

Managing File Transfers with webMethods ActiveTransfer Gateway

Version 10.5

October 2019

This document applies to webMethods ActiveTransfer Version 10.5 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 © 2012-2019 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 <http://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 <http://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 <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

Table of Contents

About this Guide.....	5
Document Conventions.....	5
Online Information and Support.....	6
Data Protection.....	7
Understanding ActiveTransfer Gateway.....	9
Overview.....	10
How ActiveTransfer Gateway Works.....	10
Configuring ActiveTransfer Gateway.....	13
Before Configuring ActiveTransfer Gateway.....	14
Setting Up ActiveTransfer Gateway.....	14
Configuring ActiveTransfer Gateway.....	14
Configuring an Internal ActiveTransfer Server to Connect to ActiveTransfer Gateway.....	15
Managing the ActiveTransfer Gateway Configuration.....	16
Viewing and Editing Details for an ActiveTransfer Gateway.....	16
Banning IP Addresses.....	17
Supporting Virus Scanning with Internet Content Adaptation Protocol.....	17
How Does Virus Scan Work?.....	18
Memory Configuration for Virus Scanning of Files Exceeding Scan Buffer Size.....	20
Configuring Antivirus Scan for Inbound Files.....	21
Monitoring File Transaction Status for Virus Scanning.....	23
Server Configuration Parameters.....	25
Server Configuration Parameters.....	26
mft.gatewayServer.....	26

About this Guide

Managing File Transfers with webMethods ActiveTransfer Gateway explains how to configure ActiveTransfer Gateway to work with ActiveTransfer Server to manage file transfers and common administrative tasks, such as configuring and managing the Gateway instances.

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

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.

Convention	Description
...	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 "<http://documentation.softwareag.com>". The site requires credentials for Software AG's Product Support site Empower. If you do not have Empower credentials, you must use the TECHcommunity website.

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.asp" and give us a call.

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at "<http://techcommunity.softwareag.com>". You can:

- Access product documentation, if you have TECHcommunity 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.

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 Gateway

■ Overview	10
■ How ActiveTransfer Gateway Works	10

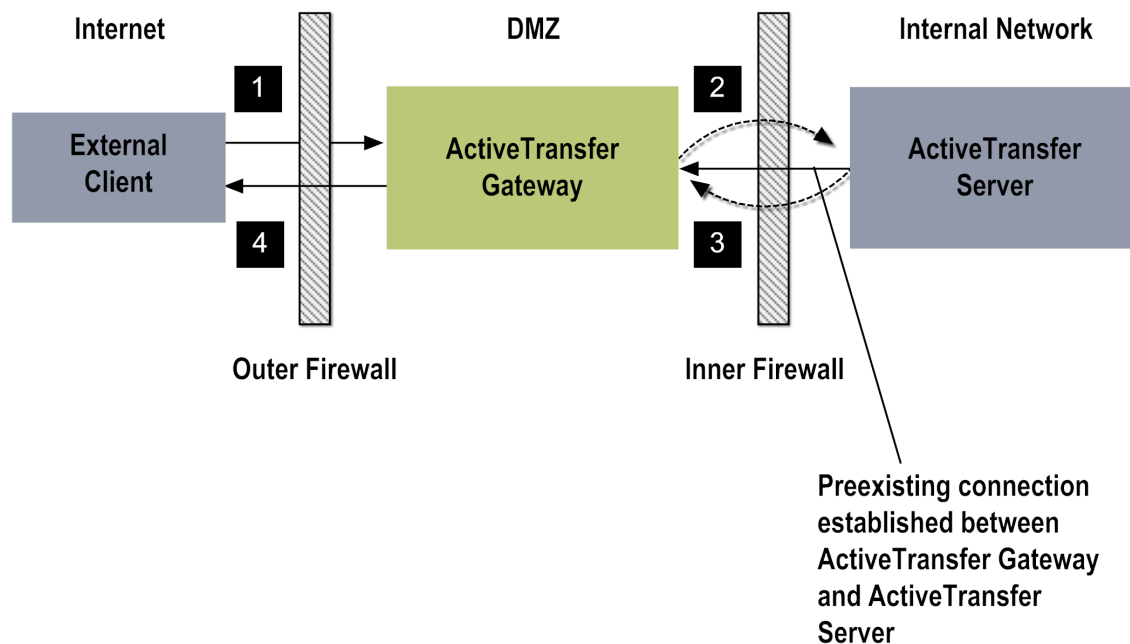
Overview

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 from 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.

