

4. Click the arrow to the left of **Encryption**.

5. In the **File-Based Encryption** section, do the following:

a. Click **Activate**.

b. In the **Public PGP Key Location** box, specify the file path to the public PGP key (for example, “C:\keylocation\simple.key” on Windows and “/usr/keylocation/enterprise.key” on UNIX).

**Note:**

You can use the `wm.mft.security.pgp:generatePGPKeyFiles` service to generate an OpenPGP key pair. For details, see *webMethods ActiveTransfer Built-In Services Reference*.

6. In the **File-Based Decryption** section, do the following:

a. Click **Activate**.

b. In the **Private PGP Key Location** box, specify the file path to the private PGP key (for example, “C:\keylocation\simple.key” on Windows and “/usr/keylocation/enterprise.key” on UNIX).

c. In the **Private PGP Key Password** box, enter the password for the private PGP key.

**Note:**

You can use the `wm.mft.security.pgp:generatePGPKeyFiles` service to generate an OpenPGP key pair. For details, see *webMethods ActiveTransfer Built-In Services Reference*.

7. Click **Save**.

You can deactivate file-based encryption or decryption at any time by clicking **Deactivate**.

## Specifying User Permissions for a Subfolder

---

Let us consider the users **Mike** and **Anna** who have the following access privileges to the **Marketing** folder:

- *View*
- *Download*

### ■ *Resume File Transfer*

As an Administrator you want to provide the additional access permission, *Upload* to **Mike** in the **inbound** folder and restrict the access permission provided to **Anna** in the **outbound** folder to *View* only, you can achieve these using the following:

#### ➤ **To override the user access privileges inherited from the Marketing folder**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the ActiveTransfer Server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the virtual folder **inbound** in the VFS tree. The folder details appear on the right side of the page.
4. Select the user **Mike** in the **User Access** section.
5. Unselect the checkbox **Inherit permissions from parent**.
6. Select the permissions that you want to assign to the user **Mike**: *View, Upload, Download, and Resume File Transfer*.
7. Click **Save**.
8. Similarly, select the virtual folder **outbound** in the VFS tree. The folder details appear on the right side of the page.
9. Select the user **Anna** in the **User Access** section.
10. Unselect the checkbox, **Inherit permissions from parent**.
11. Select the permissions that you want to assign to the user **Anna**: *View* and unselect all other permissions.
12. Click **Save**.

## User, Group, and Role Permission Propagation in VFS

### Note:

In this topic, *user* also refers to user group and role.

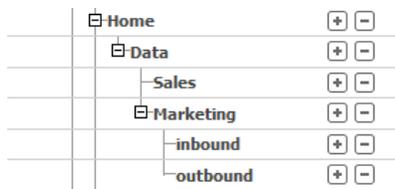
ActiveTransfer now propagates user permissions in the VFS as follows:

- If you grant a user permissions to a parent folder, the user will also have the same permissions to all subfolders.

- If you grant a user 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. These new permissions are then be inherited by any subfolders under the folder.

## Example

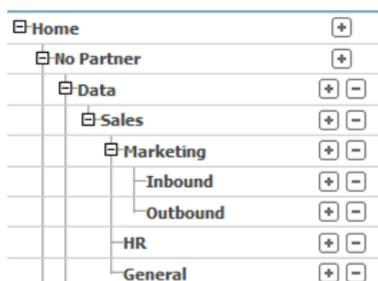
Consider the following VFS scenario in ActiveTransfer:



Let us grant the ActiveTransfer user, Mike, permission to access the Marketing folder in the VFS. The following permissions are automatically assigned to the parent folder and the subfolders of Marketing:

- Folder traverse permission: Mike has traversal permission for the parent folder Data. This means that the Mike can browse al folders from Data to Marketing.
- Inherited permission from parent folder: The Marketing subfolders, inbound and outbound inherit the permissions defined in the parent folder for Mike.

You might choose to override the permissions inherited from the parent folder and define your own permissions for Mike at the subfolder level. For details on how you can specify permissions to subfolders, see “Specifying User Permissions for a Subfolder” on page 134.



Mike has *view* permission to the Marketing folder, but you now want to also give him *view* permission to the HR and General folders too. So you could give Mike *view* permission to all subfolders of Data, the parent folder instead of setting permissions separately for each subfolder in Sales.

## Specifying User Access Privileges for a Virtual Folder

You can specify access privileges to a virtual folder by first selecting the users who can access the folder and then specifying the permissions for the actions each user can perform in the folder.

➤ **To specify user access privileges to a virtual folder**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
  2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
  3. Select the virtual folder in the virtual folder list. The folder details appear on the right side of the page.
  4. Click the arrow to the left of **User Access** to view the user access options.
  5. Click the  button above the list of users.
  6. If the user you want to access the folder already exists in the system directory, select **Search for Existing Users** and do the following:
    - a. Type the first few letters of the user’s first name, last name, or user name in the search box and then click **Search**.
    - b. In the search results, select the check box next to the user that you want to add.
    - c. If you want to change the user’s password or ports, click **Advanced Settings** and change these settings as desired. For more information, see [“Associating an Existing My webMethods Server User with ActiveTransfer ” on page 104](#).
    - d. Click **Add Existing Users**. You can add more users as needed.
  7. If the user you want to access the folder does not already exist in the system directory, select **Create a New User** and do the following:
    - a. Enter the user’s user ID, first name, last name, and email address in the respective boxes.
    - b. Click the arrow to the left of **Advanced Settings** and specify password and port settings for the user as desired. For more information, see [“Creating a New User” on page 107](#).
    - c. Click **Add New User to Selection**. You can add more users as needed.
- Note:**  
When you create a new user in this way, the user account is created in the system directory but not in any externally configured directory services such as LDAP.
8. When you are done adding users, click **OK**.
  9. In the **User Access** section, select the user whose permissions you want to specify.

10. Select the check box next to each permission you want to grant to the user (for example, view the contents of the folder, download files to the folder, create subfolders within the folder).

**Note:**

If the folder does not have a physical location, the **Upload** and **Create Folder** permissions are not applicable.

11. In the **Quota Limit** box, specify the total amount of space, in megabytes or gigabytes, to make available to this user for file transfers in this virtual folder. Then, select **MB** or **GB** from the list. If the user exceeds this limit, ActiveTransfer Server denies the user from any further file transfer activity until the user frees up space by deleting files he or she has previously uploaded or downloaded in this folder.

**Note:**

If you have assigned a user access privileges to only one virtual folder in the VFS, the contents of the folder will be directly shown to the user. ActiveTransfer Server shows the folders in the VFS only if the user has access privileges to more than one folder. If you want the user to see a root folder when the user logs in, you must create such a folder inside the ActiveTransfer Server VFS.

12. Click **Save**.

## Specifying User Permissions for a Subfolder

---

Let us consider the users **Mike** and **Anna** who have the following access privileges to the **Marketing** folder:

- *View*
- *Download*
- *Resume File Transfer*

As an Administrator you want to provide the additional access permission, *Upload* to **Mike** in the **inbound** folder and restrict the access permission provided to **Anna** in the **outbound** folder to *View* only, you can achieve these using the following:

➤ **To override the user access privileges inherited from the Marketing folder**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the ActiveTransfer Server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the virtual folder **inbound** in the VFS tree. The folder details appear on the right side of the page.

4. Select the user **Mike** in the **User Access** section.
5. Unselect the checkbox **Inherit permissions from parent**.
6. Select the permissions that you want to assign to the user **Mike**: *View, Upload, Download, and Resume File Transfer*.
7. Click **Save**.
8. Similarly, select the virtual folder **outbound** in the VFS tree. The folder details appear on the right side of the page.
9. Select the user **Anna** in the **User Access** section.
10. Unselect the checkbox, **Inherit permissions from parent**.
11. Select the permissions that you want to assign to the user **Anna**: *View* and unselect all other permissions.
12. Click **Save**.

## Specifying User Access Privileges in the Parent Folder

Let us consider the user **Mike** in the above example who has access to the **Marketing** folder. Let us now consider two more folders in the VFS, **General** and **HR** under the **Sales** folder. **Mike** currently has the following access in the VFS:

- **Marketing** folder: *View, Download, and Resume File Transfer*.
- **Inbound** folder: *View, Download, Resume File Transfer, and Upload*.
- **Outbound** folder: *View, Download, and Resume File Transfer*.

As an Administrator, you want to grant *view* access to **Mike** to the other folders in the **Sales** folder: **General** and **HR**. This can be achieved using the following:

### ➤ To specify user access privileges in the parent folder

1. In My webMethods: **Administration > Integration > Managed File Transfer > Virtual Folder Management**.
2. Select the ActiveTransfer Server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Select the virtual folder **Sales** in the VFS tree. The folder details appear on the right side of the page. The user **Mike** has folder traversal permission in this folder.

4. Unselect the **Traverse folder** checkbox. You will see the minimum permission set selected in the list.
5. Unselect all other permissions except *view*.
6. Click **Save**. **Mike** will now get *view* access to the **General** and **HR** folders under **Sales** folder.

# 9 Managing Events

---

|                                                                |     |
|----------------------------------------------------------------|-----|
| ■ About Events .....                                           | 139 |
| ■ Adding an Event .....                                        | 139 |
| ■ Defining Conditions that Trigger an Event .....              | 141 |
| ■ Defining Actions to Execute when an Event Is Triggered ..... | 144 |
| ■ File Processing in Event Actions .....                       | 144 |
| ■ Executing File Operations .....                              | 145 |
| ■ Executing an Integration Server Service .....                | 169 |
| ■ Executing a Script .....                                     | 171 |
| ■ Executing a Trading Networks Service .....                   | 173 |
| ■ Sending Universal Messaging or Broker Notification .....     | 176 |
| ■ Sending an Email Message .....                               | 178 |
| ■ Writing File Content to the Database .....                   | 180 |
| ■ Jumping to a Designated Action .....                         | 182 |
| ■ Excluding Files from an Action .....                         | 184 |
| ■ Defining an Error Action .....                               | 185 |
| ■ Activating an Event .....                                    | 186 |
| ■ Activating, Deactivating, and Deleting Multiple Events ..... | 187 |
| ■ Parameterizing Scheduled Event Actions .....                 | 188 |

- Parameterizing Scheduled Events to Poll Source URLs and Transfer Files to Destination URLs ..... 191
- Examples for Configuring an Event ..... 193

---

## About Events

---

You can define events that, when triggered, cause ActiveTransfer Server to perform a specified action or set of actions. There are two types of managed file transfer events:

- *Post-processing events* cause ActiveTransfer Server to perform a specified action or set of actions when a user uploads, downloads, or deletes a file.

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

This behavior appears for webMethods ActiveTransfer version 10.7 and later.

- *Scheduled events* cause ActiveTransfer Server to perform an action at a specified date and time.

Creating an event consists of the following high-level steps:

1. Add a post-processing or scheduled event.
2. Define the conditions that trigger the event.
3. Define one or more actions to execute when the event is triggered.
4. Define an error action to execute if the specified event action fails.
5. Activate the event.

### Using SMB Protocol for File Sharing

In ActiveTransfer, you can configure events to exchange files with an SMB server. The SMB protocol allows ActiveTransfer to read, create, and update files on a network file share or a remote server that supports SMB, with the option to specify the user name and password for access. ActiveTransfer supports SMB 1.0, SMB 2.0, and SMB 3.0 versions. By default, Microsoft Windows systems support the native SMB protocol. However, UNIX systems must have interoperability utilities like Samba. SMB also allows for cross-platform file access. For example, ActiveTransfer running on Microsoft Windows system can access files on a Linux system.

Typically, file operations are faster when you connect to a network file share using SMB protocol (SMB://host/Folder/) than when directly using a network file path (for example, FILE:///host/SharedFolder/). This is especially true when the operations are carried out on a large number of files.

---

## Adding an Event

---

You can define two types of events:

- Post-processing event, which executes an action when a user uploads, downloads, or deletes a file
- Scheduled event, which executes an action at a specified date and time

The first step in defining an event is to add the event to the **Post-Processing Events** tab or the **Scheduled Events** tab on the Event Management page.

## Adding a Post-Processing Event

### > To add a post-processing event

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Post-Processing Events** tab.
4. Click the  above the list of events.
5. In the **Add Post-Processing Event** dialog box, do one of the following:
  - If you want to create a new event that is not based on an existing, similar one, select **A new event**.
  - If you want to create a new event that is similar to one that already exists, select **A copy of an existing event**. Click the box beneath this option and select the event on which you want to base the new one.
6. Type the event name and description in the respective boxes.
7. Click **OK**. The event name appears in the event list at the top of the page.
8. Define the conditions that determine when to execute an action for this event. For details, see [“Specifying Conditions for a Post-Processing Event” on page 141](#).

## Adding a Scheduled Event

### Note:

Association of users, groups, and roles is not available for scheduled events. It is limited to post-processing events.

### > To add a scheduled event

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).

3. Click the **Scheduled Events** tab.
4. Click the  button above the list of events.
5. In the **Add Scheduled Event** dialog box, do one of the following:
  - If you want to create a new event that is not based on an existing, similar one, select **A new schedule**.
  - If you want to create a new event that is similar to one that already exists, select **A copy of an existing schedule**. Click the box beneath this option and select the event on which you want to base the new one.
6. Type the event name and description in the respective boxes.
7. Click **OK**. The event name appears in the event list at the top of the page.
8. Define the criteria that determine when to execute an action for this event. For details, see [“Specifying Conditions for a Scheduled Event” on page 142](#).
9. If you want to test the actions defined for the scheduled event, you can use the `wm.mft.schedule:executeEvent` service. For details about this service, see *webMethods ActiveTransfer Built-In Services Reference*.

## Defining Conditions that Trigger an Event

---

After you add an event, the next step is to define the conditions that trigger the event and determine when an action should be executed. For example, for a post-processing event, you can specify to execute an action immediately after any user uploads a file into a particular folder. For a scheduled event, you specify the date and time to execute the action.

## Specifying Conditions for a Post-Processing Event

### > To specify conditions for a post-processing event

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the **Post-Processing Events** tab.
4. Select the event from the list of post-processing events.

**Note:**

The remaining steps in this procedure pertain to the **Criteria** section.

- From the **Execute the actions below when a user** list, specify the file operation to consider (for example, **uploads**).

**Note:**

If you specify an event based on the deletion of a file, make sure that any subsequent actions you define for the event do not rely on the presence of the deleted file.

- If you want to specify a particular folder, select **The following name**, and then type the folder name in the box beneath this option.

**Note:**

You can use wildcard characters in the folder name box (for example, \*baseName).

By default, ActiveTransfer Server considers file activity in any virtual file system folder when evaluating event criteria.

- For the file transfer status, specify whether ActiveTransfer Server should consider successful transfers only (**Success**), unsuccessful transfers only (**Failure**), or both (**Success or Failure**).
- If you want to specify particular users, roles, or groups for whom the event should be executed, use the appropriate option:
  - If you want ActiveTransfer Server to consider operations performed by any user, select **Any user**.
  - If you want ActiveTransfer Server to execute the event for file operations performed by particular users, groups, or roles, select **The following users, groups, roles**. Then, click the **+** to search for and select the users, groups, and roles that you want to add to the criteria.
- Specify whether to execute the actions immediately, after the user exits all sessions, or after the user is idle for some seconds. If you select **After the user is idle for**, enter the number of seconds to wait before executing the action.
- Click **Save**.
- Define one or more actions to execute when the event is triggered. See [“Defining Actions to Execute when an Event Is Triggered”](#) on page 144.

## Specifying Conditions for a Scheduled Event

### ➤ To specify conditions for a scheduled event

- In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.

2. Select the server instance. For details, see [“Selecting the Instance to Work With”](#) on page 64.
3. Click the **Scheduled Events** tab.
4. Select the event from the list of scheduled events.

**Note:**

The remaining steps in this procedure pertain to the **Criteria** section.

5. From the **Execute Actions** list, specify how often to execute the action, as follows:

| <b>If you select this...</b> | <b>Do this...</b>                                                                                                                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Run Once</b>              | Specify the date and time to execute the action. Click the calendar icon to select a date from the calendar.                                                                                                                                   |
| <b>Manual</b>                | Use the <code>wm.mft.schedule:executeEvent</code> service to execute the actions defined for this event.                                                                                                                                       |
|                              | <b>Note:</b><br>This event can be triggered on demand using the <code>wm.mft.schedule:executeEvent</code> service.                                                                                                                             |
| <b>Fixed Interval</b>        | Specify a date range and the time interval that ActiveTransfer Server should wait before executing the next action for a scheduled event. For details, see <a href="#">“Calendar and Processing Options for Scheduled Events”</a> on page 419. |
| <b>Hourly</b>                | Specify a date range and the times you want to execute the action each hour. For details, see <a href="#">“Calendar and Processing Options for Scheduled Events”</a> on page 419.                                                              |
| <b>Daily</b>                 | Specify a date range and the times you want to execute the action each day. For details, see <a href="#">“Calendar and Processing Options for Scheduled Events”</a> on page 419.                                                               |
| <b>Weekly</b>                | Specify a date range, the days of the week, and the times you want to execute the action each week. For details, see <a href="#">“Calendar and Processing Options for Scheduled Events”</a> on page 419.                                       |
| <b>Monthly</b>               | Specify a date range, the days within the month, and the times you want to execute the action each month. For details, see <a href="#">“Calendar and Processing Options for Scheduled Events”</a> on page 419.                                 |
| <b>Yearly</b>                | Specify a date range, the months, the days within the month, and the times you want to execute the action each year. For details, see <a href="#">“Calendar and Processing Options for Scheduled Events”</a> on page 419.                      |

6. Click **Save**.
7. Define one or more actions to execute when the event is triggered. Ensure that a “find file” action is the first action defined for the event. See [“Defining Actions to Execute when an Event Is Triggered”](#) on page 144.

## Defining Actions to Execute when an Event Is Triggered

---

After you add an event and define the conditions that trigger the event, you define one or more actions to execute when the event is triggered. The following table describes the types of actions you can execute:

| Action                                                                            | Where to Go for Information                                                                   |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Execute a file operation, such as renaming, decrypting, or unzipping a file       | <a href="#">“Executing File Operations”</a> on page 145                                       |
| Execute an Integration Server service                                             | <a href="#">“Executing an Integration Server Service”</a> on page 169                         |
| Execute a script                                                                  | <a href="#">“Executing a Script”</a> on page 171                                              |
| Execute a Trading Networks service                                                | <a href="#">“Executing a Trading Networks Service”</a> on page 173                            |
| Send an Universal Messaging or Broker notification                                | <a href="#">“Sending Universal Messaging or Broker Notification”</a> on page 176 (Deprecated) |
| Send an email message                                                             | <a href="#">“Sending an Email Message”</a> on page 178                                        |
| Write the contents of a file to the database                                      | <a href="#">“Writing File Content to the Database”</a> on page 180                            |
| Jump to a designated action                                                       | <a href="#">“Jumping to a Designated Action”</a> on page 182                                  |
| Exclude certain files from an action or a set of actions based on a source filter | <a href="#">“Excluding Files from an Action”</a> on page 184                                  |

## File Processing in Event Actions

---

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

The first action configured in a scheduled event is the find action. The files listed by the find action is the source of input files for the event. If the find action returns more than one file, the subsequent actions will operate on all the files. Each action configured in the event will complete the operation on all the files in the list and pass on the set of files to the subsequent action. For more details on how the files are processed for specific events, refer to the *Result* section for that action.

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

## Executing File Operations

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

## Creating a Basic File Operation Action

When you create a file operation action, you must first select the file operation you want to execute. Then, you define the specific properties that apply to the selected file operation.

The following procedure describes how to create the basic file operation action. For information about defining individual file operation properties, see the topics at the end of this procedure.

### Note:

For outbound file transfers triggered through scheduled events 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 File Transactions page.

### ➤ To create a basic file operation action

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
  - a. In the resulting dialog box, click the **Select Category** list, and then click **Execute File Operation**.
  - b. In the **Select Action** list, click the file operation you want the action to execute (for example, **Copy**).

- c. Click **OK**.

You can accept the default properties for the selected file operation action, or you can modify them to meet your requirements. For details, see:

- [“Finding Files” on page 146](#)
- [“Copying or Moving Files” on page 151](#)
- [“Deleting Files” on page 155](#)
- [“Encrypting and Decrypting Files” on page 157](#)
- [“Renaming Files” on page 159](#)
- [“Unzipping Files” on page 160](#)
- [“Writing Content to a File” on page 163](#)
- [“Zipping Files” on page 166](#)

**Note:**

If you are defining a scheduled event, make sure the “find file” action is the first action you define. Otherwise, the scheduled event will fail.

6. If you require parallel processing of files in multiple threads, click the **Advanced** list.
  - a. Select **Parallel processing**.
  - b. From the **Start parallel processing for files after**, select the action after which ActiveTransfer must start parallel processing of files in multiple threads.

ActiveTransfer executes the action you selected here, and any others before it, sequentially.
  - c. In **Maximum number of parallel processes**, type the maximum number (between one and 999) of parallel threads that ActiveTransfer can create to simultaneously process files.

*Result:* You can monitor the actions performed on files using the **File Seq No** column in the **Activities** tab of the Event Log page. By default, this column is hidden, but you can configure its display.

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

## Finding Files

After you create a basic find file action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

**Note:**

If you are defining a scheduled event, make sure the “find file” action is the first action you define. Otherwise, the scheduled event will fail.

➤ **To set the properties of a find file action**

1. For **File URL**, identify the path to search by doing one of the following:

**Important:**

When you enter file path locations, be sure to end the path with a slash character (“/”) to identify the location as a folder and not a file.

- If the file URL is on your local machine or network, select **File Path** and browse to or enter the location.

**Note:**

To specify a file URL for a shared location, use the following syntax:  
*FILE:/// <host> /SharedFolder/*. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.

- If the file URL is on a remote machine or network, select **Remote File Path** and browse to or enter the location in the format: *protocol:// <host> :<port> /DestinationFolder/*.
  - If you are using **Amazon-S3** as your remote path, then configure the **Bucket name**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key**.
  - If you are using **AZURE-FILE** or **AZURE-BLOB** as your remote path, then configure the **Authentication type**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key** as required.

**Note:**

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

- If the file URL is a virtual folder in the ActiveTransfer VFS, do the following:
  1. Select **Virtual Folder**
  2. Type in the virtual folder details in the text box or use the browse option.
 

If you use the browse button, the **Select virtual folder** look up window opens.
  3. In the **Select virtual folder** window, select the virtual folder by highlighting the element and click on **Select**.
  4. If you want to point to a subfolder in the virtual folder, append the URL in the text box with the details of the subfolder.

**Note:**

The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the event is configured.

**Tip:**

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 virtual folder for the remote server in the VFS and configure the **Keystore**, **Keystore Password**, and **Key Password** parameters. You can then use the Virtual folder that you configured in the **Virtual Folder** option of the **File Path** in the event action. For additional details see [“Associating a Virtual Folder with a Physical Folder Location” on page 127](#).

2. For **File Name**, specify the name of the file to find by doing one of the following:
  - If you want ActiveTransfer to ignore folders and their contents in the Find action, select **Exclude folders**.
  - If you want ActiveTransfer to ignore folders and their contents in the Find action, select **Exclude folders**.
  - If you want to find files with any name, select **Any file name**.
  - If you want to find files with a specific name, select **File name** and enter the name of the file.
3. If **File URL** is a third-party HTTP(S) server, clear the **ActiveTransfer HTTP(S) Server** selection.

**Note:**

This field appears only if the **File URL** specified:

- Is an HTTP(S) URL.
- Is not a server variable.

For more information on how ActiveTransfer handles remote or external HTTP(S) servers, see [“Connecting to HTTP\(S\) Servers” on page 40](#).

4. Select one of the following options to determine the file name for subsequent copy actions:
  - If the **File URL** specified ends with a file name, select **Extract file name from URL**. Active transfer uses this file name in subsequent copy actions.
  - If the **File URL** specified does not end with a file name or you want to use a different file name, select **Specify file name**, and then enter the file name to use in the text box. You can also use a server variable or event parameter here.
5. Type a **User Name** and **Password** for the remote system.
6. If you want to route file transfers to remote servers through a proxy server, select the appropriate proxy server options:
  - a. Select **Use Proxy**.
  - b. Select one of these 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 event. Then select the appropriate proxy server alias to use from the available list.
7. To check the connection to the remote server with or without a proxy server, click **Test Connection**.
  8. To assign partners for the event, do the following:

**Note:**

For virtual folders, use this option only if you want to override the partners configured for the virtual folders.

- a. Select **Assign partner**.
  - b. Click in the text box and do one of the following:
    - Select the partner to assign from the list of configured partners in ActiveTransfer.
    - Type a parameterized value for the partner using the following format:  
`[partner_name], [remote_partner_name]`
9. If you want to include subfolders in the search criteria for the Find action, specify **Folder Depth**. The default value is 1 which restricts the search to the root folder.
  10. If you want to restrict the number of items in the Find action results, specify the **Maximum Items to Find**. The default is 0 which includes all the items that match the search criteria for the Find action.
  11. If you want to narrow the search by the time period in which the file was last modified, specify suitable time details:
    - a. In the **Last file modification** list, select the appropriate time variable to which to apply the time criteria:
      - **Before.** Select this option to specify the time before which files were modified.
      - **Within.** Select this option to specify the time (including the current date) within which files were modified.

**Note:**

You must specify at least one time criteria if you select a time variable.

- b. In the appropriate boxes, type the days, hours, and minutes to which to apply the selected time variable.

**Example:** Let us assume that you have specified the time variable as **Before**, with 2 days and 6 hours as the time variable. When ActiveTransfer executes the Find file action on 30 April, it searches for all files that were modified before 4 pm on 27 April. If you change the time variable to **Within**, when ActiveTransfer executes the Find file action at 12 pm on 30 April, it searches for files that were modified between 28 April and 30 April 4 am.

12. If you want the find operation to fail if no files are found, select **Fail if no files are found**.
13. For **File Stability and Scanning**, if you want to remove files that are being processed from the list of files, select **Exclude files that are being updated**. Then, if you want to delay processing of all files until no further file changes are made, select **Delay processing until all files are available for use**.
14. For **Scan for Files and Check for Stability**, do one of the following:
  - If you want the find operation to scan and check one time only, select **Once**.
  - If you want to check at regular intervals, select **Every** and enter the seconds and minutes.
15. If you want ActiveTransfer to retry a failed find action, specify the number of retries and the retry interval in **Retry [ ] times, at intervals of [ ] second(s)**.
16. If you want to execute an error action if the file operation fails, select **Execute error action**.
17. Click **Save**.
18. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
19. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

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

For example, consider the following sequence of event actions and the ActiveTransfer behavior for each event action:

| <b>Event Action Sequence</b>          | <b>What does ActiveTransfer do?</b>                                                 |
|---------------------------------------|-------------------------------------------------------------------------------------|
| 1. Find files in source <i>A</i>      | Finds files in the given source location <i>A</i> . Let us call these files list 1. |
| 2. Execute Integration Server Service | Executes the Integration Service on file list 1.                                    |

| Event Action Sequence                 | What does ActiveTransfer do?                                                        |
|---------------------------------------|-------------------------------------------------------------------------------------|
| 3. Find files in source <i>B</i>      | Finds files in the given source location <i>B</i> . Let us call these files list 2. |
| 4. Execute Integration Server Service | Executes the Integration Server service on both list 1 and list 2 files.            |
| 5. Encrypt files                      | Encrypts the files in list 1 and list 2.                                            |

## Copying or Moving Files

After you create a basic file copy or move action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

### ➤ To set the properties of a file copy or move action

1. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

2. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

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

NEW-((\*.doc)|(\*\_backup\_\*))

Includes anything starting with NEW- that either ends in .doc, or is followed by the string \_backup\_

3. Select the **Destination URL** to which the file will be copied or moved by doing one of the following:

**Important:**

When you enter file path locations, be sure to end the path with a slash character ("/") to identify the location as a folder and not a file.

- If the destination URL is on your local machine or network, select **File Path** and browse to or enter the location.

**Note:**

To specify a file URL for a shared location, use the following syntax: *FILE:///<host>/SharedFolder/*. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.

- If the destination URL is on a remote machine or network, select **Remote File Path** and browse to or enter the location in the format: *protocol://<host>:<port>/DestinationFolder/*
  - If you are using **Amazon-S3** as your remote path, then configure the **Bucket name**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key**.
  - If you are using **AZURE-FILE** or **AZURE-BLOB** as your remote path, then configure the **Authentication type**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key** as required.
- If the destination URL is a virtual folder in the ActiveTransfer VFS, do the following:
  1. Select **Virtual Folder**
  2. Type in the virtual folder details in the text box or use the browse option.
 

If you use the browse button, the **Select virtual folder** look up window opens.
  3. In the **Select virtual folder** window, select the virtual folder by highlighting the element and click on **Select**.
  4. If you want to point to a subfolder in the virtual folder, append the URL in the text box with the details of the subfolder.

**Note:**

The virtual folder specified here should be configured on the same ActiveTransfer Server instance on which the event is configured.

**Tip:**

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 virtual folder for the remote server in the VFS and configure the **Keystore**, **Keystore Password**,

and **Key Password** parameters. You can then use the Virtual folder that you configured in the **Virtual Folder** option of the **File Path** in the event action. For additional details see [“Associating a Virtual Folder with a Physical Folder Location” on page 127](#).

4. If **File URL** is a third-party HTTP(S) server, clear the **ActiveTransfer HTTP(S) Server** selection and do the following:

**Note:**

This field appears only if the **File URL** specified is an HTTP(S) URL and is not a server variable. For more information on how ActiveTransfer handles remote or external HTTP(S) servers, see [“Connecting to HTTP\(S\) Servers” on page 40](#).

- a. In **Request Method**, select either POST or PUT HTTP request method.
- b. In the **Request Headers** table, add any additional headers and values to use for the HTTP request method in the respective text boxes.

For information on the header information specific to chunking (Transfer-Encoding=chunked) and multipart messages (Content-Type= multipart/form-data), see [“Connecting to HTTP\(S\) Servers” on page 40](#).

5. Select **Create Directory** to enable ActiveTransfer to create the destination folder if the folder specified in **Destination URL** is not present.

If **Destination URL** path does not include a folder, ActiveTransfer copies or moves the file directly to the specified directory path.

6. Type a **User Name** and **Password** for the remote system.
7. If you want to route file transfers to remote servers through a proxy server, select the appropriate proxy server options:
  - a. Select **Use Proxy**.
  - b. Select one of these 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 event. Then select the appropriate proxy server alias to use from the available list.
8. To check the connection to the remote server with or without a proxy server, click **Test Connection**.
9. To assign partners for the event, do the following:

**Note:**

For virtual folders, use this option only if you want to override the partners configured for the virtual folders.

- a. Select **Assign partner**.
- b. Click in the text box and do one of the following:
  - Select the partner to assign from the list of configured partners in ActiveTransfer.
  - Type a parameterized value for the partner using the following format:

[partner\_name], [remote\_partner\_name]

10. Select additional properties for the copy or move action as follows:

| Select this option...                                 | To...                                                                                                                                             |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rename file to</b>                                 | Rename the file to the specified name.                                                                                                            |
| <b>Wait for</b>                                       | Wait for the specified number of seconds before starting the copy or move operation to ensure that an outside process is not writing to the file. |
| <b>Give up after</b>                                  | Stop the copy or move operation if it does not complete within the specified number of seconds.                                                   |
| <b>Retry [ ] times, at intervals of [ ] second(s)</b> | Retry a failed copy or move operation for the specified number of times, at the interval specified in seconds.                                    |
| <b>Resume transfer from the point of interruption</b> | Resume an interrupted copy or move operation from the point of interruption.                                                                      |
| <b>Preserve file modification date</b>                | Retain the time stamp indicating when the file was last modified.                                                                                 |
| <b>Execute error action</b>                           | Execute an error action if the file operation fails.                                                                                              |
| <b>Execute asynchronously</b>                         | Execute the file operation in a different thread so that it does not interfere with other actions.                                                |

11. If you want to execute a SITE command before copy or move operation, then choose the **Command before upload** 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: `SITE LRECL=<record_size> BLKSIZE=<block_size>`.

12. If you are using FTP, FTPS, or FTPES protocols, configure the following additional settings:

- **ASCII Transfer**, to change the file transfer mode to ASCII.
- **Simple Mode**, to change the file transfer mode to simple mode. Select this option if you are transferring files to AS/400 systems.

- If you selected the ASCII mode, select the **Convert Line Endings** option for ActiveTransfer Server to change the line endings of the file. Select **No Change** if you do not want ActiveTransfer Server to alter the line endings.

ActiveTransfer Server uses the **Binary** file transfer mode as the default for **Move** and **Copy** actions.

13. Click **Save**.
14. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
15. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

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

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

Example: An event configured with the following actions:

1. Find action: Find files in **File URL** = *<source folder>*
2. Encrypt action: Encrypt the files
3. Move Action: Moves the files to the **destination URL** = *<destination folder>*

The event results in the following:

1. Find action lists all the files in the *<source folder>*.
2. Encrypt action encrypts all the files listed by the find action.
3. Move action moves the files that are encrypted by the encrypt action to the *<destination folder>*.

## Deleting Files

After you create a basic file delete action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

### ➤ To set the properties of a file delete action

1. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

- If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expression:

|                                           |                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>       | Excludes files with the file URL containing purchaseorder                                                 |
| <code>*/out/*</code>                      | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>               | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc)   (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

- Select additional properties for the file delete action as follows:

| Select this option...                                 | To...                                                                                                 |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Retry [ ] times, at intervals of [ ] second(s)</b> | Retry a failed delete action for the specified number of times, at the interval specified in seconds. |
| <b>Execute error action</b>                           | Execute an error action if the file operation fails.                                                  |
| <b>Execute asynchronously</b>                         | Execute the file operation in a different thread so that it does not interfere with other actions.    |

- Click **Save**.
- If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).

6. If you are finished defining actions for this event, activate the event as described in [“Activating an Event”](#) on page 186.

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

## Encrypting and Decrypting Files

After you create a basic file encryption or decryption action as described in [“Creating a Basic File Operation Action”](#) on page 145, use this procedure to set the properties of the action.

### ➤ To set the properties of a file encrypt or decrypt action

1. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search”](#) on page 25.

2. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                           |                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*\$</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                     | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*)123\$</code>                | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc)   (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

3. In the **Encryption Key File** box, do one of the following:
  - For decrypt operations, enter the name of the private key file (for example, *xyz.pgp*).

**Note:**ActiveTransfer Server can decrypt the file only if the file was encrypted with the corresponding public key.

  - For encrypt operations, enter the name of the public key file (for example, *xyz.pgp*).
4. For decrypt operations, enter the password for the encryption file, in the **Password** box.
5. Select additional properties for the file encrypt and decrypt actions as follows:

| Select this option...                   | To...                                                                                                                           |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Derive file name from input file</b> | Retain the original filename of the encrypted file.                                                                             |
| <b>ASCII Armor</b>                      | Wrap PGP files in BASE64-encoded format to make them more secure when emailing them.                                            |
| <b>Delete original file</b>             | Delete the original file and retain only the decrypted files (for decrypt action) and the encrypted files (for encrypt action). |
| <b>Execute error action</b>             | Execute an error action if the file operation fails.                                                                            |
| <b>Execute asynchronously</b>           | Execute the file operation in a different thread so that it does not interfere with other actions.                              |

6. Click **Save**.
7. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
8. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

An Encrypt action encrypts files passed on from the previous action. 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 action, 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 action for processing. If you have selected **Delete original file**, the original files are deleted. If you configure a Move action after an Encrypt action, the Move action moves the encrypted file and not the original file.

A Decrypt action decrypts files passed on from the previous action and creates decrypted files without the .PGP extension. The source folder location contains both the original files and the

corresponding decrypted files. If you have selected **Delete original file**, the original files are deleted. For example, you have configured a post-processing event which is triggered by a file uploaded to a virtual folder that points to a physical location, say a folder named `incoming`. You have also configured the following actions in the event:

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

After the event 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 action that is configured to execute after the decrypt action, ensure that you do the following:

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

## Renaming Files

After you create a basic file rename action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

### ➤ To set the properties of a file rename action

1. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter `*.zip` to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter `*invoice*.zip` to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

2. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

```
^(?!.*purchaseorder).*
```

Excludes files with the file URL containing purchaseorder

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>*/out/*.*</code>                  | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*)123\$</code>              | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

3. In the **New File Name** box, enter the new file name for the file.
4. Select additional properties for the file rename action as follows:

| Select this option...                                 | To...                                                                                                    |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Retry [ ] times, at intervals of [ ] second(s)</b> | Retry a failed rename operation for the specified number of times, at the interval specified in seconds. |
| <b>Skip sub-items, if parent is already renamed</b>   | Rename a folder but not the files beneath the folder.                                                    |
| <b>Execute error action</b>                           | Execute an error action if the file operation fails.                                                     |
| <b>Execute asynchronously</b>                         | Execute the file operation in a different thread so that it does not interfere with other actions.       |

5. Click **Save**.
6. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
7. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

A “Rename” action renames the files passed on from the previous action. The files that are renamed are not passed on to the next action.

## Unzipping Files

After you create a basic file unzip action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

### > To set the properties of a file unzip action

1. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

2. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                   | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>             | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

3. If you want to delete the original zip file after it is unzipped, select **Delete original zip file**.
4. Select the **Destination URL** to which the contents of the file will be extracted by doing one of the following:

**Important:**

When you enter file path locations, be sure to end the path with a slash character (“/”) to identify the location as a folder and not a file.

- If the destination URL is on your local machine or network, select **File Path** and browse to or enter the location.

**Note:**

To specify a file URL for a shared location, use the following syntax:  
*FILE:///<host>/SharedFolder/*. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.

- If the destination URL is on a remote machine or network, select **Remote File Path** and browse to or enter the location in the format: *protocol://<host>:<port>/DestinationFolder/*
  - If you are using **Amazon-S3** as your remote path, then configure the **Bucket name**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key**.
  - If you are using **AZURE-FILE** or **AZURE-BLOB** as your remote path, then configure the **Authentication type**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key** as required.
- If the destination URL is a virtual folder in the ActiveTransfer VFS, do the following:
  1. Select **Virtual Folder**
  2. Type in the virtual folder details in the text box or use the browse option.
 

If you use the browse button, the **Select virtual folder** look up window opens.
  3. In the **Select virtual folder** window, select the virtual folder by highlighting the element and click on **Select**.
  4. If you want to point to a subfolder in the virtual folder, append the URL in the text box with the details of the subfolder.

**Note:**

The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the event is configured.

**Tip:**

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 virtual folder for the remote server in the VFS and configure the **Keystore**, **Keystore Password**, and **Key Password** parameters. You can then use the Virtual folder that you configured in the **Virtual Folder** option of the **File Path** in the event action. For additional details see [“Associating a Virtual Folder with a Physical Folder Location” on page 127](#).

5. Type a **User Name** and **Password** for the remote system.
6. If you want to route file transfers to remote servers through a proxy server, select the appropriate proxy server options:
  - a. Select **Use Proxy**.
  - b. Select one of these 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 event. Then select the appropriate proxy server alias to use from the available list.
- 7. To check the connection to the remote server with or without a proxy server, click **Test Connection**.
- 8. To assign partners for the event, do the following:
 

**Note:**  
For virtual folders, use this option only if you want to override the partners configured for the virtual folders.