How ActiveTransfer Gateway Works

The following diagram illustrates how an external client request is handled in an ActiveTransfer Gateway configuration:

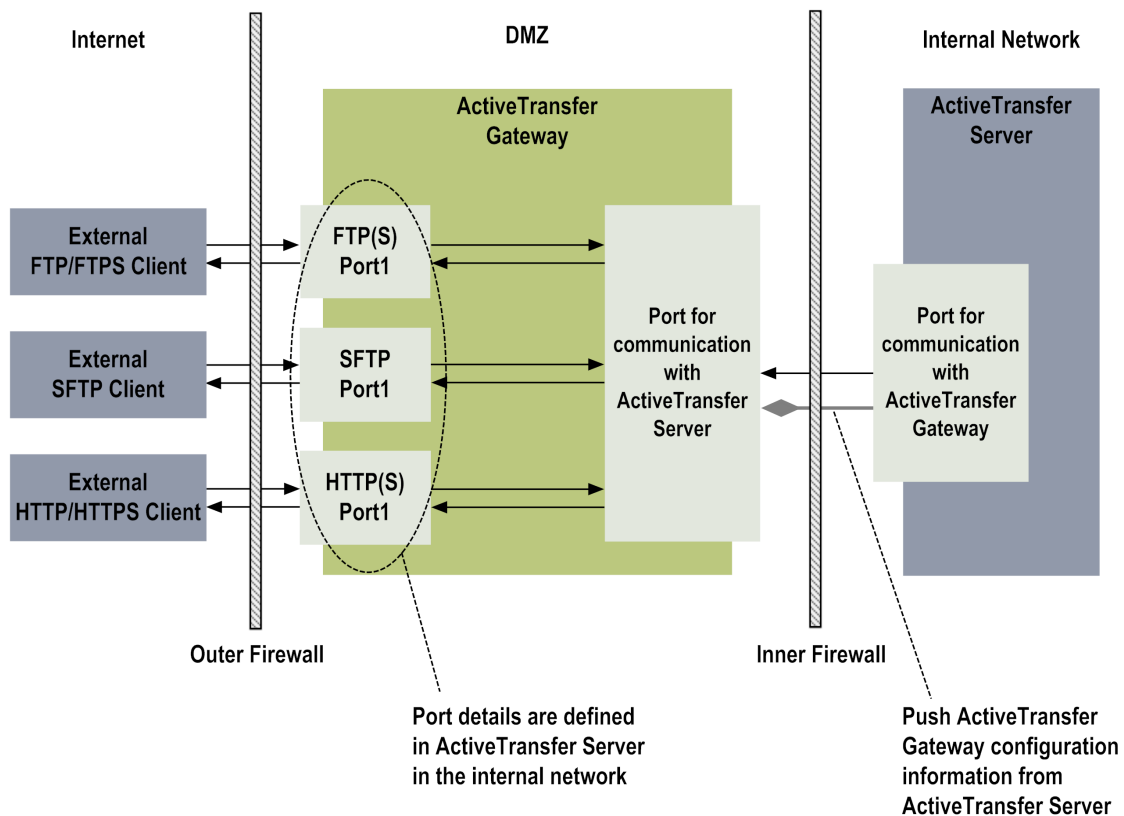


In an ActiveTransfer Gateway configuration, external clients send requests to ActiveTransfer Gateway (1). ActiveTransfer Gateway passes the requests to ActiveTransfer Server (2). After processing the requests, ActiveTransfer Server sends a

response to ActiveTransfer Gateway (3), which then passes the response to the external client (4).

The ports that ActiveTransfer Gateway uses are configured to listen for each protocol required by external clients. ActiveTransfer Server contains the core processing logic for sending and receiving files, as well as configuration settings for users, virtual file system definitions, and post-processing and scheduled events. In addition, ActiveTransfer Server has access to internal resources such as file systems, databases, and other applications. No configuration or processing logic is stored on ActiveTransfer Gateway, and ActiveTransfer Gateway cannot access any internal resources.

The following diagram provides a more detailed view of the ActiveTransfer Gateway architecture:



When the ActiveTransfer Gateway instance starts, the instance listens for connections from an ActiveTransfer Server. If ActiveTransfer Gateway can connect to ActiveTransfer Server, the Gateway establishes a communication channel with that server. This communication, which ActiveTransfer Server initiates, is over an SSL socket and uses an HTTP port called the *registration port*. ActiveTransfer Server then attaches the connection to the first HTTP port internally that it finds in its list of ports.