  - a. Select **Assign partner**.
  - b. Click in the text box and do one of the following:
    - Select the partner to assign from the list of configured partners in ActiveTransfer.
    - Type a parameterized value for the partner using the following format:  
 [partner\_name],[remote\_partner\_name]
- 9. If you want to execute an error action if the file operation fails, select **Execute error action**.
- 10. Click **Save**.
- 11. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
- 12. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

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

## Writing Content to a File

After you create a basic write action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

### ➤ To set the properties for the write action

1. In the **Source Filter** box, enter the name of the file to trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

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

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

2. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                   | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>             | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

3. In the **File Path** box, enter the path containing the file to write to.

**Important:**

Be sure to end the path with a slash character (“/”) to identify the location as a folder and not a file.

4. If the file already exists and you want to replace the entire contents of the existing file with the new content, select the **Overwrite** check box.
5. If the file does not exist, type or paste the content to write to the file in the **Contents If File Does Not Exist** box.
6. If you want to insert new content before existing content in the file, select **Add before** and then do one of the following:

- If you want to insert the content at the beginning of the file, select **Beginning of file** and then type or paste the new content in the **Contents** box.
  - If you want to insert the content before a specific string of existing content in the file, select **Find**, enter the string in the box beneath this option, and then type or paste the new content in the **Contents** box.
7. If you want to insert new content after existing content in the file, select **Add after** and then do one of the following:
    - If you want to insert the content at the end of the file, select **End of file** and then type or paste the new content in the **Contents** box.
    - If you want to insert the content after a specific string of existing content in the file, select **Find**, enter the string in the box beneath this option, and then type or paste the new content in the **Contents** box.
  8. If you want to execute an error action if the file operation fails, select **Execute error action**.
  9. Click **Save**.
  10. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
  11. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

The “Write Content to File” action 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 action, the list of files from the previous action is passed on to the subsequent action. The file created or modified by this action is not passed on to the next action.

Example: An event configured with the following actions:

1. Find action: Find files in **File URL** = *<source folder>*
2. Write Content to File action: Writes information regarding the files in a specified file
3. Move Action: Moves the files to the **destination URL** = *<destination folder>*

The event results in the following:

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

## Zippping Files

After you create a basic file zip action as described in [“Creating a Basic File Operation Action” on page 145](#), use this procedure to set the properties of the action.

### ➤ To set the properties for a file zip action

1. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

2. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                   | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*)123\$</code>              | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

3. Select the **Zip File Path** where the file will be zipped by doing one of the following:

#### Important:

When you enter file path locations, be sure to end the path with a slash character (“/”) to identify the location as a folder and not a file.

- If the path is on your local machine or network, select **File Path** and browse to or enter the location.

**Note:**

To specify a file URL for a shared location, use the following syntax: *FILE:///<host>/SharedFolder/*. Make sure that the OS user running the ActiveTransfer Server instance has full access to the shared location.

- If the path is on a remote machine or network, select **Remote File Path** and browse to or enter the location in the format: *protocol://<host>:<port>/DestinationFolder/*.
  - If you are using **Amazon-S3** as your remote path, then configure the **Bucket name**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key**.
  - If you are using **AZURE-FILE** or **AZURE-BLOB** as your remote path, then configure the **Authentication type**, **Folder path**, **Region name**, **Access Key ID**, and **Secret Access Key** as required.
- If the path is a virtual folder in the ActiveTransfer VFS, do the following:
  1. Select **Virtual Folder**
  2. Type in the virtual folder details in the text box or use the browse option.
 

If you use the browse button, the **Select virtual folder** look up window opens.
  3. In the **Select virtual folder** window, select the virtual folder by highlighting the element and click on **Select**.
  4. If you want to point to a subfolder in the virtual folder, append the URL in the text box with the details of the subfolder.

**Note:**

The virtual folder that you select should be configured on the same ActiveTransfer Server instance on which the event is configured.

**Tip:**

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 virtual folder for the remote server in the VFS and configure the **Keystore**, **Keystore Password**, and **Key Password** parameters. You can then use the Virtual folder that you configured in the **Virtual Folder** option of the **File Path** in the event action. For additional details see [“Associating a Virtual Folder with a Physical Folder Location” on page 127](#).

4. Select **Create Directory** to enable ActiveTransfer to create the destination folder if the folder specified in **Destination URL** is not present.

If **Zip File Path** path does not include a folder, ActiveTransfer zips the file directly to the specified directory path.

5. Type a **User Name** and **Password** for the remote system.

6. If you want to route file transfers to remote servers through a proxy server, select the appropriate proxy server options:
  - a. Select **Use Proxy**.
  - b. Select one of these 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 event. Then select the appropriate proxy server alias to use from the available list.
7. To check the connection to the remote server with or without a proxy server, click **Test Connection**.
8. To assign partners for the event, do the following:

**Note:**

For virtual folders, use this option only if you want to override the partners configured for the virtual folders.

- a. Select **Assign partner**.
- b. Click in the text box and do one of the following:
  - Select the partner to assign from the list of configured partners in ActiveTransfer.
  - Type a parameterized value for the partner using the following format:  
`[partner_name],[remote_partner_name]`
9. In the **Zip File Name** box, enter a name for the zip file. Alternatively, you can provide a variable name such as `{stem}.zip` for the zip file name.  
  
For more information about specifying variables, see [“Server Configuration Parameters and Variables” on page 399](#).
10. If you want to execute an error action if the file operation fails, select **Execute error action**.
11. Click **Save**.
12. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
13. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

The “Zip” action compresses a specified file or a set of files and copies the compressed file to the location specified in **Zip File Path**. After the successful execution of the zip action, the original source file(s) and the target zip file are available to the subsequent action. 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 event results in a single zip file. However, if the “Zip” action occurs after parallel processing starts, each thread results in a separate zip file.

## Executing an Integration Server Service

### ➤ To execute an Integration Server service

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, do the following:
  - a. Click the **Select Category** list and select **Execute Integration Server Service**.
  - b. Click the **Package** box and select the Integration Server package that contains the service you want to execute.
  - c. Click the **Service** box and select the service you want to execute.
  - d. Click **OK**.
7. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

8. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                           |                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*\$</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                     | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>               | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc)   (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

9. In the **Configure input to IS service** section, specify values for the input parameters of the service that you select. For more information about the Integration Server services and their signatures, see the Integration Server documentation.

You can directly enter the values for the input parameters or specify a file path variable, *{path}* that contains the value to be passed to the parameter.

10. In the **Extract Service Output** section, list the variables that you want to assign to the output parameters of the service and the path (iData path) of the output parameter.
11. Select the **Execute action even if there are no files** option if you want to execute the action even when no files are passed on to this action from the previous action. For example, you might have a requirement to trigger an Integration Server service from a scheduled event 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.
12. If you want to execute an error action if the file operation fails, select **Execute error action**.
13. Click **Save**.
14. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
15. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

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

## Executing a Script

### > To execute a script

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, click the **Select Category** list, select **Execute Script**, and then click **OK**.
7. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

8. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

`^(?!.*purchaseorder).*`

Excludes files with the file URL containing purchaseorder

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>*/out/*.*</code>                  | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>             | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

- In the **Command** box, type a command. Keep in mind that running a batch (.bat) file requires running cmd.exe at a command prompt and passing it the arguments to execute the batch file.
- In the **Arguments** box, type the command's arguments. For example, enter `{real_path}/archive/{name}:`. If the file is uploaded to /uploads/stuff.zip, it will be copied to /archive/stuff.zip.

**Note:**

The execution of the script takes place in the underlying operating system and cannot be controlled by ActiveTransfer. So, ensure that the script handles the sanitization of the arguments (especially the file name) that are passed to the script to avoid or mitigate security risks.

- In the **Separator** box, type a regular expression to separator arguments.
- In the **Working Directory** box, type the path to the directory where the command will execute. For example, when an application looks for a resource such as a configuration file, the application looks in the location specified here.

**Important:**

Make sure the path ends with "/" to identify the location as a folder and not a file.

You should configure the **Execute Script** action settings depending on your operating system. One example each for the Windows and Unix/Linux platforms are listed below:

- **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 action 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 settings in the Execute Script action.

**Command** /bin/bash

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

**Separator** ;

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

The above configuration settings 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.

13. If you want to execute an error action if the file operation fails, select **Execute error action**.
14. Click **Save**.
15. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
16. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

The “Execute a Script” action runs a script for each file in the list that is passed on to the action by the previous action. 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 a Script” action waits for the script to complete execution before passing on the control to the next action. The script that is executed as part of this action should include an `exit` command so that the execution control is transferred back to ActiveTransfer. This action does not modify the list of files from the previous action.

## Executing a Trading Networks Service

### 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 Network instances in the parameter `mft.aliases.tn`. For details on `mft.aliases.tn`, see [“mft.aliases.tn” on page 400](#).
- If you have ActiveTransfer, list remote server aliases of ActiveTransfer nodes in the parameter `mft.group.aliases`. For details on `mft.group.aliases`, see [“mft.group.aliases” on page 404](#).

Use this procedure to create an event action that sends a file to Trading Networks for processing. For details on how ActiveTransfer and Trading Networks file transfers work, see [“How does ActiveTransfer work with Trading Networks?” on page 19](#).

**> To execute a Trading Networks service**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, click the **Select Category** list, and then select **Execute Trading Networks Service**.
7. In the **Select Type** box and do one of the following:
  - If you want to execute the Trading Networks service `wm.tn:receive` to process XML document types, select **XML**.
  - If you want to execute the Trading Networks service `wm.tn:receive` to process EDI document types, select **EDI**.
  - If you want to execute a particular Trading Networks service to process flat file document types, do the following:
    1. Select **Flat File**.
    2. In the **Package** box, select a package.
    3. In the **Service** box, select your document gateway service for processing and sending the flat file to Trading Networks.

For details on flat file processing, see the Trading Networks documentation.

**Note:**

If you are submitting flat files to a remote Trading Networks instance, you must have the document gateway service defined on your local Integration Server. This local service is used for the configuration of input and output parameters in My webMethods Server. For details on the document gateway service, see the Trading Networks documentation.

8. Click **OK**.
9. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

10. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                           |                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*\$</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                     | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>               | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc)   (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

11. In the **Configure input to IS service** section, specify values 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.

**Note:**

ActiveTransfer post-processing and scheduled events on remote Trading Networks does not support TN\_params document type as input for the Trading Networks Service action execution. For Flat File documents, the input parameter field supports only **String** values for services.

12. In the **Extract Service Output** section, list the variables that you want to assign to the output parameters of the service and the path (iData path) of the output parameter.
13. If you want to execute an error action if the file operation fails, select **Execute error action**.
14. Click **Save**.

15. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action”](#) on page 185.
16. If you are finished defining actions for this event, activate the event as described in [“Activating an Event”](#) on page 186.

*Result:*

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

## Sending Universal Messaging or Broker Notification

---

**Note:**

This feature is deprecated.

➤ **To send an Universal Messaging or Broker notification**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With”](#) on page 64.
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, do the following:
  - a. Click the **Select Category** list and select **Send Universal Messaging/Broker Notification**.
  - b. Click the **Package** box and select the package that contains the Integration Server document type you want to use.
  - c. Click the **Service** box and select the Integration Server document type you want to use.
  - d. Click **OK**.
7. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

8. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).**\$</code>  | Excludes files with the file URL containing purchaseorder                                                 |
| <code>*/out/*</code>                    | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*)123\$</code>              | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

9. If you want ActiveTransfer to provide the path of the target file to the respective service, select **Include file path**. The file path information is available as input parameter `filePath`.
10. If you want to populate the `fileContent` parameter, select **Include file content**.
11. 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 Universal Messaging, Broker, and Integration Server documentation.
12. If you want to execute an error action if the file operation fails, select **Execute error action**.
13. Click **Save**.
14. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
15. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

The “Send Universal Messaging/Broker Notification” action, sends an Universal Messaging or Broker notification for each file in the list that is passed on to the action by the previous action. This action does not modify the list of files from the previous action.

## Sending an Email Message

---

Use this procedure to configure sending of emails for file actions.

### > To send an email message

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, click the **Select Category** list, select **Send Email**, and then click **OK**.
7. In **Source Filter**, type the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

8. If you want to use a regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*\$</code>   | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                   | Include files with the file URL containing the folder out                                                 |
| <code>^a bc(.*?)123\$</code>            | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

- Address the email by entering valid email addresses in the **From**, **To**, **CC**, and **BCC** boxes.

The value you specify for **From** overrides the value specified in the `mft.user.email.from` parameter for this action. For more information about this parameter, see [“Server Configuration Parameters” on page 400](#).

- In the **Subject** box, enter text to appear in the subject line of the email (for example, `Disconnect:?User %user_name%`).

The value you specify overrides the value specified in the `mft.user.email.subject` parameter for this action. For more information about this parameter, see [“Server Configuration Parameters” on page 400](#).

- To assist you in completing the body of the email, several examples of common email messages are available. Select the appropriate template from the **Variables/Template** list.

- Modify the content in the **Body** box, or type your own text.

You can use variables in the body of the email. For more information, see [“Server Variables” on page 411](#) [“Server Configuration Parameters and Variables” on page 399](#).

- If you want to execute an error action if the file operation fails, select **Execute error action**.

- Click **Save**.

- If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).

- If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

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

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

## Writing File Content to the Database

---

### > To write file content to the database

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, do the following:
  - a. Click the **Select Category** list and select **Write File to Database**.
  - b. Click the **Package** box and select the package that contains the service you want to execute.
  - c. Click the **Service** box and select the service you want to execute.
  - d. Click **OK**.
7. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

You can use wildcard characters to filter the file names. For example, enter \*.zip to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to trigger the event 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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

8. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                           |                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>       | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                     | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>               | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc)   (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

9. If you want ActiveTransfer to provide the path of the target file to the respective service, select **Include file path**. The file path information is passed to the service as input parameter *filePath*.
10. If you want to pass the contents of the file to the service, select the **Include file content** check box and select the transmission method (**as bytes** or **as stream**). The file content is passed to the service as input parameters *fileContent* and *fileBytes*, or as *fileContent* and *fileStream*. Code your input parameter as *fileContent* + *fileBytes* or *fileContent* + *fileStream*.

**Note:**

Selecting this check box is not necessary 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).

11. Specify values for the input parameters of the service that you selected, as required.
12. If you want to execute an error action if the file operation fails, select **Execute error action**.
13. Click **Save**.
14. If you selected the **Execute error action** check box, define an error action as described in [“Defining an Error Action” on page 185](#).
15. If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

The “Write File to Database” action 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 byte or stream form to the service according to the format that the service’s input signature requires. This action does not modify the list of files from the previous action.

## Jumping to a Designated Action

---

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

### » To define a Jump action

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab that contains the event for which you are creating the Jump action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, click the **Select Category** list and select **Jump Action**.
7. Type an action name in **Action Name** or retain the name that is automatically assigned by ActiveTransfer Server.

**Note:**

Each action in an event must have a unique name. ActiveTransfer Server assigns a default name for an action which is the action type itself. For example, `Jump Action` for a Jump action. When you add an action that already exists in the event with its default name, ActiveTransfer Server appends the default name with a numeral starting at 1; for example, `Jump Action1`.

8. In the **Source Filter** box, enter the name of the file whose transfer will trigger this event. By default, ActiveTransfer Server considers all files.

**Note:**

You can use wildcard characters to filter the file names. For example, enter `*.zip` to trigger the event only when zip files are uploaded or downloaded. To trigger an event based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter `*invoice*.zip` to trigger the event

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 **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

- If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>*/out/*</code>                    | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>             | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

- If you want to configure ActiveTransfer Server to execute a Jump action based on a condition, specify the **Jump Condition**.

**Note:**

The jump condition has three parts: *server variables*, the *qualifier*, and the *value of the server variables*. For example, `{ext} Equals xml` triggers a Jump action for all XML files. For additional details on configuring jump conditions, see [“Working with Jump Conditions” on page 423](#).

- Specify the **Jump to action**.
- If you want to execute an error action if the file operation fails, select **Execute error action**.
- Click **Save**.
- If you selected **Execute error action**, define an error action as described in [“Defining an Error Action” on page 185](#).
- If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

*Result:*

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

## Excluding Files from an Action

---

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

### » To define an Exclude action

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click the tab that contains the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event in the event list.
5. In the **Actions** section, click the **Select Action** list.
6. In the resulting dialog box, click the **Select Category** list and select **Exclude Action**.
7. Type an action name in **Action Name** or retain the name that is automatically assigned by ActiveTransfer Server.
8. In the **Source Filter** box, enter the name of the file that you want to exclude in the actions following this action. By default, ActiveTransfer Server considers all files.

#### Note:

You can use wildcard characters to exclude files. For example, enter \*.zip to exclude zip files. To exclude a file based on a name string in the zip files, use the name string in the **Source Filter** box, preceded and followed by wildcard characters. For example, enter \*invoice\*.zip to exclude files based on the file URLs, where zip files contain the character string invoice in their file names. If you define a **Source Filter** for an action, the action acts only on the files that are filtered out.

For information on the use of wildcards in ActiveTransfer Server, see [“Use of Special Characters in Search” on page 25](#).

9. If you want to use regular expression in the source filter, specify a valid regular expression in **Source Filter** and select **Use regular expression**.

Examples for regular expressions:

|                                         |                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>^(?!.*purchaseorder).*</code>     | Excludes files with the file URL containing purchaseorder                                                 |
| <code>.*out/.*</code>                   | Include files with the file URL containing the folder out                                                 |
| <code>^abc(.*?)123\$</code>             | Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def |
| <code>NEW-((*.doc) (*_backup_*))</code> | Includes anything starting with NEW- that either ends in .doc, or is followed by the string _backup_      |

- If you want to execute an error action if the file operation fails, select **Execute error action**.
- Click **Save**.
- If you selected **Execute error action**, define an error action as described in [“Defining an Error Action” on page 185](#).
- If you are finished defining actions for this event, activate the event as described in [“Activating an Event” on page 186](#).

## Defining an Error Action

You can have ActiveTransfer execute an error action if any of the configured actions for a post-processing or scheduled event fail. You can use any of the event actions that ActiveTransfer offers as the defined error action. For example, if a file copy action fails, you can use the Send Email action to notify an administrator of the failure.

The error action is subject to the following conditions:

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

### > To define an error action

- In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
- Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).

3. Click the tab containing the event for which you are creating the file operation action (**Post-Processing Events** or **Scheduled Events**).
4. Select the event from the event list.
5. In the **Actions** section, click the **Select Error Action** list, highlighted in pink.
6. In the resulting dialog box, click the **Select Category** list, and then select the type of action you want to execute if an error occurs. For more information about these actions, see [“Defining Actions to Execute when an Event Is Triggered” on page 144](#).
7. Define the properties for the selected error action. For more information, see the reference table in [“Defining Actions to Execute when an Event Is Triggered” on page 144](#).
8. Click **Save**.
9. If you are finished defining event and error actions for this event, activate the event. See [“Activating an Event” on page 186](#).

## Activating an Event

---

By default, a newly created post-processing or scheduled event is inactive. This enables you to work on configuring the event without any concern that the partially configured event is actually running. After you have fully configured the event, you can activate it to put it into service.

You can also select and delete more than one event at a time. For more information on how to delete multiple events, see [“Activating, Deactivating, and Deleting Multiple Events” on page 187](#).

### > To activate an event

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click either the **Post-Processing Events** tab or the **Scheduled Events** tab.
4. Select the event from the event list.
5. Select the **Active** check box beneath the event description.
6. Click **Save**.

To deactivate an event, clear the **Active** check box.

## Activating, Deactivating, and Deleting Multiple Events

You can select multiple post-processing events or scheduled events to activate, deactivate, or delete in a single action.

### ➤ To activate, deactivate, or delete multiple events

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Click either the **Post-Processing Events** tab or the **Scheduled Events** tab.
4. In the event list, select the rows corresponding to the required events.

#### Tip:

Each page of the event list displays a maximum of 50 events. Only select the events visible in a single page.

5. Do one of the following:

Click...

To...

**Activate**

Activate all selected events.

#### Note:

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

**Deactivate**

Deactivate all selected events.



Delete all selected events.

You can even delete active events. If you delete any event being executed at the time of deletion, the though the event is deleted, ActiveTransfer completes the event execution.

6. Click **OK** to confirm the action.
7. If you have more events to select in additional pages of the event list, click **Next >>** or the required page number, and repeat steps 4 to 6.

## Parameterizing Scheduled 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.

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

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management > Scheduled Events** tab.
2. Select the event in the event list or add a new event.
3. In the **Actions** section, click the **Select Action** list.
4. Select the action that you want to configure.
5. 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 188](#).

6. Click **Save**.

## Additional Information on Parameterizing Event Actions

- 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:

|              |                   |
|--------------|-------------------|
| 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     |
|                | Last Modification Days    |
|                | Last Modification Hours   |
|                | Last Modification Minutes |
|                | Retry Interval            |
|                | Retry Count               |
|                | Copy                      |
| Rename file to |                           |
| Source Filter  |                           |
| File Name      |                           |
| Wait for Sec   |                           |
| Give up After  |                           |
| Retry Interval |                           |
| Decrypt        | Decryption Key File       |
|                | Source Filter             |
| Delete         | Retry Interval            |

| <b>Action</b>  | <b>Action Settings</b> |
|----------------|------------------------|
| Send Email     | Retry Count            |
|                | From                   |
|                | To                     |
|                | CC                     |
|                | BCC                    |
|                | Subject                |
|                | Body                   |
| Encrypt        | Source Filter          |
|                | Decryption Key File    |
| Execute Script | Source Filter          |
|                | Command                |
|                | Arguments              |
|                | Separator              |
|                | Working Directory      |
| Jump           | Source Filter          |
|                | variable               |
|                | variable2              |
| Move           | Source Filter          |
|                | 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          |

| Action        | Action Settings |
|---------------|-----------------|
|               | 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   |

## Parameterizing Scheduled Events to Poll Source URLs and Transfer Files to Destination URLs

Parameterize only those scheduled events that you have set to run in `Manual` mode. If you parameterize an event action scheduled to run at a specific time, the event fails or gives you unexpected results because you cannot assign values to the parameterized settings at runtime.

➤ **To configure a parameterized event to transfer files from a set of source URLs to the corresponding destination URLs**

1. Create a scheduled event with **event type**, `manual`.
2. Add a find action to this event and set the value of the property `FindURL` to `[myFindURL]`.
3. Add a copy action to this event and set the value of the property `DestinationURL` to `[myDestinationURL]`.
4. Run the service `wm.mft.schedule:executeEventwith` following values:
  - Create an `eventParams` entry for each parameterized event setting, type in the *name* of the setting and specify a *value* to the parameterized setting.
  - `scheduleName = Name of the event`
  - `eventParams[0]\name = myFindURL`
  - `eventParams[0]\value = <source path>`
  - `eventParams[1]\name = myDestinationURL`

- `eventParams[1]\value = <destination path>`

For information on the event action settings that you can parameterize, see `wm.mft.schedule.executeEvent` in *webMethods ActiveTransfer Built-In Services Reference*.

## Examples of Event Configurations and Actions

Let us configure a scheduled event, `ParamEvent` which finds a set of files that match the filter `invoice*` in a remote server and copies the files to another remote server after renaming the files. Let us parameterize the source URL and the destination URL in the event actions.

1. Create a new scheduled event, `ParamEvent`.
2. Set the event criteria **Execute actions** to `Manual`.
3. Configure a find action in the event and parameterize the **Find URL** field as follows:
  - Select the **Remote File Path** option.
  - Type in `[sourceURL]` in the field.
  - Specify `invoice*` in the **File Name** field.
4. Configure a copy action after the find action and parameterize the **Destination URL** as follows:
  - Select the **Remote File Path** option.
  - Type in `[destinationURL]` in the field.
  - Configure the **Rename file to** option as `{stem}_processed{ext}`
5. Execute the service `wm.mft.schedule:executeEvent` as follows:
  - Create an `eventParams` entry for each parameterized event setting, type in the *name* of the setting and specify a *value* to the parameterized setting.
  - `scheduleName = ParamEvent`
  - `eventParams[0]\name = [sourceURL]`
  - `eventParams[0]\value = ftp://enterprise.ftp.server/invoices/partner1/`
  - `eventParams[1]\name = [destinationURL]`
  - `eventParams[1]\value = ftp://partner1.ftp.server:21/incoming/invoices/`

Let us consider the following files in the source folder,

`ftp://enterprise.ftp.server/invoices/partner1/`

```
P1-currentmonth-invoice.xml
P1-currentmonth-invoice.pdf
P1-currentmonth-details.xml
P1-currentmonth-ack.xml
```

*Result:* After the successful execution of the event, ParamEvent the /incoming/invoices/ folder on the ftp://partner1.ftp.server server contains the following files:

P1-currentmonth-invoice\_processed.xml P1-currentmonth-invoice\_processed.pdf

## Examples for Configuring an Event

The examples specified in this section show how you can configure events with up to two actions.

### Scheduled Event:

Let us configure a scheduled event, Payables that consists of two actions - find and copy. The event when triggered, finds the monthly invoice for a specific partner in the Enterprise's server and copies the same to the partners's FTP server on the fourth day of the month. You can configure such an event as follows:

- Create a new scheduled event, Payables.
- Schedule the event to run on the fourth day of every month. Configure a new schedule for the event with the following parameters:

|                        |         |
|------------------------|---------|
| <b>Execute Actions</b> | Monthly |
| <b>Days of Month</b>   | 4       |
| <b>Hours</b>           | 17      |

- Define a find action in the event with the following parameters:

|                 |                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File URL</b> | Select the <b>Virtual Folder</b> option and browse to a folder in the VFS say, EnterpriseFTP<br><br>This virtual folder is mapped to a remote server,<br>ftp://enterprise.ftp.server/invoices/partner1/<br>in the <b>Virtual Folder Management</b> page.<br><br>The folder invoices/partner1 in the enterprise.ftp.server contains the following files before the event is executed: |
|                 | P1-currentmonth-invoice.xml<br>P1-currentmonth-invoice.pdf<br>P1-currentmonth-details.xml<br>P1-currentmonth-ack.xml                                                                                                                                                                                                                                                                 |

**Note:**

The virtual folder used in this example should already exist in the Active Transfer VFS.

**File name** \*invoice\*

- Define a copy action in the event after the `find` action with the following parameters:

**Destination URL** Select the **Virtual Folder** option and browse to a folder in the VFS say, `Partner1FTP`

This virtual folder is mapped to a remote server,  
`ftp://partner1.ftp.server:21/incoming/invoices/`  
in the **Virtual Folder Management** page.

Let us assume that the folder  
`incoming/invoices` in the partner's FTP server has no files.

**Retry [ ] times, at intervals of [ ] second(s)** Select the checkbox and input the values, 2 for retry times and 10 for retry interval.

- Activate the event, `Payables`.

Result -When the event executes successfully, the result is as follows: The `incoming/invoices` folder in the partner's FTP server contains the following files:

`P1-currentmonth-invoice.xml`  
`P1-currentmonth-invoice.pdf`

**Note:**

If the Copy action fails the first time, ActiveTransfer will retry the copy action two more times at intervals of 10 seconds.

Post-processing Event:

Let us configure a post-processing event, `Notify` which is triggered when a file is uploaded to the `invoices` folder corresponding to a specific partner in the enterprise's server. The event when executed sends an email to the partner with the subject - `Invoice for the month - {MM}/{yy}` and specifies the URL of the file. You could configure such an event as follows:

- Create a new post-processing event.
- Define the trigger for the event as follows:

**Execute the actions below when a user** uploads files

**The folder name is** Select the **The following name:** option and browse to a folder in the VFS say, `EnterpriseFTP`

This virtual folder is mapped to a remote server

ftp://enterprise.ftp.server/invoices/partner1/  
in the **Virtual Folder Management** page.

The folder invoices/partner1 in the enterprise.ftp.server contains the following files:

```
P1-currentmonth-invoice.xml
P1-currentmonth-invoice.pdf
P1-currentmonth-details.xml
P1-currentmonth-ack.xml
```

|                                        |                                   |
|----------------------------------------|-----------------------------------|
| <b>The file transfer status is</b>     | Success                           |
| <b>The operation is carried out by</b> | Any user                          |
| <b>Execute the actions</b>             | After the user exits all sessions |

- Define a send\_email action in the event with the following parameters:

|                             |                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source Filter</b>        | */invoice/*.pdf                                                                                                                                    |
|                             | For information on the use of wildcards in ActiveTransfer Server, see <a href="#">“Use of Special Characters in Search”</a> on page 25.            |
| <b>From</b>                 | %user_email%                                                                                                                                       |
| <b>To</b>                   | incoming@partner1.com                                                                                                                              |
| <b>Subject</b>              | Invoice for the month - {MM}/{yy}                                                                                                                  |
| <b>Variables / Template</b> | Name to current file                                                                                                                               |
| <b>Body</b>                 | Modify the template as follows: The current invoice is available for download at:<br>ftp://enterprise.ftp.server/invoices/partner1/%the_file_name% |

- Activate the event, Notify.

Result - When the event executes successfully, an email is sent to partner1 with the following content: Subject Invoice for this month -12/2014 The current invoice is available for download at:ftp://enterprise.ftp.server/invoices/partner1/P1-currentmonth-invoice.pdf



# 10 Monitoring ActiveTransfer

---

|                                                       |     |
|-------------------------------------------------------|-----|
| ■ Overview .....                                      | 198 |
| ■ Monitoring File Transaction Activity .....          | 198 |
| ■ Monitoring Events .....                             | 201 |
| ■ Viewing ActiveTransfer Analytical Information ..... | 202 |

## Overview

---

You can monitor the activity within your environment using the following:

- **File Transactions** log. ActiveTransfer Server logs all file transactions. You can filter file transactions based on such criteria as period of time, trigger source, file name, status of the file transfer, and view additional details for a specific file transaction. For more information about viewing the file transaction log, see [“Monitoring File Transaction Activity” on page 198](#).
- **Event Log**. ActiveTransfer Server logs the event details for all (post-processing and scheduled) events. You can filter the event log based on the criteria: period of time, event type, and status. For more information about viewing event logs, see [“Monitoring Events” on page 201](#).
- **Analytics** dashboard. ActiveTransfer analytics dashboard provides insight into all the file transfers happening within your environment by showing metrics, making comparisons, and summarizing key activity. For more information about viewing this information, see [“Viewing ActiveTransfer Analytical Information” on page 202](#).

## Monitoring File Transaction Activity

---

To monitor file transaction activity on your ActiveTransfer Server, you first define a file transaction filter to populate a search results list. You can then view the details of a transaction and the activities that occurred during a transaction.

### Defining a File Transaction Filter

You define a file transaction filter to narrow the search results list to a specific time period, transfer direction, protocol, partner or user, or status.

#### ➤ To define a file transaction filter

1. In My webMethods: **Monitoring > Integration > Managed File Transfer > File Transactions**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. In the **Filters** section, define a filter for the file transactions you want to view, based on the following criteria:
  - For **Period of Time**, select from the available time periods in the list or specify a custom date range, and then click **OK**.
  - For **Trigger Source**, select the source that triggered the file transaction (**All, User, Event, or Trading Networks**).
  - If you have selected the **Trigger Source User**, you can specify additional filters for:
    - **Partner**, select **All Partners**. Or, select **The Following Partner**, click the box to select a partner, and then click **OK**.

- **User**, select **All Users**. Or, select **The Following User**, click the box to select a user, and then click **OK**.
  - **Direction**, select a file transaction direction (**Upload**, **Download**, or **All Directions**).
  - **Protocols**, select one or more transmission protocols. You can select all protocols, all secure protocols (FTPS, SFTP, HTTPS, SCP, and WebDAVs), or all protocols that are not secure (HTTP, FTP, and WebDAV). You can also select individual protocols by selecting the appropriate check boxes.
  - If you have selected the **Trigger Source Event**, you can specify additional filters for:
    - **Source Path**,
    - **Destination Path**,
  - For **Status**, select whether to show all transactions or only the successful or unsuccessful ones.
  - If you want to search for the **Comment Text** and **Activities** related information, type the information in the **Comment** box.
  - If you want to search the transactions for matches to a specified file name, type the same in the **File Name** box.
  - For **File Name**, enter the partial or complete file name based on which you want to filter out or search the event log entries. To search for a file with the exact name entered in **File Name**, select the **Match whole word** checkbox.
  - For **Transaction ID**, enter the transaction ID of the file transfer.
4. If you want to search for a specific file transfer transaction ID, type the transaction ID in **Transaction ID**.

## Viewing File Transaction Details

You can view detailed information for any of the file transactions shown in the results list.

### ➤ To view the details of a file transaction

1. Determine the specific file transactions you want to appear in the results list, as described in [“Defining a File Transaction Filter” on page 198](#).
2. In the results list, click the file transaction you want to work with.
3. You can view the message generated by ActiveTransfer Server for the transaction in **Comment Text**.
4. View the following information in the **Transaction Details** section of the **Details** tab:

| Field                             | Description                                                                   |
|-----------------------------------|-------------------------------------------------------------------------------|
| <b>Trigger Source</b>             | Source of the file transaction. Could be a <b>User</b> or an <b>Event</b> .   |
| <b>User</b>                       | Name of the user who executed the file transfer.                              |
| <b>Transfer Date (Start time)</b> | Start time of the transfer.                                                   |
| <b>Elapsed Time</b>               | Amount of time that the file transfer took to complete.                       |
| <b>File Name</b>                  | Name of the file that was transferred.                                        |
| <b>File Size</b>                  | Size of the file.                                                             |
| <b>Transfer Status</b>            | Whether the transfer was successful or unsuccessful.                          |
| <b>Transaction ID</b>             | Transaction ID for the file transfer.                                         |
| <b>Transfer Direction</b>         | Direction of the transaction (upload or download).                            |
| <b>Protocol</b>                   | Protocol used for the file transfer.                                          |
| <b>Port Name</b>                  | Name of the ActiveTransfer Server port on which the file transfer took place. |
| <b>Client IP Address</b>          | IP address of the client that asked for the file transfer.                    |
| <b>Compression</b>                | Whether compression was used to perform the file transfer.                    |

## Viewing File Transaction Activities

You can view activities that occurred as part of a file transaction.

### ➤ To view file transaction activities

1. Determine the specific file transactions you want to appear in the results list, as described in [“Defining a File Transaction Filter” on page 198](#).
2. In the results list, click the file transaction you want to work with.
3. Click the **Activities** tab.
4. View the following file transaction activity information:

| Field            | Description                                          |
|------------------|------------------------------------------------------|
| <b>Timestamp</b> | Date and time of the associated activity.            |
| <b>Status</b>    | Whether the transfer was successful or unsuccessful. |

| Field                | Description                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------|
| <b>Type</b>          | The event type, post-processing or Scheduled event                                               |
| <b>Event Name</b>    | Name of the event in ActiveTransfer Server.                                                      |
| <b>Brief Message</b> | Actual activity executed during the file transaction.                                            |
| <b>Full Message</b>  | Full list of the parameters and their values that were applied to the file transaction activity. |

## Monitoring Events

To monitor events on your ActiveTransfer Server, you first define a filter to populate a search results list. You can then view the details of an event and the activities that occurred during the event.

### Defining an Event Filter

You define an event filter to narrow the search results list to a specific time period, event type, or status.

#### > To define an event filter

1. In My webMethods: **Monitoring > Integration > Managed File Transfer > Event Log**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. In the **Filters** section, define a filter for the events you want to view, based on the following criteria:
  - For **Period of Time**, select from the available time periods in the list or specify a custom date range, with a time range in the *HH:MM:SS* (12-hour clock) format, and then click **OK**.
  - For **Event Type**, select the type of event (**Post-Processing**, **Scheduled**, or **All**).
  - For **Status**, select whether to show all events or only the successful or unsuccessful ones.
4. Click **Apply** to apply the filter.

### Viewing Event Details

You can view detailed information for any of the events shown in the results list.

#### > To view the details of an event

1. Determine the specific events you want to appear in the results list, as described in [“Defining a File Transaction Filter”](#) on page 198.
2. In the results list, click the event you want to work with.
3. View the following information in the **Event Details** section of the **Details** tab:

| Field             | Description                                               |
|-------------------|-----------------------------------------------------------|
| <b>Start Time</b> | Time at which the event was triggered.                    |
| <b>Event Type</b> | Type of event, <b>Post-Processing</b> or <b>Scheduled</b> |
| <b>Status</b>     | Whether the event was successful or unsuccessful.         |

## Viewing Event Activities

You can view activities that occurred as part of an event.

### > To view event activities

1. Determine the specific events you want to appear in the results list, as described in [“Defining a File Transaction Filter”](#) on page 198.
2. In the results list, click the event you want to work with.
3. Click the **Activities** tab.
4. View the following event activity information:

| Field                | Description                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------|
| <b>Timestamp</b>     | Date and time of the associated activity.                                                        |
| <b>Status</b>        | Whether the event was successful or unsuccessful.                                                |
| <b>Type</b>          | The event type, post-processing or Scheduled event                                               |
| <b>Brief Message</b> | Actual activity executed during the file transaction.                                            |
| <b>Full Message</b>  | Full list of the parameters and their values that were applied to the file transaction activity. |

## Viewing ActiveTransfer Analytical Information

---

You can view ActiveTransfer analytical information by way of the following components:

- The analytics user interface in My webMethods: **Monitoring > Integration > Managed File Transfer > Analytics**.
- Software AG MashZone Server and MashApps created with Software AG MashZone. Both contain predefined formats for ActiveTransfer analytical information. For instructions on configuring MashZone, see [“Configuring MashZone NextGen” on page 47](#).
- ActiveTransfer data sources that contain the analytical data. Software AG MashZone Server connects to the appropriate data sources, retrieves the data to create the analytical details, and displays this information in the Analytics user interface. If you want to view analytical details other than those that ActiveTransfer provides, contact your Software AG sales representative.

**Note:**

Analytical details are available only in English. However, Software AG MashZone supports the localization of those details. For more information, refer to the MashZone documentation.

## Types of Analytical Information

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

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

## Viewing Analytical Details in My webMethods

### ➤ To view analytical details in My webMethods

1. In My webMethods: **Monitoring > Integration > Managed File Transfer > Analytics**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. In the **Filters** section, specify filter criteria for the file transactions for which you want to view analytical details:
  - For **Period of Time**, select from the available time periods in the list or specify a custom date range, and then click **OK**.
  - For **Direction**, select a file transaction direction (**Upload**, **Download**, or **All Directions**).
  - For **Status**, select a file transaction status (**Success**, **Failure**, or **Show All**).

- For **Sender**, select **All Partners** or select **The Following Partner** and click the box to select a partner, and then click **OK**.
- For **Receiver**, select **All Partners** or select **The Following Partner** and click the box to select a partner, and then click **OK**.
- For **User**, select **All Users** or select **The Following User** and click the box to select a user, and then click **OK**.
- For **Protocols**, select one or more transmission protocols. You can select all protocols, all secure protocols (FTPS, SFTP, HTTPS, SCP, and WebDAVs), or all protocols that are not secure (File, HTTP, FTP, and WebDAV). You can also select individual protocols by selecting the appropriate check boxes.

**Note:**

You can click **Reset** at any time to restore the default filter settings.

4. Click **Apply**.

# 11 Managing and Viewing Log Information

---

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| ■ Managing Log Files .....                                             | 206 |
| ■ Configuring Logging in the Installation Directory .....              | 206 |
| ■ Setting Up Audit Logging from the My webMethods User Interface ..... | 209 |
| ■ Viewing ActiveTransfer Server Logs in My webMethods .....            | 209 |
| ■ Viewing Server Information in My webMethods .....                    | 210 |
| ■ Searching for Keywords in ActiveTransfer Server Log .....            | 211 |
| ■ Filtering ActiveTransfer Server Logs for Keywords .....              | 211 |
| ■ Viewing User Information in My webMethods .....                      | 212 |
| ■ Viewing Audit Logs in My webMethods .....                            | 213 |

## Managing Log Files

---

ActiveTransfer uses the Integration Server OSGi log framework. Log entries for ActiveTransfer Server and ActiveTransfer Gateway are available in the default log file, ActiveTransfer.log located in the *Integration Server\_directory* \profiles\IS\_default\logs directory.