ActiveTransfer Gateway configuration settings, such as ports to be opened and settings for encryption or server access, are stored on ActiveTransfer Server, not on ActiveTransfer Gateway. ActiveTransfer Gateway does not store any information on its own and does not require a database for ActiveTransfer.

After the connection is established, ActiveTransfer Server pushes the configuration settings to ActiveTransfer Gateway. ActiveTransfer Gateway opens the required ports for each of the protocols according to the configuration settings. External clients can connect to ActiveTransfer Gateway using any of these ports. When the Gateway receives a request from an external client, the Gateway forwards the request to ActiveTransfer Server using the communication channel opened between them by way of the registration port. From there, ActiveTransfer Server authenticates the user and performs the required validations.

Note: ActiveTransfer Gateway uses port 8501 to communicate with ActiveTransfer Server: the registration port and the next consecutive port. For example, if the registration port is 8500, ActiveTransfer Server needs to be able to open ports 8500 and 8501 to connect to ActiveTransfer Gateway.

ActiveTransfer Gateway streams data and commands between the inbound connection with the external client and the connection to ActiveTransfer Server. No data or temporary files are stored in the DMZ.

2 Configuring ActiveTransfer Gateway

■ Before Configuring ActiveTransfer Gateway	14
■ Setting Up ActiveTransfer Gateway	14
■ Managing the ActiveTransfer Gateway Configuration	16
■ Viewing and Editing Details for an ActiveTransfer Gateway	16
■ Banning IP Addresses	17
■ Supporting Virus Scanning with Internet Content Adaptation Protocol	17

Before Configuring ActiveTransfer Gateway

Before you start performing the configuration tasks described in this chapter, make sure you complete these tasks:

- Ensure that you have a valid license file for ActiveTransfer Gateway.
For details, see the "ActiveTransfer License File" section in *Managing File Transfers with webMethods ActiveTransfer*.
- Ensure that ActiveTransfer Gateway is installed. For details, see *Installing Software AG Products*.
- Ensure that all the Gateway nodes in the ActiveTransfer installation run the same webMethods ActiveTransfer version, with the same fixes applied.
- Ensure that My webMethods Server and Integration Server are started, in that order.

Setting Up ActiveTransfer Gateway

You must complete two main tasks when setting up an ActiveTransfer Gateway:

- Install and configure an ActiveTransfer Gateway within the demilitarized zone (DMZ) of your firewall.
- Configure your internal ActiveTransfer Server to connect to ActiveTransfer Gateway.

Configuring ActiveTransfer Gateway

Prerequisites: ActiveTransfer Server is installed and configured.

Follow these high-level steps to get ActiveTransfer Gateway up and running.

To configure an internal ActiveTransfer Server to connect to ActiveTransfer Gateway

1. Install ActiveTransfer Gateway according to the instructions in *Installing Software AG Products*.

These next configuration steps assume that you have already completed all the steps listed in the summary of configuration of steps. For details, see the "Summary of Configuration Steps" in *Managing File Transfers with webMethods ActiveTransfer*.

2. If you want to change the default registration port for ActiveTransfer Gateway, set the new value in the `mft.gatewayServer.port` parameter. For details, see "[Server Configuration Parameters](#)" on page 26.
3. Specify the ActiveTransfer Servers that ActiveTransfer Gateway should accept connections from by providing the IP address of those servers in the `mft.gatewayServer.accept.ip.list` parameter. If this parameter is left blank,

ActiveTransfer Gateway accepts connections from any ActiveTransfer Server. For details, see [“Server Configuration Parameters” on page 25](#).


Note: Ensure that you configure ActiveTransfer Gateway to accept client connections through the registration port only from ActiveTransfer Servers. In addition, make sure that your network settings (firewall, proxy, and so on) for ActiveTransfer Servers are configured to block the connections from other applications for enhanced security.

4. Start ActiveTransfer Gateway. When the Gateway starts, it listens for a connection from one of the ActiveTransfer Servers specified in the `mft.gatewayServer.accept.ip.list` parameter.

Configuring an Internal ActiveTransfer Server to Connect to ActiveTransfer Gateway

All ActiveTransfer Gateway configuration information is stored within the firewall, on the internal ActiveTransfer Server. This configuration information is pushed to the applicable ActiveTransfer Gateways when you save a configuration on the Server Management page. Use the following procedure to configure an internal ActiveTransfer Server to connect to ActiveTransfer Gateway.