The ActiveTransfer.log file contains details of the run-time operations that ActiveTransfer Server performs, including connecting to clients, transferring files, and executing events. The log file also contains information and error messages related to configuration activities that you perform using My webMethods pages such as Server Management, Templates, and Event Management.

The ActiveTransfer.log file name and location are configurable. For details on how to configure the log name, location, and log level see [“Configuring Logging in the Installation Directory” on page 206](#).

## Configuring Logging in the Installation Directory

---

Use this procedure to configure a new log appender with log file name, log file location, and logging levels on both, ActiveTransfer Server and ActiveTransfer Gateway.

### ➤ To configure ActiveTransfer logging

1. In ActiveTransfer Server installation, navigate to the following directory:

```
Integration Server_directory \IS_default\configuration\logging
```

2. Using a text editor, open the log4j2.properties file.
3. Follow these steps to configure the log appender, which specifies the log file name, log file location, and global log level:
  - a. Ensure that the following entries are present. If not, then add them:

```
logger.mft.name = com.softwareag.mft
logger.mft.level = info
logger.mft.additivity = false
logger.mft.appenderRef.rolling.ref = ActiveTransfer.RollingLogFile
appender.mft.type = RollingFile
appender.mft.name = ActiveTransfer.RollingLogFile
appender.mft.fileName =
 Integration Server_directory
 \profiles\IS_default\logs\ActiveTransfer.log
appender.mft.filePattern =
 Integration Server_directory
 \profiles\IS_default\logs\ActiveTransfer-%i.log.gz
appender.mft.layout.type = PatternLayout
appender.mft.layout.pattern = %d{DEFAULT} %-5p [%-40.60c{10}]
[%scgMsgKey] - %m%n
appender.mft.policies.type = Policies
appender.mft.policies.size.type = SizeBasedTriggeringPolicy
appender.mft.policies.size.size=10MB
```

```
appender.mft.strategy.type = DefaultRolloverStrategy
appender.mft.strategy.max = 10
```

- b. In the log appender, make suitable modifications to the log file name, log file location, and global log level:

```
appender.mft.fileName = Integration Server_directory
\profiles\IS_default\logs\ActiveTransfer.log
```

Provides the log file location and log file name. Make the following modifications:

- In place *Integration Server\_directory*, specify the exact Integration Server installation directory, or provide any other location of your choice for the log file.
- If required, you can modify the default log file name, *ActiveTransfer.log*, to a file name of your choice.

```
logger.mft.level = info
```

Is the default log level. You can modify it, if required. The possible log levels are:

- fatal: Severe errors that might cause ActiveTransfer to abort.
- error: Errors that caused during the execution of ActiveTransfer operations.
- info: Informational messages about ActiveTransfer events.
- warn: Non-critical errors that might potentially lead to unexpected results.
- debug: Debug information for errors and analysis.
- trace: Trace information for analysis.
- off: Turn off logging. If you turn off logging important log messages are not logged. Not recommended at the global level.

**Note:**

- If you use *off*, important log messages are not logged. Software AG does not recommend its use at the global level.
- *trace* and *debug* log levels will result in large amount of log messages for analysis.

**Note:**

If you omit the next step, the global setting for the log level is applied to all modules unless you set the log modules from the user interface. For details on how set up audit

logging for modules or sub-modules from the user interface, see [“Setting Up Audit Logging from the My webMethods User Interface”](#) on page 209.

4. To specify specific log levels for a module or sub-module, add the following logger entries for the relevant modules or sub-modules:

```
logger.module_submodule.name = value
logger.module_submodule.level = info
```

Where, *module or sub-module* can be:

| Module           | Sub-Module | Value                                    |
|------------------|------------|------------------------------------------|
| Port             |            | com.softwareag.mft.port                  |
| Port             | ftp        | com.softwareag.mft.port.ftp              |
| Port             | sftp       | com.softwareag.mft.port.sftp             |
| Port             | http       | com.softwareag.mft.port.http             |
| Port             | message    | com.softwareag.mft.port.message          |
| Event            |            | com.softwareag.mft.event                 |
| External_Session |            | com.softwareag.mft.external.session      |
| External_Session | ftp        | com.softwareag.mft.external.session.ftp  |
| External_Session | sftp       | com.softwareag.mft.external.session.sftp |
| External_Session | http       | com.softwareag.mft.external.session.http |
| External_Session | file       | com.softwareag.mft.external.session.file |
| Asset            |            | com.softwareag.mft.asset                 |
| Common           |            | com.softwareag.mft.common                |
| Database         |            | com.softwareag.mft.database              |
| Tunnel           |            | com.softwareag.mft.acceleration          |
| Gateway          |            | com.softwareag.mft.gateway               |
| Security         |            | com.softwareag.mft.security              |

**Note:**

- If you do not specify the sub-module, then the log levels of a module is applicable to all the sub-modules of the module. For example, the log level for Port is applicable to Port, Port\_ftp, Port\_sftp, Port\_http, and Port\_message.
- The messages related to the communication between ActiveTransfer Server and ActiveTransfer Gateway are logged in the Port and External Session modules in ActiveTransfer Gateway. The default log level for these messages is debug.

- The messages related to the communication between an external client and ActiveTransfer Server or ActiveTransfer Gateway are logged in the Port module. These messages include commands interchanged, response to commands, and HTTP(S) request and response headers. The Port module is also used to log messages related to the communication between ActiveTransfer Server and ActiveTransfer Gateway in ActiveTransfer Server. The default log level for these messages is debug.

**Example:**

To get trace level logs for all FTP user sessions, add the following logger entries:

```
logger.external_Ftp.name = com.softwareag.mft.external.session.ftp
logger.external_Ftp.level = trace
```

5. Repeat the procedure in the ActiveTransfer Gateway installation.

## Setting Up Audit Logging from the My webMethods User Interface

Use this procedure to select the ActiveTransfer assets for which ActiveTransfer must create audit logs in the My webMethods user interface.

➤ **To set up audit logging**

1. In My webMethods: **Administration > Integration > Managed File Transfer > MFT Settings**.
2. Select **Create audit logs**.
3. Remove or retain the default selections for the available ActiveTransfer assets.
4. Click **Save**.

*Result:* ActiveTransfer Server immediately creates or stops creating audit logs for the enabled and disabled assets, respectively.

## Viewing ActiveTransfer Server Logs in My webMethods

You can view the contents of ActiveTransfer.log for ActiveTransfer Server in the My webMethods user interface.

**Note:**

ActiveTransfer Gateway logs are not available in My webMethods. To access ActiveTransfer Gateway logs, use the ActiveTransfer.log file available in the configured log directory of the ActiveTransfer Gateway installation: *Integration Server\_directory \profiles\IS\_default\logs\*. For details on how to configure the log file location, see [“Configuring Logging in the Installation Directory” on page 206](#).

➤ **To access ActiveTransfer Server log content in My webMethods**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Log**.
2. Select the server instance. For details, see [“Selecting the Instance to Work With” on page 64](#).
3. Do one of the following:
  - To view logged information for ActiveTransfer Servers, click the **Server Info** tab. For more information, see [“Viewing Server Information in My webMethods ” on page 210](#).
  - To view logged information for ActiveTransfer users, click the **User Info** tab. For more information, see [“Viewing User Information in My webMethods ” on page 212](#).

## Viewing Server Information in My webMethods

---

The **Server Info** tab of the Logs page contains entries for port activity, server login and session information, and data transfer summaries.

The **Servers** section shows the following details about the ActiveTransfer Server:

- Protocol in use
- Host name or external IP address
- Security mode, if applicable
- Number of users connected
- Number of connections processed

The **Info** tab displays the following details about the ActiveTransfer Server:

The **Login Information** section of the **Info** tab shows details about the last login that occurred, the total number of logins, and the total number of successful and unsuccessful login attempts.

The **Data Transferred** section shows the total number of bytes transferred in and out, the number of files uploaded and downloaded, and the number of files sent and received.

The **Speed Information** section shows the average speed of outgoing and incoming transfers.

The **Session Information** section shows the number of concurrent users presently connected, the number of connected sessions, and the number of busy and free threads.

The **Log** tab contains the following:

You can view the ActiveTransfer Server logs on this page. The **find and filter** section provides a search box for keywords in the log entries. For additional details, see [“Searching for Keywords in ActiveTransfer Server Log” on page 211](#). You can also filter the server logs using keywords and choose to display only the log entries containing the keyword, or hide the log entries containing the keyword. For additional details, see [“Filtering ActiveTransfer Server Logs for Keywords” on page 211](#).

---

## Searching for Keywords in ActiveTransfer Server Log

---

You can search for keywords in the ActiveTransfer.log.

➤ **To search for a specific keyword in the ActiveTransfer.log entries**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Log**.
2. Click the **Server Info** tab.
3. In the **Servers** section, click the **Log** tab.
4. Click the **Show Find and Filters** link.
5. Enter the keyword (for example: READ) in the text box below **Find in Log**.
6. Click the colored box next to the **Find in Log** text box to view and select a color for the highlighter, from the color palette.
7. If you want to specify additional keywords for **Find in Log**, click .
8. Click the **Find and Filter** button.

---

## Filtering ActiveTransfer Server Logs for Keywords

---

You can filter the ActiveTransfer.log for specific keywords and choose one of the following display options:

- Only show lines containing this text
- Hide lines containing this text

➤ **To filter the ActiveTransfer Server logs entries for a specific keyword**

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Log**.
2. Click the **Server Info** tab.
3. In the **Servers** section, click the **Log** tab.
4. Click the **Show Find and Filters** link.
5. Enter the keyword (for example: READ) in the text box below **Filter**.

6. Select a display option. **Only show lines containing this text** or **Hide lines containing this text**.
7. If you want to specify additional keywords for **Filter**, click .
8. Click the **Find and Filter** button.

## Viewing User Information in My webMethods

The **User Info** tab enables you to monitor and act on individual user sessions on ActiveTransfer Server. You can view session information by selecting a session in either of the following lists:

- The **Current Sessions** list displays the current sessions on the ActiveTransfer Server.
  - To terminate a session, select the session and click **Terminate Session**.
  - To permanently ban the connected user, select a user session and click **Permanent Ban**. Consult the live log entry for **Accepting connection from:** to determine where the connection originates.
  - To temporarily ban the connected user, select a user session and click **Temporary Ban**.
- The **Recent Sessions** list displays recent live and completed user sessions running on ActiveTransfer Server. This section retains up to 100 sessions, after which older sessions are removed and replaced with newer ones.

For a selected session, the **Session Information** section provides the following information:

| Field                       | Description                                            |
|-----------------------------|--------------------------------------------------------|
| <b>Login Time</b>           | Time that the user logged in to ActiveTransfer Server. |
| <b>Working Directory</b>    | Directory that the user is working on.                 |
| <b>IP</b>                   | IP address of ActiveTransfer Server.                   |
| <b>Bytes Sent</b>           | Bytes sent in the file transfer.                       |
| <b>Bytes Received</b>       | Bytes received in the file transfer.                   |
| <b>Upload Count</b>         | Number of files uploaded.                              |
| <b>Download Count</b>       | Number of files downloaded.                            |
| <b>Overall Speed</b>        | Average speed of the transfer.                         |
| <b>Current Speed</b>        | Current speed of the transfer.                         |
| <b>Position in Transfer</b> | Number of the transfer in the queue.                   |
| <b>File Size</b>            | Size of the file being transferred.                    |

| Field                 | Description                     |
|-----------------------|---------------------------------|
| <b>Time Remaining</b> | Time remaining in the transfer. |

You can view log entries for the selected session in the **Live Log** section. To refresh the log at any point, click **Refresh Log**. For a live update of new server log entries, click **Live update**. For a live scroll of new server log entries, click **Scroll with activity**.

## Viewing Audit Logs in My webMethods

You can view the audit logs for all ActiveTransfer assets for which audit logging is enabled in the Audit Log page.

The audit logs are strictly limited to information about:

- The ActiveTransfer assets, and do not include any linked external Software AG or third party product assets that might be your organization uses. For example, My webMethods Server user profiles, Integration Server services, JDBC pools, and so on.
- Configuration of VFS and partners, but not their behavioral changes caused by dependent assets. For example, let us consider that a VFS referenced in an event. If the VFS path is changed, no audit log is available for the change in the corresponding event.

### ➤ To access audit logs in My webMethods

1. In My webMethods: **Administration > Integration > Managed File Transfer > Audit Log**.
2. If you want to use specific filters to locate the audit logs, click **Filters**.
3. Define a filter for the audit logs you want to view, based on the following criteria:
  - a. In **Period of Time**, select from the available time periods in the list or specify a custom date range, with a time range in the *HH:MM:SS* (12-hour clock) format.
  - b. Click **OK**.
  - c. In **Action**, select the required user action (all, create, update, or delete) affecting the asset type:
  - d. In **Asset Type**, select from the required asset type.
  - e. If you want to filter for actions of specific users, in **User**, select **The Following User**.
  - f. Type the user names, separated by commas and click **OK**.
  - g. In **Asset Name**, type the asset name.

- h. In **Asset ID**, type the asset ID.
  - i. In **Asset Summary**, type the words that the asset summary should include.
4. Click **Apply** to apply the filter.
  5. Select the required audit log from the table to view the summary and details of the log.

# 12 Partitioning the Database

---

|                                                  |     |
|--------------------------------------------------|-----|
| ■ Partitioning the ActiveTransfer Database ..... | 216 |
|--------------------------------------------------|-----|

## Partitioning the ActiveTransfer Database

ActiveTransfer transactional data is stored in the database that is configured in the database component (JDBC pool). Transactional data includes event execution details, file transfer information, and so on. However, if you have large volumes of file transfers or event executions, transactional data can grow quite rapidly and become difficult to maintain.

ActiveTransfer database tables are designed to use the partitioning feature offered by most database types. Database partitioning facilitates better product performance and management of data by storing the data of a single table in separate partitions, which can be managed and accessed independently. For example, the Oracle database supports *Interval Partition* that allows you to partition data in a table by a specified date range or interval. All ActiveTransfer database tables that store run-time data are equipped with a *partition key column* or a column that you can use for partitioning. The database tables and their partition key columns are:

| ActiveTransfer Table    | Partition Key Column | Data Stored in Table is...                                                                          |
|-------------------------|----------------------|-----------------------------------------------------------------------------------------------------|
| MFTTransaction          | TransactionDate      | File transfer information                                                                           |
| MFTEventLog             | PartitionTimestamp   | Event execution details                                                                             |
| MFTActivityLog          | PartitionTimestamp   | Task execution details associated with a file transfer<br><br>Task details for each event execution |
| MFTActivityLogMessage   | PartitionTimestamp   | Activity Log messages that are larger than the maximum value permitted in VARCHAR columns           |
| MFTActivityDetails      | EventExecutionTime   | Attribute details of agent activities                                                               |
| MFTAgentEventLog        | TimeofExecution      | Agent event execution details, at each event execution level                                        |
| MFTAgentActivity        | PartitionTimestamp   | Agent activity details<br><br>Event execution details at the agent level                            |
| MFTAgentActivityDetails | PartitionTimestamp   | Detailed task level information on agent activities                                                 |

# 13 Migrating Assets

---

|                                                                                             |     |
|---------------------------------------------------------------------------------------------|-----|
| ■ Overview .....                                                                            | 218 |
| ■ ActiveTransfer Assets You Can Migrate .....                                               | 218 |
| ■ Migration Methods .....                                                                   | 219 |
| ■ ActiveTransfer Asset Dependencies .....                                                   | 219 |
| ■ How ActiveTransfer Server Detects Assets on the Target System Before Importing Them ..... | 221 |

## Overview

---

You can migrate ActiveTransfer assets from one ActiveTransfer database 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.

### Note:

Merged with server instance asset in Deployer.

- **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 events:** You can migrate post-processing event configuration, including actions to execute when the event is triggered.
- **Scheduled events:** You can migrate scheduled event configuration, including actions to execute when the event 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 in My webMethods. These settings are used to connect ActiveTransfer Server and the MashZone NextGen server to My webMethods, 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*.

## 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><br/>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><br/>If Trading Networks is installed, migrate partner profiles defined in Trading Networks separately.</p>                       |
| Post-processing events                  | Post-processing events have a dependency on users, associated VFS folders, and associated actions 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><br/>If Trading Networks is installed, migrate partner profiles defined in Trading Networks separately.</p>                                               |
| Scheduled events and associated actions | <p>Scheduled events have a dependency on associated VFS folders and partners who have been granted access to the folders.</p> <p><b>Note:</b><br/>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.

When migrating virtual folders, if ActiveTransfer Server finds a matching folder name on the target system, the server updates the folder with the information from the imported folder.

However, this can lead to unexpected results due to the possible conflicts in folder hierarchy and partner association between the source and target systems. If you want to migrate virtual folders, Software AG recommends that you delete the folder on the target system before importing the matching folder from the source system.



# 14 Removing User Data from ActiveTransfer

---

|                                                             |     |
|-------------------------------------------------------------|-----|
| ■ Removing User Data .....                                  | 224 |
| ■ Removing PII from the ActiveTransfer Log Files .....      | 224 |
| ■ Removing PII from the ActiveTransfer Database .....       | 225 |
| ■ Removing PII from the My webMethods Server Database ..... | 225 |

## Removing User Data

---

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. For information about configuring GDPR settings in My webMethods Server, see the "Configuring GDPR Settings" in *Administering My webMethods Server*. To comply with data protection requirements and user requests, in addition to deleting the user account, you may need to complete activities such as deleting or masking 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. For more information about working with ActiveTransfer logs, see ["Managing and Viewing Log Information" on page 205](#).

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:

| <b>PII data in log</b>                                                  | <b>How to find and remove</b>                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User ID of the user logged into ActiveTransfer Server                   | 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.<br><br>You can also avoid logging this information by setting <code>&lt;level value="info"/&gt;</code> to <code>off</code> . |
| Client IP Address from which the user logged into ActiveTransfer Server | 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> .                                                                                                                                                                                                |
| Email address of external user logged into the Web client               | 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> .                                                                                                                                                                                   |

**PII data in log****How to find and remove**

Additionally, this information is also available in the `info.xml` file under your temporary shared directory, as configured in the `mft.sharing.account.tempdir` property in the `\packages\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 <code>MFTActivityLog.UserID</code> 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 <code>MFTTransaction.USERIP</code> table in the database, and delete the records for a particular user or replace it with an anonymous string or a blank string. |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Removing PII from the My webMethods Server Database

---

The My webMethods Server database contains information about user ID, email address, first name, and last name.

When a user is added in ActiveTransfer, the user is automatically added to the My webMethods Server database as well. All the user information stored in the My webMethods Server database and authentication of users at runtime is performed in the My webMethods Server database.

When a user is deleted from ActiveTransfer, all user information is deleted from the ActiveTransfer database but still stored in the My webMethods Server database. This is because the same user might be used in other applications. If you want to delete the user from My webMethods Server and all other applications, you should delete the user from the My webMethods Server User Management screen.



# 15 Administering ActiveTransfer with Command Central

---

|                                                             |     |
|-------------------------------------------------------------|-----|
| ■ Overview .....                                            | 228 |
| ■ Managing ActiveTransfer Licenses in Command Central ..... | 228 |
| ■ Lifecycle Actions and Statuses of The WmMFT Package ..... | 228 |

## Overview

---

The ActiveTransfer run-time component is a layered product of Integration Server and appears listed by its package name `WmMFT` in the Command Central web user interface. In order to manage ActiveTransfer from the Command Central user interface, you must install ActiveTransfer as a sub-component of My webMethods Server in the Software AG Installer.

You can use Command Central to perform the following operations for ActiveTransfer from **IS\_Instance Name > WmMFT**:

- Start, stop, and restart the ActiveTransfer instances.
- Manage ActiveTransfer Server ports.
- Access and download ActiveTransfer log files.
- Manage ActiveTransfer licenses.