To configure an internal ActiveTransfer Server to connect to ActiveTransfer Gateway

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see the "Selecting the Instance to Work With" section in *Managing File Transfers with webMethods ActiveTransfer*.
3. Click the **Gateway** tab and then click the  button.
4. In the **Name** box of the Add a Gateway Server Configuration dialog box, type the name of the ActiveTransfer Gateway to which you are connecting.
5. In the **Host IP Address** box, type the IP address for the ActiveTransfer Gateway.
6. In the **Port** box, type the registration port number through which ActiveTransfer Server will connect to the ActiveTransfer Gateway. Specify the same port that you specified in the `mft.gatewayServer.port` parameter in [“Understanding ActiveTransfer Gateway” on page 9](#).
7. Click **OK**.
8. Select the ActiveTransfer Gateway instance that you just configured using **Select Servers**.
9. Add a port on the Gateway instance. For details about adding ports, see the "Adding a Port" section in *Managing File Transfers with webMethods ActiveTransfer*.

Note: You can use this port to access the Gateway from an ActiveTransfer Server instance by logging in with the users configured on the server.

10. Click the **Check Status** button on the **Basic** tab to check the status of the ActiveTransfer Gateway. If the **Connect to ActiveTransfer Gateway** check box is not already selected, select it to establish the connection between the Gateway and the specified ActiveTransfer Server.

Managing the ActiveTransfer Gateway Configuration

Use any of the procedures documented in *Managing File Transfers with webMethods ActiveTransfer* to configure ActiveTransfer Gateway with one difference—after selecting the server instance, select the gateway instance in the **Server Management > Gateway** tab. This Gateway page lists the ActiveTransfer Gateways configured for the specified ActiveTransfer Server. You must apply the following configurations specifically to the gateway instance because ActiveTransfer Gateway does not share these configurations with ActiveTransfer Server:

- Ports
- Throttling
- Restrictions
- Banning
- Encryption
- Miscellaneous

Adding Ports to ActiveTransfer Gateway

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

Viewing and Editing Details for an ActiveTransfer Gateway

Use this procedure to view and edit details about a specific ActiveTransfer Gateway, including the Gateway's status and host and port information.

To view and edit details for an ActiveTransfer Gateway

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management**.
2. Select the server instance. For details, see the "Selecting the Instance to Work With" section in *Managing File Transfers with webMethods ActiveTransfer*.
3. Click the **Gateway** tab.
4. Select an ActiveTransfer Gateway from the list of Gateways.
5. In the **Status** section, do the following:

- a. The **Connect to ActiveTransfer Gateway** check box indicates whether ActiveTransfer Server and ActiveTransfer Gateway are connected. Do one of the following:

- To establish the connection, select this check box.

Note: If the internal server was connected to another ActiveTransfer Gateway, clear the check box for that Gateway when you are finished performing the remaining steps in this procedure, and then restart ActiveTransfer Server.

- To disconnect ActiveTransfer Gateway from ActiveTransfer Server the next time the server restarts, clear this check box.

- b. Click the **Check Status** button to confirm the connection.

6. In the **Settings** section, view and change the ActiveTransfer Gateway name, host, and port as desired.

Note: If you change the port number, be sure that the next consecutive port is available. For example, if you specify 8800, make sure that port 8801 is also available.

7. If you have made changes to the Gateway's configuration, click **Save**.

Banning IP Addresses

For details on how to restrict or free access from IP addresses to your ActiveTransfer Gateway, see the "Banning IP Addresses" section *Managing File Transfers with webMethods ActiveTransfer*.

Supporting Virus Scanning with Internet Content Adaptation Protocol

You can configure ActiveTransfer Gateway to perform antivirus scanning of inbound files by using a third-party antivirus scanner which supports Internet Content Adaptation Protocol (ICAP). Antivirus scanning is limited to the scanning of inbound files, and does not support scanning of the internal ActiveTransfer Server environment or outbound files.

Virus scanning of files uploaded to ActiveTransfer Gateway requires the following:

- A dedicated ICAP-compliant server that is accessible from ActiveTransfer Gateway and performs an antivirus scan on all inbound files to detect malicious content.

Note: The set up and configuration of an ICAP server are independent of ActiveTransfer Gateway, and are not in the scope of this document.

- Configuration of ActiveTransfer Gateway to connect to the ICAP server.
- Activation of antivirus scanning by the configured ICAP server.