For details on how to use each of the Command Central operations listed, see *Software AG Command Central Help*.

## Managing ActiveTransfer Licenses in Command Central

---

In Command Central, you can configure ActiveTransfer licenses, view the details of the configured licenses, and retrieve the location of the license files. However, you cannot change the location of ActiveTransfer license files. For information on how to manage licenses in Command Central, see *Software AG Command Central Help*.

## Lifecycle Actions and Statuses of The WmMFT Package

---

You can perform the following operations on the WmMFT package. The resultant statuses of the WmMFT package are:

| Life Action | Description                                                                     |
|-------------|---------------------------------------------------------------------------------|
| Start       | Starts the WmMFT package. When successful, the runtime status is set to ONLINE. |
| Stop        | Stops the WmMFT package. When successful, the runtime status is set to STOPPED. |
| Restart     | Restarts the WmMFT package. When successful, the runtime status is ONLINE.      |

# 16 Working with the New User Interface

---

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| ■ Understanding ActiveTransfer .....                                     | 231 |
| ■ Configuring ActiveTransfer .....                                       | 237 |
| ■ Managing Listeners .....                                               | 247 |
| ■ Managing Gateways .....                                                | 261 |
| ■ Managing Virtual Folders .....                                         | 267 |
| ■ Managing Actions .....                                                 | 279 |
| ■ Managing Users and Templates .....                                     | 331 |
| ■ Viewing and Downloading Logs .....                                     | 347 |
| ■ Managing Proxy Servers .....                                           | 359 |
| ■ Managing Certificates .....                                            | 365 |
| ■ Managing ActiveTransfer Settings .....                                 | 367 |
| ■ Managing User Interface Permissions for Users, Roles, and Groups ..... | 385 |
| ■ Archiving Data .....                                                   | 387 |
| ■ Managing ActiveTransfer Account Settings .....                         | 393 |
| ■ Removing User Data from ActiveTransfer .....                           | 395 |

Administering webMethods ActiveTransfer Server explains how to configure webMethods ActiveTransfer, manage file transfers, and common administrative tasks, such as managing listeners, gateways, virtual folders, actions, users, proxy servers, and settings. This help assumes you are familiar with webMethods Integration Server.

# Understanding ActiveTransfer

---

## 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.

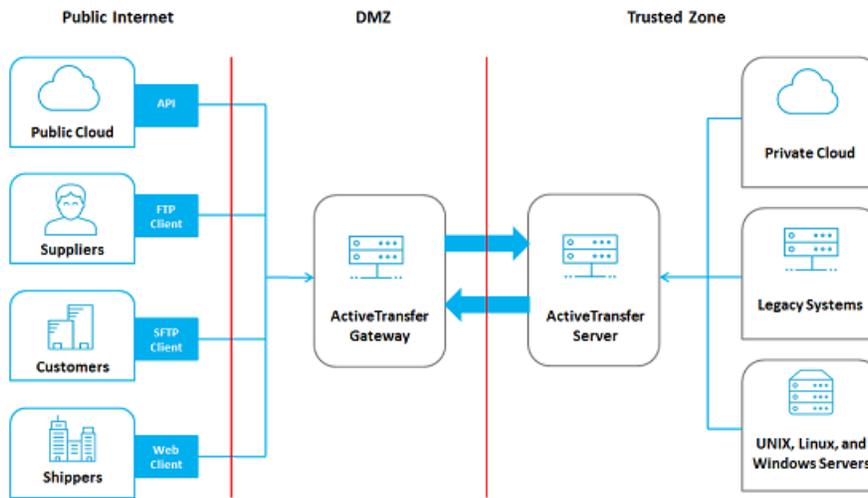
MFT offers a number of security, administration, and scalability advantages over non-secure file transfer protocols such as FTP. With MFT, there is no need to develop custom code for routine functions such as delivery confirmation, reporting, audit, security provisioning, and trading partner/community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

## 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 WebDAV's protocols.

**Note:**

The HTTP(S) port defined in ActiveTransfer can also be used as WebDAV and WebDAV's 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:

| ActiveTransfer asset | Supported protocols                                                                         |
|----------------------|---------------------------------------------------------------------------------------------|
| 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. |

| ActiveTransfer asset | Supported protocols                                                                         |
|----------------------|---------------------------------------------------------------------------------------------|
| Actions              | FTP, FTPES, FTPS, HTTP, HTTPS, SFTP, SMB (1.0, 2.0, and 3.0 versions), WebDAV, and WebDAVs. |
| Proxy servers        | HTTP and HTTPS.                                                                             |

---



# Configuring ActiveTransfer

---

## 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`
  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, My webMethods roles, or Integration Server groups to log into ActiveTransfer. For more information, see [“Configuring UI Permissions to Users, Roles, or Groups” on page 385](#).
  - 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 Single Sign-On for ActiveTransfer” on page 256](#).

## 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 MashZone NextGen

Before you can display analytical information in ActiveTransfer, you must configure MashZone NextGen by performing the following tasks:

1. Set up the MashZone NextGen environment and the dashboard for ActiveTransfer. For details, see [“Setting Up the MashZone NextGen Server Environment” on page 240](#).
2. Configure ActiveTransfer to connect to MashZone NextGen server to view the analytical information in ActiveTransfer. For details, see [“Configuring ActiveTransfer to connect to MashZone NextGen Server” on page 243](#).

For additional information about configuring MashZone NextGen and managing MashZone NextGen dashboards, see the MashZone NextGen documentation.

## Setting Up the MashZone NextGen Server Environment

When you install ActiveTransfer using Software AG Installer, the monitoring MashApps for ActiveTransfer Server are downloaded but not installed on the MashZone NextGen server. Complete the configuration of MashZone NextGen environment as listed below.

### > To set up the MashZone NextGen environment

1. Copy the necessary files to the MashZone NextGen installation as follows:
  - a. Copy the corresponding JDBC driver for your database to the directory:  
`MashZone_Installation_directory\MashZoneNG\mashzone\data\jdbcdrivers` directory.  
  
 For details on which JDBC drivers to copy, see the MashZone NextGen documentation.
  - b. Copy the Red .less file from *Integration Server\_directory*  
`\IntegrationServer\instances\instance_name\packages\WmMFT\mashzone\columnchart` to  
`MashZone_Installation_directory\MashZoneNG\active-transfer\apps\mashzone\lib\dashboard\assets\custom-look-and-feel\dashboard\default\columnchart`
2. Update the XFrame-Options filters and content security policies in the MashZone NextGen directory using the contents of the ActiveTransfer file as follows:
  - a. Navigate to the *Integration Server\_directory*  
`\IntegrationServer\instances\instance_name\packages\WmMFT\mashzone\security-filter` directory.
  - b. Using an XML editor, open the `applicationContext-security-filters.xml` file.
  - c. Copy the complete header content (all content within the open and close tags) for the following to a temporary file, such as a text file.
    - `http pattern="/**/*.jsp" use-expressions="false"`
    - `http pattern="/hub/(login|reset_password)\.html.*" request-matcher="regex"`
    - `http pattern="/**/*.html" use-expressions="false"`
  - d. In the copied header content, locate each instance of `otherServerHost:otherServerPort` and replace:
    - `otherServerHost` with the ActiveTransfer Server host name.
    - `otherServerPort` with the port for ActiveTransfer Server user interface.

#### **Important:**

Once you perform these configuration changes, you will not be able to view the reports in My webMethods Server.

- e. Close the `applicationContext-security-filters.xml` file.
  - f. Navigate to the directory  
`MashZone_Installation_directory\MashZoneNG\apache-tomcat\webapps\mashzone\WEB-INF\classes.`
  - g. Open the file `applicationContext-security-filters.xml`.
  - h. Replace the following header content (all content within the open and close tags) with the corresponding header content that you copied and edited earlier:
    - `http pattern="/**/*.jsp" use-expressions="false"`
    - `http pattern="/hub/(login|reset_password)\.html.*" request-matcher="regex"`
    - `http pattern="/**/*.html" use-expressions="false"`
  - i. Save and close the `applicationContext-security-filters.xml` file.
3. To configure Single Sign On (SSO), configure `ssoProcessingFilter` in the `MashZone_Installation_directory\MashZoneNG\apache-tomcat\webapps\mashzone\WEB-INF\classes\applicationContext-security.xml` file. To do this:
    - a. Open `applicationContext-security.xml` file in any text or XML editor. This file is located in the `MashZone_Installation_directory\MashZoneNG\apache-tomcat\webapps\mashzone\WEB-INF\classes` folder.
    - b. Add a comment to the `ssoProcessingFilter` bean `<bean id="ssoProcessingFilter" class="com.jackbe.jbp.sas.security.ui.sso.SSONullPreAuthenticatedFilter">` as follows:
 

```
<!--bean id="ssoProcessingFilter" class="com.jackbe.jbp.sas.security.ui.sso.SSONullPreAuthenticatedFilter">
<property name="authenticationManager" ref="authenticationManager" />
<property name="continueFilterChainOnUnsuccessfulAuthentication" value="true" />
</bean> -->
```
    - c. Remove the comment for the bean `<bean id="ssoProcessingFilter" class="com.jackbe.jbp.sas.security.ui.sso.SSOPreAuthenticatedFilter">`.
    - d. For this bean, configure the `principalExtractor` property with the following settings:
 

```
<property name="principalExtractor">
<bean class="com.jackbe.jbp.sas.security.ui.sso.HttpHeaderOrParamTokenExtractor">
<property name="httpHeaderName" value="MFT_USER"/>
</bean>
</property>
```
    - e. Configure the `principalTransformation` property with the following settings:

```
<property name="principalTransformation">
<bean class="com.jackbe.jbp.common.util.
NoOpStringTransformation"></bean>
</property>
```

For more details, see the "Configuration for Agent-Based SSO Solutions" section in the MashZone NextGen documentation.

4. Start the MashZone NextGen server.
5. Browse to the MashZone NextGen welcome page `http://host:8080/mashzone`, and log on as a system user.

The default system user name and password are `Administrator` and `manage` respectively.

6. Depending on the system directory that you use to store user credentials, do the following
  - By default, ActiveTransfer uses the My webMethods Server system directory. If you use the My webMethods Server system directory to store user profiles, create a matching user profile in MashZone NextGen for each user who has permission to view or manage ActiveTransfer analytical information as follows:

1. In the MashZone NextGen welcome page, click **Administrator > Admin Console**.
2. On the Admin Console page, click **Users & Groups > Users**.
3. Click **Add new user**.
4. Specify the login ID defined for the user in My webMethods Server and other relevant details.
5. Click **Add this user**.

- Instead of the My webMethods Server system directory, if you use LDAP as your central user profile repository, integrate your LDAP directory with Software AG MashZone NextGen.

For details on how to integrate your LDAP repository with MashZone NextGen, see the MashZone NextGen documentation.

7. In the MashZone NextGen, Admin Console page, add user groups and associate users with the user groups, as required.

For details on how to add user groups and associate users to user groups, see the MashZone NextGen documentation.

**Tip:**

Instead of specifying privileges for each user individually, define privileges for multiple users at a time by creating a user group, and then associating users with the group.

8. Import the ActiveTransfer analytics dashboard into MashZone NextGen:

- a. Navigate to the *Integration Server\_directory* \IntegrationServer\instances\default\packages\WmMFT\mashzone\dashboard directory.
- b. Copy the ActiveTransfer\_Analytics\_Dashboard.zip file to any location on your local machine.
- c. Navigate to the *MashZone\_Installation\_directory*\MashZoneNG\prestocli\bin directory.
- d. Open the command prompt and run the following command:

```
padmin importDashboard -l http://host:port/mashzone -f Location of
ActiveTransfer_Analytics_Dashboard.zip -u Administrator -w manage -o
```

9. Define a data source in MashZone NextGen to the ActiveTransfer database as follows:

- a. On the Admin Console page, click **JDBC Configuration > Data Sources**.
- b. Click **Add data source**.
- c. In **Data Source Name**, type MFTDB, the name of the ActiveTransfer database.  
For the ActiveTransfer analytics dashboard to work, the MFTDB database is mandatory.
- d. Specify other relevant details for the ActiveTransfer database component.  
Provide a normal JDBC URL in the **JDBC URL** field instead of providing the URL in the webMethods format.
- e. Click **Save Changes**.
- f. To test the database connection, click .

10. Share the dashboard with the users or groups you defined previously as follows:

- a. On the MashZone NextGen welcome page, open the **ActiveTransfer Analytics** dashboard.
- b. In the menu, click  > **Manage > Permissions**.
- c. In the Manage dashboard permissions dialog box, select view or edit permissions for the user or group.
- d. Click **Save**.

## Configuring ActiveTransfer to connect to MashZone NextGen Server

Before you view analytical information in ActiveTransfer, you must configure ActiveTransfer to connect to MashZone NextGen server.

➤ **To configure ActiveTransfer to connect to MashZone NextGen server**

1. On the navigation pane, select **Logs > Analytics**.
2. Click .
3. In the **Add MashZone NextGen server** dialog box, type the **Host** and **Port** details of the machine on which MashZone NextGen is installed.
4. Click **Add**.

ActiveTransfer is connected to the MashZone NextGen instance.

**Note:**

- You can view the MashZone NextGen dashboards for ActiveTransfer only from **Analytics** page.
- If you want to connect ActiveTransfer to MashZone NextGen server over SSL, you must first configure the SSL port on the MashZone NextGen server, and then direct ActiveTransfer to the configured SSL port.

## 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.



# Managing Listeners

---

## 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 249](#).

## 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 249.

### ➤ 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.
	<p><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).</p>

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.  <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” on page 238</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</b>	Select <b>Active</b> to enable RSA encryption, and type the file name or browse to the location of the file containing the key for the RSA algorithm.
<b>Password</b>	Type the password to access the RSA key, if required.
<b>DSA</b>	Select <b>Active</b> to enable DSA encryption, and type the file name or browse to the location of the file containing the key for the DSA algorithm.
<b>Password</b>	Type the password to access the DSA key, if required.
<b>SSH: Authentication</b>	
<b>Require password authentication</b>	Select this option if you want to make password authentication mandatory for a user.

Field	Description
<b>Require public key authentication</b>	Select this option if you require a certificate or public key when a secure connection is established with a partner. Whether password-based authentication is mandatory or not, authentication of a connection established with a partner is done with the public key.
<b>SSH: Supported ciphers</b>	Select the required ciphers from the list.
<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).

Field	Description
<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 238</a> . Also, to 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 location</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.  <b>Note:</b> This keystore file overrides any global SSL encryption settings that apply to all listeners on the server.
<b>Keystore password</b>	Type the keystore password.
<b>Private key password</b>	Type 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.  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.  For details on how to map client certificates to users, see "User Certificate Mapping" section in the document.  When establishing a connection with the server, ActiveTransfer validates only the client certificate but not the password.  <b>Tip:</b> To store valid certificates: <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>

Field	Description
<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> <li>■ <b>SSLv3</b></li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <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.

- 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.



# Managing Gateways

---

## 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 263](#).

## 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 263](#).

### > To add a Gateway

1. On the navigation pane, select **Gateways**.
2. On the Gateways page, click  **Add**.
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.

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>	Select this option to perform a virus scan check on all the files that are uploaded.
	<b>Note:</b>

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 261</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.



# Managing Virtual Folders

---

## 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 same 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 269](#). 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>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, or HTTPS protocol, type the certificate alias for the <b>Keystore alias</b>.</li> <li>■ If you select SFTP protocol, type the certificate alias in the <b>Key alias</b>.</li> </ul> <p>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.</p> <p>You can configure the preferred cipher from the list of supported cipher in <b>Preferred cipher</b> field. Additionally, if you want to</p>

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

remove a cipher from the supported cipher list, then you set configure it on the **Excluded cipher** field.

- If you select **SMB** protocol, you can choose the version of SMB version that you want to connect to. Additionally, you need to select the SMB 2.0 to use the services of the SMB version 2.0 or later.
- 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.
--------------------	------------------------------------------------------------------------------------------------------------------------

<b>Access key ID</b>	Specify the access key id to access the <b>Amazon-S3</b> bucket. .
----------------------	--------------------------------------------------------------------

<b>Secret cccess 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.
--------------------------	----------------------------------------------------------------------------------------------------------------------

**Note:**

For more information about **Amazon-S3** service, refer Amazon documentation.

**Note:**

For a list of known endpoint specific limitations, see “[Limitations](#)” on page 433.

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

Field	Description														
	<table border="1"> <thead> <tr> <th>Fields</th> <th>Description/Action</th> </tr> </thead> <tbody> <tr> <td><b>Bucket name</b></td> <td>Specify the <b>Hosted-S3</b> bucket name.</td> </tr> <tr> <td><b>Folder path</b></td> <td>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.</td> </tr> <tr> <td><b>Access key ID</b></td> <td>Specify the access key id to access the <b>Hosted-S3</b> bucket. .</td> </tr> <tr> <td><b>Secret access key</b></td> <td>Specify the secret key which corresponds to the <b>Access Key ID</b> that has the access to <b>Hosted-S3</b> bucket.</td> </tr> <tr> <td><b>Endpoint</b></td> <td>Specify the <b>Endpoint</b> to access the <b>Hosted-S3</b> bucket.</td> </tr> <tr> <td><b>URL Style</b></td> <td>           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, https://s3-hosted.example.com/bucket-name/</li> <li>■ <b>Virtual host.</b> This URL model involves including the bucket name as a subdomain of the hostname.  For example, https://bucket-name.s3-hosted.example.com/</li> </ul> </td> </tr> </tbody> </table>	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, https://s3-hosted.example.com/bucket-name/</li> <li>■ <b>Virtual host.</b> This URL model involves including the bucket name as a subdomain of the hostname.  For example, https://bucket-name.s3-hosted.example.com/</li> </ul>
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, https://s3-hosted.example.com/bucket-name/</li> <li>■ <b>Virtual host.</b> This URL model involves including the bucket name as a subdomain of the hostname.  For example, https://bucket-name.s3-hosted.example.com/</li> </ul>														

**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:**

Field	Description
	<p>ActiveTransfer currently supports only <b>AZURE-FILE</b> shares and <b>AZURE-BLOB</b> containers.</p> <ul style="list-style-type: none"> <li>■ To configure the VFS with <b>AZURE-FILE</b>, use the following fields:</li> </ul>
Fields	Description/Action
<b>Authentication type</b>	<p>Specifies the authentication information that must be sent to the <i>Azure</i> storage type for authorizing the access to specific resources. File shares supports <b>Shared Key</b> and <b>Shared access signature (SAS)</b> authentication type. Choose one of the following ways to provide the authentication information:</p> <ul style="list-style-type: none"> <li>■ <b>Shared Key:</b> 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: <ul style="list-style-type: none"> <li>■ <b>Account name:</b> Specify the account name that corresponds to the <i>Azure</i> account for the <b>AZURE-FILE</b> location.</li> <li>■ <b>Account key:</b> Specify the key which you create at the <i>Azure</i> portal for the corresponding <b>Account name</b>.</li> </ul> </li> <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. <p>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.</p> <ul style="list-style-type: none"> <li>■ <b>Account name:</b> Specify the account name that corresponds to the <i>Azure</i> account for the <b>AZURE-FILE</b> 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> </ul> </li> </ul>

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

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

**Location** 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**.
- **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.

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 blob location.