While configuring the ICAP server, ensure that you address the following:

- The maximum file size that the ICAP server can handle is higher than the **Total Scan Buffer Size** configured in ActiveTransfer Gateway.
- The ICAP server can process encrypted files. If you do not include this configuration, the ICAP server might report the virus scan result incorrectly.

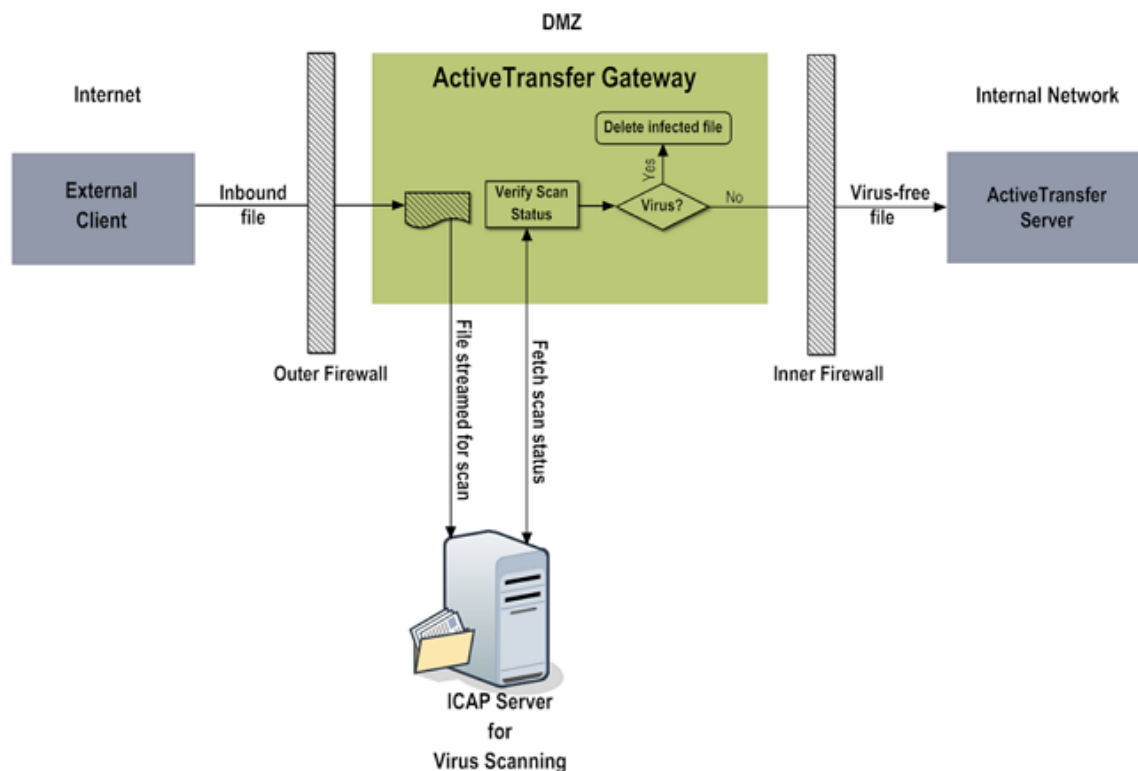
How Does Virus Scan Work?

Once you have configured your ICAP server, configured ActiveTransfer Gateway to connect to the ICAP server, and activated virus scanning in ActiveTransfer Gateway, all files uploaded to ActiveTransfer Gateway are scanned for viruses.

The configured **Scan Buffer Size Per Upload** determines the exact process used to handle files of varying sizes for the antivirus scan. ActiveTransfer Gateway handles the virus scan process differently for files and files that exceed the **Scan Buffer Size Per Upload** limit.