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>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> </tbody> </table>	Fields	Description		<ul style="list-style-type: none"> <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>
Fields	Description				
	<ul style="list-style-type: none"> <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 location where the folder for blob container resides.				
<b>Advanced</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>	<p>Add the additional header parameters to set the extra metadata for the blob container. Click  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:**

Field	Description
	<p data-bbox="597 262 1307 331">For more information on <b>AZURE-FILE</b> shares and <b>AZURE-BLOB</b> containers, refer Azure documentation.</p> <ul style="list-style-type: none"> <li data-bbox="500 367 1356 472">■ 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="548 493 1372 598">■ <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="548 619 1372 724">■ <b>Select proxy alias:</b> 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.</li> </ul> </li> <li data-bbox="500 745 1339 808">■ Click <b>Test Connection</b> to check the connection to the remote location.</li> <li data-bbox="500 840 1364 945">■ Select <b>High availability download recovery</b> if you want ActiveTransfer Server to recover from a download that was not completed.</li> <li data-bbox="500 966 1323 1071">■ Select <b>High availability upload recovery</b> if you want ActiveTransfer Server to recover from an upload that was not completed.</li> <li data-bbox="500 1092 1372 1239">■ Select <b>Passive</b> 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.</li> <li data-bbox="500 1260 1380 1407">■ 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 data-bbox="503 1438 1356 1512"><b>Note:</b> Sending <b>MKDIR</b> or <b>CWD</b> to a directory with no files results in error.</p> <p data-bbox="503 1543 1356 1617"><b>Note:</b> Sending <b>RMD</b> after deleting all files in a directory results in error.</p>
<b>Permissions</b>	<p data-bbox="500 1648 1380 1816">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>.</p>

Field	Description
	<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 331</a>.</p>
<b>Encryption/Decryption</b>	
<b>File-based encryption</b>	Select the public PGP certificate alias in the <b>Public PGP Key alias</b> box.
<b>File-based decryption</b>	Select the private PGP certificate alias in the <b>Private PGP Key alias</b> box.

- (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.

- 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

- On the navigation pane, select **Virtual folders**.
- On the Virtual folders page, click on a virtual folder that you want to edit.
- 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: <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 users:</b> To search for virtual folders associated with all the users in ActiveTransfer.</li><li>■ <b>Specific user:</b> To search for virtual folders associated with a specific user in ActiveTransfer. Select this option, type the name of the user, 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** to reset values and **Apply** for the changes to take effect. The virtual folders list is populated with the virtual folders matching your search criteria.

# Managing Actions

---

## 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. However, the ActiveTransfer assets in My webMethods Server user interface and APIs still follow the old naming convention.

- *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.
<b>Active</b>	Click the toggle button to activate (  ) or deactivate (  ) the action.
<b>Criteria</b>	Click  . In the Criteria dialog box, configure the following criteria based on which ActiveTransfer Server will execute tasks, and click <b>Ok</b> .
<b>Execute the tasks below when a user <input type="checkbox"/> files</b>	<p>Select the file operation from the list.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p><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.</p> </div>
<b>Virtual folder</b>	<p>To specify any folder or a particular folder, select <b>Any folder</b> or <b>Specific folder</b> respectively.</p> <p>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.</p>
<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>	<p>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>.</p>
<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>	<p>Select one or more of the following tasks, and define configurations for each of the tasks in the <b>Properties</b> section accordingly:</p> <ul style="list-style-type: none"> <li>■ File operations <ul style="list-style-type: none"> <li>■ <a href="#">“Find Task Configuration” on page 290</a></li> <li>■ <a href="#">“Copy Task Configuration” on page 293</a></li> <li>■ <a href="#">“Move Task Configuration” on page 297</a></li> <li>■ <a href="#">“Delete Task Configuration” on page 302</a></li> </ul> </li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <a href="#">“Rename Task Configuration” on page 303</a></li> <li>■ <a href="#">“Encrypt Task Configuration” on page 304</a></li> <li>■ <a href="#">“Decrypt Task Configuration” on page 305</a></li> <li>■ <a href="#">“Zip Task Configuration” on page 307</a></li> <li>■ <a href="#">“Unzip Task Configuration” on page 309</a></li> <li>■ <a href="#">“Write Content Task Configuration” on page 311</a></li> <li>■ <a href="#">“Execute Integration Server Service Task Configuration” on page 313</a></li> <li>■ <a href="#">“Execute Script Task Configuration” on page 314</a></li> <li>■ <a href="#">“Execute Trading Networks Service Task Configuration” on page 316</a></li> <li>■ <a href="#">“Send Universal Messaging/Broker Notification Task Configuration” on page 318</a></li> <li>■ <a href="#">“Send Email Task Configuration” on page 319</a></li> <li>■ <a href="#">“Write File to Database Task Configuration” on page 321</a></li> <li>■ <a href="#">“Jump Task Configuration” on page 322</a></li> <li>■ <a href="#">“Exclude Task Configuration” on page 324</a></li> <li>■ <a href="#">“Error Task Configuration” on page 325</a></li> </ul> <p>For descriptions of fields for task configurations, see <a href="#">“Task Configuration Definitions” on page 289</a>.</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>

### Parallel processing

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

Field	Description
<b>parallel processes</b>	

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 .
  - .
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>	<p>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>:</p> <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> </ul>

Field	Description
	<ul style="list-style-type: none"> <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>
<b>Tasks</b>	<p>Select one or more of the following tasks and define configurations for each of the tasks in the <b>Properties</b> section accordingly:</p> <ul style="list-style-type: none"> <li>■ File operations <ul style="list-style-type: none"> <li>■ <a href="#">“Find Task Configuration” on page 290</a></li> <li>■ <a href="#">“Copy Task Configuration” on page 293</a></li> <li>■ <a href="#">“Move Task Configuration” on page 297</a></li> <li>■ <a href="#">“Delete Task Configuration” on page 302</a></li> <li>■ <a href="#">“Rename Task Configuration” on page 303</a></li> <li>■ <a href="#">“Encrypt Task Configuration” on page 304</a></li> <li>■ <a href="#">“Decrypt Task Configuration” on page 305</a></li> <li>■ <a href="#">“Zip Task Configuration” on page 307</a></li> <li>■ <a href="#">“Unzip Task Configuration” on page 309</a></li> <li>■ <a href="#">“Write Content Task Configuration” on page 311</a></li> </ul> </li> <li>■ <a href="#">“Execute Integration Server Service Task Configuration” on page 313</a></li> <li>■ <a href="#">“Execute Script Task Configuration” on page 314</a></li> <li>■ <a href="#">“Execute Trading Networks Service Task Configuration” on page 316</a></li> <li>■ <a href="#">“Send Universal Messaging/Broker Notification Task Configuration” on page 318</a></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <a href="#">“Send Email Task Configuration” on page 319</a></li> <li>■ <a href="#">“Write File to Database Task Configuration” on page 321</a></li> <li>■ <a href="#">“Jump Task Configuration” on page 322</a></li> <li>■ <a href="#">“Exclude Task Configuration” on page 324</a></li> <li>■ <a href="#">“Error Task Configuration” on page 325</a></li> </ul> <p>For descriptions of fields for task configurations, see <a href="#">“Task Configuration Definitions” on page 289</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>

**Parallel processing**

<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.

- Click **Add**.

The new scheduled action appears in the scheduled actions list.

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

**Note:**  
You can test only deactivated scheduled actions.

- In the Test scheduled action dialog box, type the values for the parameters defined in tasks.
- 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.
<b>Criteria</b>	<p>Click . In the <b>Criteria</b> dialog box, fill the following fields and click <b>Ok</b>:</p> <ul style="list-style-type: none"> <li>■ <b>Monitor folder</b>: Type or browse to the folder to monitor. When ActiveTransfer Server starts monitoring a folder, a lock file with format <code>_{event_id}.mftlock</code> gets automatically created. This is to ensure only a single instance of the monitor folder action can monitor the particular folder.</li> </ul> <p>After the lock file is created successfully, ActiveTransfer Server will start monitoring the folder. However, if the lock gets deleted by an external entity, then ActiveTransfer Server will stop monitoring the folder.</p>

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

- **Select the file operation:** Select the file operation that will trigger the action:
  - **Create file:** If you choose this option, ActiveTransfer Server will trigger 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 are 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 will trigger 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 will not trigger monitor folder action.
- **File filter:** Type the name of the file if you want to filter 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 **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 ZIP files are created or deleted. 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 names, when ZIP files containing the character string invoice in their file names are created or deleted.

Few examples for regular expressions are:

- `^(?!.*purchaseorder).*`: Excludes files with the file name containing purchaseorder.
- `^abc(.*?)123$`: Includes anything that starts with abc and ends with 123. Matches abc123, abcxyz123, but not abcxyz123def.
- `NEW-((*.doc)|(*_backup_*))`: Includes anything starting with NEW- that either ends in .doc, or is followed by the string \_backup\_.

Field	Description
	<ul style="list-style-type: none"> <li data-bbox="488 258 1468 325">■ <b>Completion folder:</b> Type or browse to the folder to move the file after the successful execution of an action.</li> <li data-bbox="488 352 1468 420">■ <b>Error folder:</b> Type or browse to the folder to move the file after an execution fails for the action.</li> <li data-bbox="488 447 1468 514">■ <b>Watch frequency (sec):</b> Specify the time interval in seconds to monitor the folder.</li> <li data-bbox="488 541 1468 609">■ <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 data-bbox="542 642 618 667"><b>Note:</b></p> <ul style="list-style-type: none"> <li data-bbox="542 695 1430 762">■ 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 0.</li> <li data-bbox="542 768 1446 898">■ If the specified value for the retention period is greater than 0, and if the monitor folder action for those files is active, then the files gets deleted from the completion folder or error folder after the specified number of days.</li> <li data-bbox="542 905 1446 1035">■ 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>

<b>Tasks</b>	<p data-bbox="488 1060 1468 1127">Select one or more of the following tasks and define configurations for each of the tasks in the <b>Properties</b> section as required:</p> <ul style="list-style-type: none"> <li data-bbox="488 1155 732 1180">■ File operations <ul style="list-style-type: none"> <li data-bbox="537 1213 1089 1239">■ <a href="#">“Find Task Configuration” on page 290</a></li> <li data-bbox="537 1272 1105 1297">■ <a href="#">“Copy Task Configuration” on page 293</a></li> <li data-bbox="537 1331 1105 1356">■ <a href="#">“Move Task Configuration” on page 297</a></li> <li data-bbox="537 1390 1105 1415">■ <a href="#">“Delete Task Configuration” on page 302</a></li> <li data-bbox="537 1449 1122 1474">■ <a href="#">“Rename Task Configuration” on page 303</a></li> <li data-bbox="537 1507 1122 1533">■ <a href="#">“Encrypt Task Configuration” on page 304</a></li> <li data-bbox="537 1566 1122 1591">■ <a href="#">“Decrypt Task Configuration” on page 305</a></li> <li data-bbox="537 1625 1073 1650">■ <a href="#">“Zip Task Configuration” on page 307</a></li> <li data-bbox="537 1684 1105 1709">■ <a href="#">“Unzip Task Configuration” on page 309</a></li> <li data-bbox="537 1743 1203 1768">■ <a href="#">“Write Content Task Configuration” on page 311</a></li> </ul> </li> <li data-bbox="488 1801 1414 1827">■ <a href="#">“Execute Integration Server Service Task Configuration” on page 313</a></li> </ul>
--------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Field	Description
	<ul style="list-style-type: none"> <li>■ <a href="#">“Execute Script Task Configuration” on page 314</a></li> <li>■ <a href="#">“Execute Trading Networks Service Task Configuration” on page 316</a></li> <li>■ <a href="#">“Send Universal Messaging/Broker Notification Task Configuration” on page 318</a></li> <li>■ <a href="#">“Send Email Task Configuration” on page 319</a></li> <li>■ <a href="#">“Write File to Database Task Configuration” on page 321</a></li> <li>■ <a href="#">“Jump Task Configuration” on page 322</a></li> <li>■ <a href="#">“Exclude Task Configuration” on page 324</a></li> <li>■ <a href="#">“Error Task Configuration” on page 325</a></li> </ul> <p>For descriptions of the fields for these task configurations, see <a href="#">“Task Configuration Definitions” on page 289</a>.</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>Import</b>	<p>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 279</a>.</p>
Field	

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 [“Activating or Deactivating Actions” on page 325](#).

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> <p><b>Note:</b> If you want to find and copy files from remote, third-party HTTP(S) servers, ensure that you provide appropriate 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> </ul>

Field	Description
	<ul style="list-style-type: none"> <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 325</a> .
<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>	Specify one of the following time period in which the file was last modified to narrow the search: <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>

Field	Description
	<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> <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 [ ] times at an interval of [ ] seconds</b>	If you want ActiveTransfer to retry a failed find task. Type the number of retries and the retry interval 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></p>

Field	Description
	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.

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.
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>	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><b>Note:</b></p> <p>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>

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 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>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 style="background-color: #f0f0f0; padding: 5px; margin: 10px 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>■ 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: 10px 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</p> </div>

Field	Description
	<p>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> <ul style="list-style-type: none"> <li>■ <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> <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>
<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 325</a> .

### Advanced

**Rename file to** Select this option to rename the file to the specified name in the box.

**Check if the file exists at destination** Select this option to check if the file already exists at the destination and perform one of the following options:

- **Skip the transfer if file exists:** 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.

**Example:** 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.

- **Fail the action if file exists:** 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.

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.

**Example:**

- For parallel execution:

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.

- For non-parallel execution:

Field	Description
	<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>
	<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>	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 [ ] times at an interval of [ ] seconds</b>	Select this option to retry a failed copy operation for the specified number of times at the interval specified 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>	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</b> , <b>CR - MAC OS Classic</b> , <b>LF - Unix</b> , or <b>No change</b> .

Field	Description
	<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> <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 <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>

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 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>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 style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <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 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</p> </div>

Field	Description
	<p>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>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 325</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>	<p>Select this option to check if the file already exists at the destination location 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.</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:</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</p>

Field	Description
	<p>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: <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> </li> </ul> <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 [ ] times at an interval of [ ] seconds</b>	<p>Select this option to retry a failed move operation for the specified number of times at the interval specified 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</p>

Field	Description
	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 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: <code>[partner_name]</code>, where <code>[partner_name]</code> 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; margin-top: 10px;"> <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; margin: 10px 0;"> <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 325</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> <div style="background-color: #f0f0f0; padding: 10px;"> <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 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>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.

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 325</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>	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><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 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>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.

Field	Description
<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.
<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.

## 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.

Few examples for regular expressions are:

Field	Description
	<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>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 325</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; margin: 10px 0;"> <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>. <ul style="list-style-type: none"> <li>■ Type the <b>User name</b> and <b>Password</b> for the remote system.</li> </ul> </li> </ul>

Field	Description
	<ul style="list-style-type: none"> <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> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b></p> </div>

Field	Description
	For virtual folders, use this option only if you want to override the partners configured for the folders.
<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 325</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 325</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 325</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 <code>filePath</code> .
<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 <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> . <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 325</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.

Field	Description
<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 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 (.bat) 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>
<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 325</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> <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>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: <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> </li> </ul> <p>For details about flat file processing, see the Trading Networks documentation.</p>

Field	Description
	<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. This local service is used for the configuration of input and output parameters in My webMethods Server. For details on 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 325</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>	<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</p>

Field	Description
	<p>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>
<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 325</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;"> <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>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.
<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>	<p>Type text to appear in the subject line of the email (for example, <i>Disconnect:?User %user_name%</i>).</p> <p>The value you specify in <b>Subject</b> overrides the value specified in the <code>mft.user.email.subject</code> parameter for this task.</p>
<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.

Field	Description
<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 325</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.

### 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>	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>	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> . <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>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 325</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>	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; margin-top: 10px;"> <p><b>Note:</b></p> </div>

Field	Description
	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.
<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>■ <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>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 325</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>	<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, <code>Jump</code> 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, <code>Jump1</code>.</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 <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 not 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>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 325</a>.</p>

## 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.

## Activating or Deactivating 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 activate or deactivate 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.

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 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.

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

1. In My webMethods: **Administration > Integration > Managed File Transfer > Event Management > Scheduled Events** tab.
2. Select the event in the event list or add a new event.
3. In the **Actions** section, click the **Select Action** list.
4. Select the action that you want to configure.
5. 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 327](#).

6. 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

Action	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
	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

Action	Action Settings
	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 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

Action	Action Settings
	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

# Managing Users and Templates

---

## Overview

ActiveTransfer users are My webMethods Server users who have an ActiveTransfer profile. The ActiveTransfer profile 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 the user is already defined as a My webMethods Server user, either through internal My webMethods Server 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. For details, see [“Associating an Existing User with ActiveTransfer” on page 334](#).

**Note:**

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

- If the user is not already defined as a My webMethods Server user, you can create the user in the My webMethods Server system directory and define an ActiveTransfer profile for the user at the same time. For details, see [“Creating a New User” on page 333](#).

In My webMethods Server, 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 336

“.” on page 342

## Creating a New User

If a user is not already defined as a My webMethods Server user and does not have an ActiveTransfer profile, then you can create the user in the My webMethods Server system directory 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 My webMethods Server user but does not have an ActiveTransfer profile, you can associate the user with ActiveTransfer.

### ➤ To associate an existing My webMethods Server 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 My webMethods Server with ActiveTransfer. For details on how to create a role in My webMethods Server, see *Administering My webMethods Server*.

### > To associate an existing My webMethods Server 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 My webMethods Server with ActiveTransfer. For details on how to create a group in My webMethods Server, see *Administering My webMethods Server*.

### > To associate an existing My webMethods Server group 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>	

Field	Description
<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.
<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> . <p><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.</p>
<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>	
<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; margin-top: 10px;"> <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; margin-top: 10px;"> <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>
<b>Authentication and login</b>	
<b>Maximum simultaneous logins</b>	<p>Type the maximum number of simultaneous logins allowed for the same user.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> File transfer clients like FileZilla or WinSCP may create additional login sessions to optimize file transfer.</p> </div>
<b>Require public key and password</b>	<p>Select this option if you want ActiveTransfer Server to require the user to provide a public key and password.</p>

Field	Description
<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>	<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.</li> </ul>
<b>File-based encryption</b>	
<b>Public PGP key alias</b>	Type or browse the certificate alias for the public PGP key.
	<p><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>.</p>
<b>File-based decryption</b>	
<b>Private PGP key alias</b>	Type or browse the certificate alias for the private PGP key.
<b>Active tunnels</b>	
<b>Tunnels</b>	<p>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> <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.

## 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 342](#).

### 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 342](#).

➤ **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.

Field	Description
	<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.
<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>	

Field	Description
<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> <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</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>	

Field	Description
<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>	<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.</li> </ul>
<b>File-based encryption</b>	
<b>Public PGP key alias</b>	Type or browse the certificate alias for the public PGP key.
	<p><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>.</p>
<b>File-based decryption</b>	
<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 template from the list of available tunnels on the Acceleration page.
	<p><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.</p>

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.

# Viewing and Downloading Logs

---

## 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:

Field	Description
<b>User</b>	<p>This option filters the transactions initiated by a user or group of users.</p> <p>You can specify the following additional filters:</p> <ul style="list-style-type: none"> <li>■ <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>■ <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>■ <b>Operation:</b> Select <b>All</b>, <b>Upload</b>, or <b>Download</b> based on transaction type.</li> <li>■ <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>You can specify the following additional filters:</p> <ul style="list-style-type: none"> <li>■ <b>Source location:</b> Use this option to query the files which match the transactions from a particular source.</li> </ul> <p>You can either specify the partial or complete source location, which can include protocols as well.</p> <p>The source location will have the following format: <code>&lt;protocol&gt;://&lt;source location&gt;/&lt;filename&gt;</code>.</p> <p>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> <ul style="list-style-type: none"> <li>■ <b>Destination location:</b> Use this option to query the files which match the transactions from a particular destination.</li> </ul> <p>You can either specify the partial or complete destination location, which can include protocols as well.</p>

Field	Description
	<p>The destination location will have the following format: <code>&lt;protocol&gt;://&lt;destination location&gt;/&lt;filename&gt;</code>.</p> <p>Example, for SFTP protocol, the destination location can be, <code>SFTP://dcmft01.eur.ad.sag:2121/var/www/sftp/sftpuser/test1/ATG_10.0.xml</code>.</p>
<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>Search text</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>	<p>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.</p> <p><b>Match complete file name</b> performs the query faster when you have large volumes of data that can utilize the underlying database optimization.</p>

- 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.
- **File size:** Size of the file.
- **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> <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>

Field	Description
<b>Status</b>	Select an option to display <b>All</b> , <b>Success</b> , or <b>Failed</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.