Antivirus Scan Process for Small or Medium-Sized Files

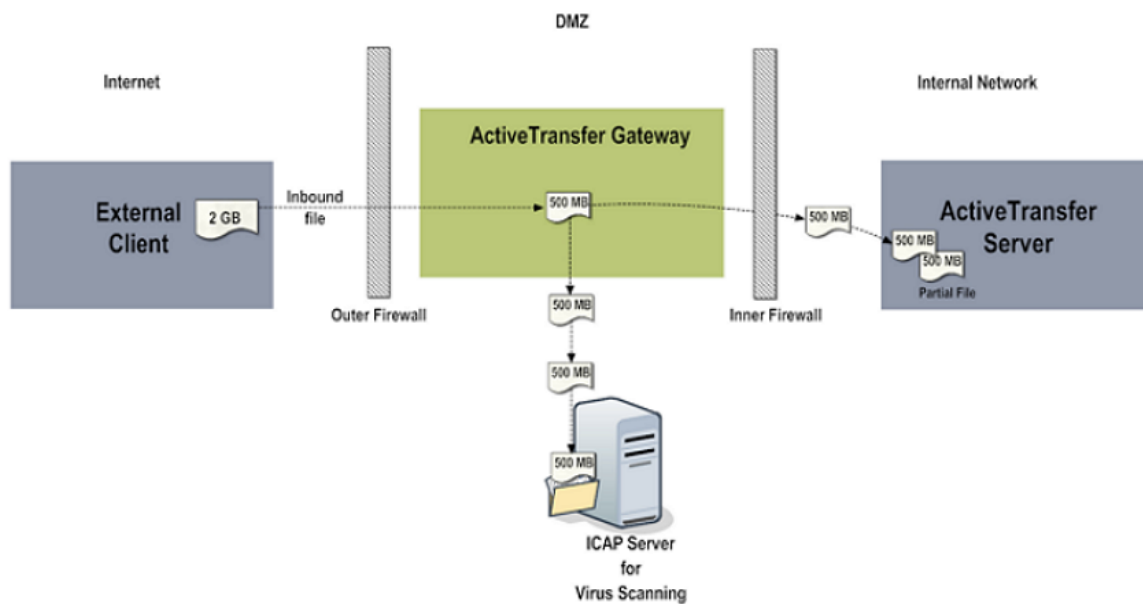
The following diagram illustrates the antivirus scan process for files that are within the **Scan Buffer Size Per Upload** limit—that is, small or medium-sized files.



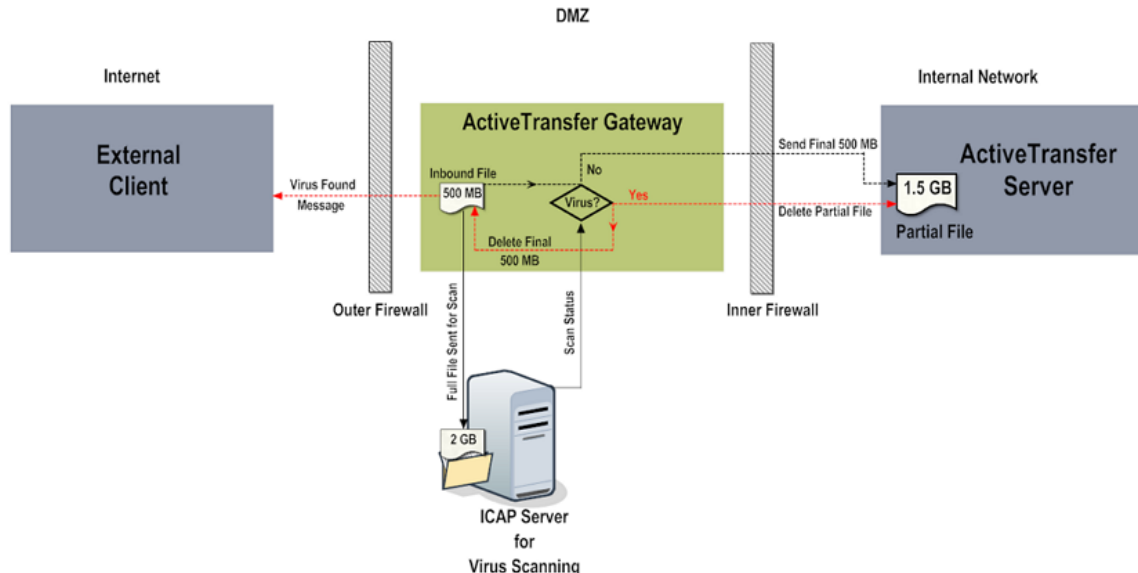
ActiveTransfer Gateway holds the file data in-memory, and forwards the file data to the ICAP server for virus scanning. The ICAP server scans the file data for malicious content and sends the scan result to ActiveTransfer Gateway. If the ICAP server detects a virus, ActiveTransfer Gateway discards the data and does not send the file to ActiveTransfer Server. The corresponding file transaction in ActiveTransfer Server is marked as failed. If the file is virus-free, ActiveTransfer Gateway forwards the file to ActiveTransfer Server for further processing. The corresponding file transaction is marked as successful.