## 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.
- **Comment**: 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 [“Configuring MashZone NextGen” on page 239](#).

### 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> .

Field	Description
<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.

- 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

- In the navigation pane, select **Logs > Agent action log**.
- 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> </ul>

Field	Description
	<ul style="list-style-type: none"> <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> </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>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> <li>c. Click <b>Ok</b>.</li> </ol>
<b>File name</b>	<p>Type either the partial or complete name of the file to search for agents or agent actions that match the specified file name.</p> <p>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.</p>

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 399](#).

### ➤ 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.

# Managing Proxy Servers

## 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	■ HTTPS ■ SOCKS	■ HTTPS ■ SOCKS
HTTP	■ HTTP ■ SOCKS	■ HTTP ■ SOCKS
HTTPS	■ HTTPS ■ SOCKS	■ HTTPS ■ SOCKS
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> </ul>

Parameter location	Parameter name	Description
		<ul style="list-style-type: none"> <li>■ <i>false</i>: ActiveTransfer treats the connection attempt as failed.</li> </ul>
Integration Server	watt.net.proxySkipList	<p>Set this parameter in <i>Integration Server_directory \ instances\instance_name\config directory\cnfserver.cnf</i>.</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	watt.net.proxy.useNonDefaultProxies	<p>Set this parameter in <i>Integration Server_directory \ instances\instance_name\config directory\cnfserver.cnf</i>.</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.

Field	Description
<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>■ HTTP</li> <li>■ HTTPS</li> <li>■ SOCKS</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.

4. Click **Add**.

The new proxy server appears in the proxy servers list.

5. 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. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;"> <p><b>Note:</b> You can designate only one proxy server alias as the default proxy server alias for a particular file transfer protocol.</p> </div>
<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>■ HTTP</li> <li>■ HTTPS</li> <li>■ SOCKS <ul style="list-style-type: none"> <li>■ SOCKS v4</li> <li>■ SOCKS v5</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.

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

---

6. Click **Save**.

The proxy server is updated with the additional settings.



# Managing Certificates

---

## 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.

### Note:

Field	Action/Description
	<p>The button remains in the disabled state until you add and save a particular certificate.</p> <p><b>Note:</b> The default certificates will not show any usage. However, it can be referenced in multiple MFT assets explicitly.</p>
<b>Description</b>	Type a suitable description for the certificate you choose. The maximum limit is 1024 characters.
<b>Certificate type</b>	<p>Select one of the following supported certificate by ActiveTransfer Server:</p> <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>Certificate provider email</b>	Type the email alias to update the information on the certificate expiry.
<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 it's 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, either use My webMethods Server or ActiveTransfer new user interface.
- If the certificates are linked to a database, these assets may not be displayed correctly in ActiveTransfer user interface in My webMethods Server.

# Managing ActiveTransfer Settings

---

## 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. On the navigation pane, select **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.
<b>Active time window</b>	Select the required 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:

Field	Description
	<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> <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> Any characters except wildcard characters or 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 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> 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 would type: ~/system/bin/*</p>
--------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Hammering

<b>Ban IP address after unsuccessful attempts</b>	<p>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 time period in seconds.</li> <li>■ <b>Ban duration (min):</b> Type the number of minutes to ban the IP address.</li> </ul> <p>You can ban a user’s IP address after a certain number of connection, password, or command execution attempts.</p>
---------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Ban the IP addresses of users after the first incorrect password</b>	<p>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> <p>You can ban the IP address associated with a specific user after the user’s first incorrect password attempt.</p>
-------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Field	Description
<b>Ban specified IP addresses</b>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>■ Select <b>Permanently</b> to ban the user's IP address permanently.</li> <li>■ Select <b>For x minutes</b>, and type the number of minutes that the user's IP address should be banned.</li> </ul>
<b>Cache invalid user names 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 user names is useful for blocking robots that make repeated attempts to discover valid user credentials. As a robot scans ActiveTransfer Server or ActiveTransfer Gateway during the user validation process, this option blocks subsequent login attempts made using an invalid user name for the specified number of seconds. If the user name 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 way of an FTP connection.</p> <p>This setting doubles the server's response time 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, 192.28.90.66.</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</p>

Field	Description
	file in the same location as the keystore file, with the name <i>keystoreName_trust</i> . For example, if the keystore file name is <i>server_ks.jks</i> , the truststore name should be <i>server_ks.jks_trust</i> . You should add all the valid client certificates to this truststore.
<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>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> 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.</p>
<b>File-based encryption</b>	
<b>Activate</b>	Select this option to activate 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 file-based decryption.
<b>Private PGP key alias</b>	Type or browse the certificate alias for the private PGP key.
<b>Protocol options</b>	

Field	Description
<b>Welcome message</b>	Type a welcome message for display in the client console (FileZilla client and others) 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 users from changing modified times on uploaded files.
<b>Delete partial uploads</b>	Select this option to delete any incomplete 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> <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 than 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**.

The server instance is updated 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 374](#).

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 374](#).

#### > To add a tunnel

1. On the navigation pane, select **Settings > Acceleration**.
2. On the Acceleration page, click  **+ Add**.
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. <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</b>	
<b>Maximum number 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 number 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.

Field	Description
<b>Channel ramp-up</b>	Type the number of channels to be added as the data transfer speed increases.
<b>Channel ramp-up 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>Channel ramp-down 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 (not configured in My webMethods Server) 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> </ul>

Field	Description
	<ul style="list-style-type: none"> <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:           <div data-bbox="548 1310 1365 1434" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>A user would like to share a file with you: {web_link} This link will expire on {date} at {time}. User Name: {username} Password: {password}</pre> </div> </li> </ul> <p>Where,</p> <ul style="list-style-type: none"> <li>■ <code>{web_link}</code> is the link to the location of the shared file.</li> <li>■ <code>{date} at {time}</code> are the date and time on which the file share link will become inactive.</li> <li>■ <code>{username}</code> is the temporary user name to use when accessing the shared file. In emails, <code>{username}</code> is encrypted in the file share link.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <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>	<p>Select the default file share permissions from the following options:</p> <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 381](#).

- 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 380](#). For more information about configuring the default email settings, see [“Configuring Default Email Settings in the User Interface” on page 380](#) or [“Configuring Default Email Settings in `properties.cnf`” on page 381](#).

## 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.
<b>Template for user email</b>	<p>Email template for the user creation alert.</p> <p>You can configure the following server variables in your user 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>{password}</i>: Password for the user.</li> <li>■ <i>{serverList}</i>: Listener URLs for the user.</li> </ul>
<b>Template for password email</b>	<p>Email template for the password creation alert.</p> <p>You can configure the following server variables in your 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>{password}</i>: Password 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`

**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 249](#).

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. For details, see [“Configuring Additional Settings for a Listener” on page 249](#).
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.



# Managing User Interface Permissions for Users, Roles, and Groups

---

## Overview

Delegated administration access enables administrators to provide restricted access to users, My webMethods roles, and Integration Server groups with granular permissions to specific ActiveTransfer screens. With controlled access to ActiveTransfer screens; users, My webMethods roles, 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, My webMethods 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, My webMethods 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.

# Archiving Data

---

## 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 390](#).
- By executing the stored procedure scripts in the database. See [“Executing the Stored Procedure for Data Archive” on page 391](#).
- 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 390](#).
- 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 dox, 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.



# Managing ActiveTransfer Account Settings

## 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 or *MFT Administrators* role in My webMethods Server can modify the default settings.

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.

Field	Description
<b>Language</b>	Select your preferred language from the list.
<b>Virtual folder</b>	
<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.

4. Click **Save**.

The configured settings are updated under **My settings** or **Default settings** respectively.

# Removing User Data from ActiveTransfer

---

## 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. For information about configuring GDPR settings in My webMethods Server, see *Administering My webMethods Server*. To comply with data protection requirements and user requests, in addition to deleting the user account, you may need to complete activities such as deleting or masking 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	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.  You can also avoid logging this information by setting <code>&lt;level value="info"/&gt;</code> to off.
Client IP Address from which the user logged into ActiveTransfer Server	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> .

**PII data in log**

**How to find and remove**

Email address of external user logged into the Web client

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 `ActiveTransfer.log`.

Additionally, this information is also available in the `info.xml` file under your temporary shared directory, as configured in the `mft.sharing.account.tempdir` property in the `\packages\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.

## Removing PII from the My webMethods Server Database

The My webMethods Server database contains information about user ID, email address, first name, and last name.

When a user is added in ActiveTransfer, the user is automatically added to the My webMethods Server database as well. All the user information stored in the My webMethods Server database and authentication of users at runtime is performed in the My webMethods Server database.

When a user is deleted from ActiveTransfer, all user information is deleted from the ActiveTransfer database but still stored in the My webMethods Server database. This is because the same user

might be used in other applications. If you want to delete the user from My webMethods Server and all other applications, you should delete the user from the My webMethods Server User Management screen.



# A Server Configuration Parameters and Variables

---

■ Server Configuration Parameters .....	400
■ Security Configuration Parameters .....	410
■ Server Variables .....	411

## 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.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. For more information about email configuration, see [“Configuring ActiveTransfer to Send Emails” on page 41](#).

### **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. For more information about configuring these parameters, see [“Replacing the Default SSL Certificate” on page 34](#).

**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:

If you are using the ActiveTransfer Web Client and you want to use these variables, enclose them within percent sign characters (%) instead of curly braces. For example, `{user_name}` would be represented in the Web Client as `%userName%`.

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 events
<code>{n}</code>	New line character.	Post-processing and scheduled events
<code>{task_error}</code>	Returns the last error that occurred in an event.	Post-processing and scheduled events
<code>{task_errors}</code>	Returns the list of all the errors in an event.	Post-processing and scheduled events
<code>{error_trace}</code>	Used to get the stack trace in case of any exception.	Post-processing and scheduled events
<code>{event_execution_id}</code>	Returns the event execution ID which is unique for each event.	Post-processing and scheduled events
<code>{task_error_types}</code>	Returns the type of actions where the error occurred.	Post-processing and scheduled events
<code>{host name}</code>	Host name of the ActiveTransfer Server.	Post-processing and scheduled events
<code>{outbound_proxy_alias }</code>	Proxy server name that is defined for use with an event.	Post-processing and scheduled events

Variable	Description	Supported Event Type
{task_error_names}	Name of the event that results in an error.	Post-processing and scheduled events
{parent_url}	Actual URL that points to the parent folder in which the file resides.	Post-processing and scheduled events
{parent_url_decoded}	Decoded value of the variable {parent_url}	Post-processing and scheduled events
{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 which 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

Variable	Description	Supported Event Type
{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 group, <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 owner, <i>os-depend-fact</i> in MLST RFC 3659.	Scheduled event
{parent_path}	Path to the parent folder.	Scheduled event
{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	Scheduled event

Variable	Description	Supported Event Type
	not available, the format is <code>r,w,a,d,f</code> , and is retrieved from <code>perm</code> .	
<code>{real_parent_path}</code>	Local path of the parent folder for the file on the disk.	Post-processing and scheduled events
<code>{real_parent_path_decoded}</code>	Decoded value of the variable <code>{real_parent_path}</code>	Post-processing and scheduled events
<code>{real_path}</code>	Complete path to the file in the local or remote file system.	Post-processing and scheduled events
<code>{real_path_decoded}</code>	Decoded value of the variable <code>{real_path}</code>	Post-processing and scheduled events
<code>{resume_loc}</code>	Location in the file where the transfer should resume if interrupted.	Post-processing and scheduled events
<code>{size}</code>	Size of the file.	Post-processing and scheduled events
<code>{speed}</code>	Speed of the file transfer.	Post-processing event  Note that when the actual speed is 0, this variable value might be inaccurate.
<code>{start}</code>	Start time for the file transfer.	Post-processing event
<code>{stem}</code>	First part of the file name, before the period.	Post-processing and scheduled events
<code>{the_file_error}</code>	Any error during file transfer.	Post-processing and scheduled events
<code>{the_file_name}</code>	Name of the file.	Post-processing and scheduled events
<code>{the_file_size_formatted}</code>	Size of the file.	Post-processing and scheduled events
<code>{the_file_speed}</code>	Speed of the file transfer (upload/download) for post-processing events.	Post-processing event
<code>{the_file_path}</code>	Path of the file.	Post-processing and scheduled events
<code>{url}</code>	Actual URL that points to the file.	Post-processing and scheduled events

Variable	Description	Supported Event Type
{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

<b>Variable</b>	<b>Description</b>	<b>Supported Event Type</b>
{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

## 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.

<b>Variable</b>	<b>Description</b>	<b>Supported Event Type</b>
{firstName}	First name of the user.	Post-processing and scheduled events
{lastName}	Last name of the user.	Post-processing and scheduled events

<b>Variable</b>	<b>Description</b>	<b>Supported Event Type</b>
{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
{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 .....	420
---------------------------------	-----

## Scheduled Event Options

---

This section describes the calendar and processing options that are available when you specify conditions for a scheduled event.

**Note:**

Date and time formats are defined in *My webMethods*. For information about changing the default date and time format, see *Working with My webMethods*.

### 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 or manually in “Specifying Conditions for a Scheduled Event” on page 142.

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 <i>My webMethods</i> 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 <i>My webMethods</i> 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, at a fixed interval, or manually in “Specifying Conditions for a Scheduled Event” on page 142.

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.

Option	Description
<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.
<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 in “Specifying Conditions for a Scheduled Event” on page 142.

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 .....	424
■ Jump Condition Elements .....	424
■ Defining a Jump Condition .....	426

## 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 action in My webMethods: **Administration > Integration > Managed File Transfer > Event Management**, 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 [“Use of Special Characters in Search” on page 25](#).

3. Specify the **Jump Condition** as follows:
  - a. Enter or select server variables. For a list of server variables, see [“Server Variables” on page 424](#).
  - 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 ActiveTransfer Access Points

---

■ Overview .....	430
■ Ports that ActiveTransfer Uses .....	430
■ IP Addresses and Host Names that ActiveTransfer Uses .....	431
■ Products to Which ActiveTransfer Connects .....	431
■ File Paths .....	432

## Overview

---

This appendix summarizes the ports and host names or IP addresses that ActiveTransfer uses, the products to which ActiveTransfer Server and ActiveTransfer Gateway connect, the file paths used for virtual folders and file operations, and where to go for details about configuring these items.

## Ports that ActiveTransfer Uses

---

This section describes the ports that ActiveTransfer uses and where to go for details about configuring those ports.

Port	Where to Go for More Information
HTTP port that ActiveTransfer Server uses to collect data for the Logs page (default is 2080)	<a href="#">“Server Configuration Parameters” on page 400</a> (mft.http.default.port parameter)
Port for the Integration Server that hosts the ActiveTransfer Server instance (default is 5555)	<a href="#">“Adding an ActiveTransfer Server Instance to My webMethods” on page 32</a>
Registration port for ActiveTransfer Gateway (default is 8500)	<i>Managing File Transfers with webMethods ActiveTransfer Gateway</i> (mft.gatewayServer.port parameter)
FTP and HTTP ports used for file acceleration tunnels	<a href="#">“Configuring Tunnels for Acceleration” on page 43</a>
Ports for destination server for accelerating data transfer (defaults are 55580 and 55555)	<a href="#">“Accelerating Data Transfer” on page 88</a>
Software AG MashZone load balancing port (default is 80)	<i>Installing Software AG Products</i>
Software AG MashZone SSL port, for communication between the MashZone client and the MashZone server (default is 443)	<i>Installing Software AG Products</i>
Ports used to transfer files and execute commands on ActiveTransfer Server	<a href="#">“Managing ActiveTransfer Ports” on page 68</a>
Port used for passive FTP port connections	<a href="#">“Setting Passive FTP Mode for ActiveTransfer Server” on page 72</a>
HTTP(S) port that ActiveTransfer Server uses to connect to Command Central to synchronize ActiveTransfer Agent installations	<i>Managing File Transfers with webMethods ActiveTransfer Agent</i> (mft.server.commandCentral.port)

## IP Addresses and Host Names that ActiveTransfer Uses

This section describes the IP addresses and host names that ActiveTransfer uses and where to go for details about configuring them. For information, see *Managing File Transfers with webMethods ActiveTransfer Gateway*.

IP Address or Host Name	Where to Go for More Information
Host for the ActiveTransfer Server instance being connected to My webMethods Server	<a href="#">“Adding an ActiveTransfer Server Instance to My webMethods”</a> on page 32
Host in the URL that is emailed to users for logging in to the server	<a href="#">“Server Configuration Parameters”</a> on page 400 (mft.user.email.public.ip parameter)
Host used for file acceleration through FTP and HTTP ports	<a href="#">“Configuring Tunnels for Acceleration”</a> on page 43 and <a href="#">“Accelerating Data Transfer”</a> on page 88
Default IP address for destination server for accelerating data transfer (127.0.0.1)	<a href="#">“Configuring Tunnels for Acceleration”</a> on page 43 and <a href="#">“Accelerating Data Transfer”</a> on page 88
<p><b>Important:</b> Do not change this value.</p>	
Host name of the Software AG MashZone server	<a href="#">“Setting Up the MashZone NextGen Environment”</a> on page 47
Host used to connect ActiveTransfer Gateway to ActiveTransfer Server	<i>Managing File Transfers with webMethods ActiveTransfer Gateway</i>
Hosts used to transfer files and execute commands on ActiveTransfer Server	<a href="#">“Managing ActiveTransfer Ports”</a> on page 68
Host name of the ActiveTransfer Server to connect to using passive FTP mode	<a href="#">“Setting Passive FTP Mode for ActiveTransfer Server ”</a> on page 72
IP addresses of the ActiveTransfer Servers from which ActiveTransfer Gateway should accept connections	<i>Managing File Transfers with webMethods ActiveTransfer Gateway</i>  (mft.gatewayServer.accept.ip.list parameter)

## Products to Which ActiveTransfer Connects

This section describes the products that ActiveTransfer connects to and where to go for details about configuring connections to those products.

<b>Product</b>	<b>Where to Go for More Information</b>
My webMethods Server	<a href="#">“Adding an ActiveTransfer Server Instance to My webMethods” on page 32</a>
Integration Server (for Single Sign-On and central user management, by way of My webMethods Server)	<i>webMethods Integration Server Administrator’s Guide</i>
SMTP server (for sending emails, by way of Integration Server)	<a href="#">“Configuring ActiveTransfer to Send Emails” on page 41</a>
Software AG MashZone	<a href="#">“Setting Up the MashZone NextGen Environment” on page 47</a>
ActiveTransfer Server (when connecting from ActiveTransfer Gateway)	<i>Managing File Transfers with webMethods ActiveTransfer Gateway</i> (gatewayServer.accept.ip.list parameter)
ActiveTransfer Gateway (when connecting from ActiveTransfer Server)	<i>Managing File Transfers with webMethods ActiveTransfer Gateway</i>

## File Paths

---

This section describes the physical file paths that ActiveTransfer uses for virtual folders and file operations, and where to go for details about specifying those file paths.

<b>File Path</b>	<b>Where to Go for More Information</b>
Path associated with a virtual folder’s physical local or remote location	<a href="#">“Associating a Virtual Folder with a Physical Folder Location” on page 127</a>
Path that represents the destination for copy or move file operations for configured events	<a href="#">“Copying or Moving Files” on page 151</a>
Path that represents the destination for unzip file operations for configured events	<a href="#">“Unzipping Files” on page 160</a>
Path that represents the location of files for find operations for configured events	<a href="#">“Finding Files” on page 146</a>
Path that represents the destination for file write operations for configured events	<a href="#">“Writing Content to a File” on page 163</a>
Path that represents the location of files for zip file operations for configured events	<a href="#">“Zipping Files” on page 166</a>

# E Limitations

---

■ Limitations .....	434
---------------------	-----

## 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	Does not support the Rename operations.
	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.