Antivirus Scan Process for Files Exceeding the Scan Buffer Size Per Upload

When a file exceeds the **Scan Buffer Size Per Upload**, ActiveTransfer Gateway accepts and forwards the configured scan buffer file data successively and simultaneously to the ICAP server for scanning and ActiveTransfer Server as illustrated in the following diagram:



The following diagram illustrates what occurs when the ICAP server reports the virus scan result:



If the ICAP server detects any virus in the file data sent for scanning, the ICAP server reports it to ActiveTransfer Gateway. ActiveTransfer Gateway then stops the file upload, deletes the file data from in-memory, and triggers deletion of the partial file data in ActiveTransfer Server. If the virtual folder for the file upload points to a remote server, the user that ActiveTransfer uses to access the remote server must have delete permissions to remove the partially infected file. The corresponding file transaction in ActiveTransfer Server is marked as failed. If the file is virus-free, ActiveTransfer Gateway forwards the file to ActiveTransfer Server for further processing. The corresponding file transaction is marked as successful.

Important: If the virtual folder users access the partial file before the virus scan is complete, they run the risk of infecting their network or internal file system.

Memory Configuration for Virus Scanning of Files Exceeding Scan Buffer Size

Files that exceed the specified scan buffer size require you to plan memory configurations across multiple applications for the expected volume of inbound file load.

For example, if 100 MB is the scan buffer size and you have 10 files of size greater than 100 MB being uploaded concurrently, then 1000 MB of available memory will be used by the virus scanning process. The upload of any additional files will fail because JVM has reached its memory limit. To handle such scenarios, you must consider the following points:

- **Scan buffer size configured in ActiveTransfer Gateway.** In the **Antivirus Scan** tab of the ActiveTransfer Gateway management page, set the **Scan Buffer Size** for file data as any one the following:

- No value: If you don't define any value here, the default scan buffer size is 100 MB. The default scan buffer size is *Unlimited* (that is, zero). This value means ActiveTransfer Gateway retains the whole file in-memory while scanning is in progress.
- 0. Set this value for ActiveTransfer Gateway to accept unlimited file buffer size. Software AG does not recommend the use of 0 because it could consume all the available memory.
- *Limited scan buffer size*: You can specify any scan buffer size other than zero.
- **File size configured in the ICAP server.** When configuring the ICAP server, ensure that the ICAP server supports the maximum file size you expect to receive. For example, if you set the maximum file size as 80 MB, and the file received is 100 MB, the virus scan result might not be accurate. ICAP might report that the file is virus-free despite the file being infected.

For recommendations on optimal configuration of your ICAP server, see the ICAP server documentation.

- **JVM memory configured in Integration Server.** When configuring for antivirus, ensure that the JVM size is considerably larger than the scan buffer size you set for inbound files in ActiveTransfer Gateway.

If a file size exceeds the JVM memory limits, file upload fails.

Configuring Antivirus Scan for Inbound Files

Prerequisites:

1. JVM memory is configured appropriately in ActiveTransfer Gateway.
2. The ICAP server is accessible from ActiveTransfer Gateway.

You can configure an ActiveTransfer Gateway instance to connect to an 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.

To configure ActiveTransfer Gateway for antivirus scanning of inbound files

1. In My webMethods: **Administration > Integration > Managed File Transfer > Server Management.**
2. Select the server instance. For details, see the "Selecting the Instance to Work With" section in *Managing File Transfers with webMethods ActiveTransfer*.
3. Click the **Antivirus Scan** tab.
4. In the **Status** section, select **Activate Antivirus Scan**.

You can deactivate virus scanning at any time by clearing the **Activate Antivirus Scan** check box.

5. In the **Settings** section, specify the ICAP server details:

Field	Description
ICAP Server Name	Type a suitable name for the ICAP server.
Host	Type the hostname or IP address of the server that hosts the ICAP server.
Port	Type the port number assigned to the ICAP server host.
Service Configuration	<p>Specify the virus scan service name of the ICAP server and the run-time parameter values to send to the ICAP server in the format:</p> <pre>service name?parameter 1vaule&parameter 2vaule&parameter 3vaule&...</pre> <p>Here, . . . indicates any additional parameters that you might want to include.</p> <p>For example, the c-icap server's virus service expects the following parameters</p> <pre>virus_scan?allow 204=onforce=on sizelimit=off mode=simple</pre> <p>where:</p> <ul style="list-style-type: none"> ■ <code>allow 204=on</code> 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 <code>No modification needed</code>, it indicates that no virus was found in the file. ■ <code>force=on</code> Enables scan of the file even if its file type is not included in the <code>srv_clamav.ScanFileTypes</code> directive in <code>c-icap.conf</code> file. ■ <code>sizelimit=off</code> Enables the virus scan service to ignore the <code>srv_clamav.MaxObjectSize</code> directive in <code>c-icap.conf</code> file.

Field	Description
	<ul style="list-style-type: none"> ■ <code>mode=simple</code> enables the allow204 response only when no virus is found and an error message if a virus found. <p>For details on the parameters you can use, see your ICAP server documentation.</p>
Scan Buffer Size Per Upload	<p>Type the maximum data buffer size (in MB) that ActiveTransfer Gateway must store in-memory for an individual upload before streaming the file data to the ICAP server for scanning.</p> <p>For more details on how you can determine the scan buffer size, see “Memory Configuration for Virus Scanning of Files Exceeding Scan Buffer Size” on page 20.</p>
Total Scan Buffer Size	<p>Type the maximum data buffer size (in MB) 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.</p>

6. To check the ActiveTransfer Gateway connection to the ICAP server, click **Test Connection**.
7. Click **Save**.

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

Note: You can deactivate virus scanning at any time by clearing the **Activate Antivirus Scan** selection.

Monitoring File Transaction Status for Virus Scanning

ActiveTransfer reports file uploads that pass the virus scanning successfully as successful file transactions.

ActiveTransfer reports file uploads that pass the virus scanning successfully as successful file transactions. When virus scanning is enabled, file uploads could fail for the following reasons:

- The ICAP server reports the presence of a virus in the file.

- The file size exceeds the configured **Total Scan Buffer Size**.
- ActiveTransfer Gateway loses connection to ActiveTransfer Server while transmitting a file that was successfully scanned for viruses.
- The file being scanned is an encrypted file and the ICAP server is not configured to scan encrypted files.
- ActiveTransfer Gateway fails to connect to the ICAP server.

The file transaction status is recorded in the ActiveTransfer Gateway log, ActiveTransfer Server log, and File Transactions page. For failed file transactions, ActiveTransfer sends error messages to the client from which the file was uploaded. If the failure is specifically because the ICAP server detected a virus, the error message also includes this information.

A Server Configuration Parameters

■ Server Configuration Parameters	26
---	----

Server Configuration Parameters

This section contains a description of the parameters relevant to ActiveTransfer Gateway that you can specify in the properties configuration file, `properties.cnf`. The `properties.cnf` file is located in the *Integration Server_directory*\instances*instance_name*\packages\WmMFT\config directory on ActiveTransfer Gateway. To update this file, you should first shut down ActiveTransfer Server and then ActiveTransfer Gateway. Edit the file using a text editor. After you make the changes, restart the server and the Gateway.

You can also use the `wm.mft.admin:property` service to view and change the current values of some of these parameters. For details, see *webMethods ActiveTransfer Built-In Services Reference*.

mft.gatewayServer.

This section describes the parameters you can configure for ActiveTransfer Gateway, in the properties configuration file on the Gateway. For more information about ActiveTransfer Gateway configuration, see [“Configuring ActiveTransfer Gateway” on page 13](#).

mft.gatewayServer.port

Specifies the default registration port for ActiveTransfer Gateway. This value is used when an ActiveTransfer Gateway is configured on the **Gateway** tab of the Server Management page. The default is 8500.

When ActiveTransfer Gateway runs on a port (for example, 8500), the Gateway uses the next numbered port (for example, 8501) as the data port. Therefore, when you configure the registration port, make sure the next port on the machine is also available.

mft.gatewayServer.accept.ip.list

Specifies a list of IP addresses, separated by commas, representing the ActiveTransfer Servers that ActiveTransfer Gateway should accept connections from. When the Gateway is started, only the ActiveTransfer Servers running on these IP addresses can connect to the Gateway. The default is blank, which means ActiveTransfer Gateway accepts connections from any ActiveTransfer Server.

Note: If no value is set for this property, the Gateway denies connections to ActiveTransfer Servers with IP addresses on a different subnet mask than the ones that are already connected to the Gateway. To avoid this issue, include this parameter in the `properties.cnf` file with the IP addresses of the servers on different subnet masks separated by commas.

mft.gateway.is.external.port

Specifies the external port configured for the Enterprise Gateway Server.

mft.gateway.ping.interval

Specifies the interval (in seconds) at which the ActiveTransfer Gateway will ping the ActiveTransfer Server to check if the server is running.

mft.gateway.ping.retry.count

Specifies the number of failed pings after which the ActiveTransfer Gateway ports will be disabled. Set this property to 0 if you want the ports to be disabled on first failure.