



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

| | |
|---|----|
| Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector | 4 |
| Product Overview | 5 |
| Configuring the Server | 6 |
| Threat Management Gateway 2010 | 6 |
| Threat Management Gateway 2004/2006 | 9 |
| Grant Access Privilege for Network Share | 11 |
| Install the SmartConnector | 13 |
| Prepare to Install Connector | 13 |
| Install Core Software | 13 |
| Set Global Parameters (optional) | 14 |
| Select Connector and Add Parameter Information | 15 |
| Select a Destination | 15 |
| Complete Installation and Configuration | 16 |
| Run the SmartConnector | 17 |
| Device Event Mapping to ArcSight Fields | 18 |
| Threat Management Gateway 2010 Web Proxy Service Log Mappings | 18 |
| Threat Management Gateway Firewall Service Log Mappings | 19 |
| Troubleshooting | 21 |
| Send Documentation Feedback | 22 |

Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Forefront Threat Management Gateway File (formerly Microsoft ISA Multiple Server File) and configuring the device for event collection. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Microsoft Forefront Threat Management Gateway is a comprehensive, secure Web gateway for protecting against Web-based events, providing multiple layers of continuously updated, integrated protection. The Forefront Threat Management Gateway (TMG) server provides URL filtering, anti-malware inspection, intrusion prevention, firewall, and HTTP/HTTPS inspection in a single solution.

This SmartConnector can be used to collect events from one or more Threat Management Gateway servers.

Configuring the Server

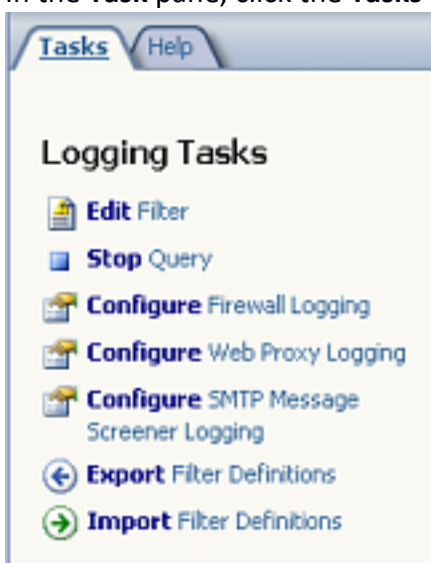
Perform the following steps for each server from which the SmartConnector is to collect events.



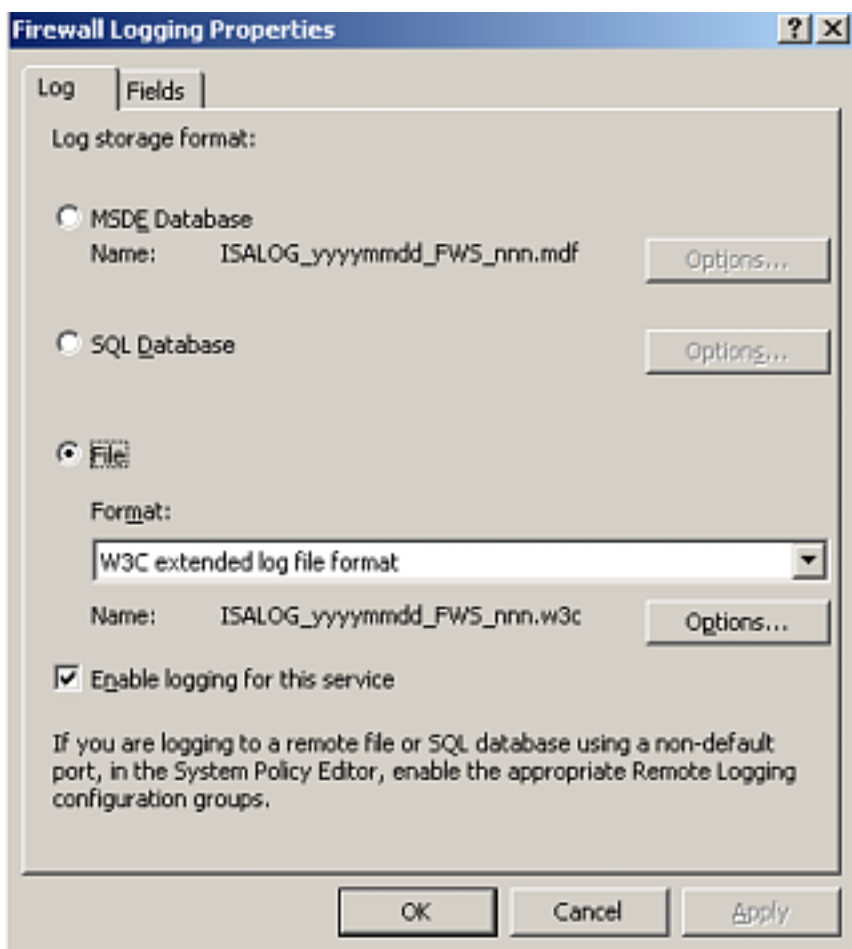
If you are planning to run the installed SmartConnector as a service, and the connector will be collecting events from multiple servers, the machine on which the connector is installed must have the same user credentials as the servers from which it is to collect events. Note that this connector cannot be run as a service when it is run remotely.

Threat Management Gateway 2010

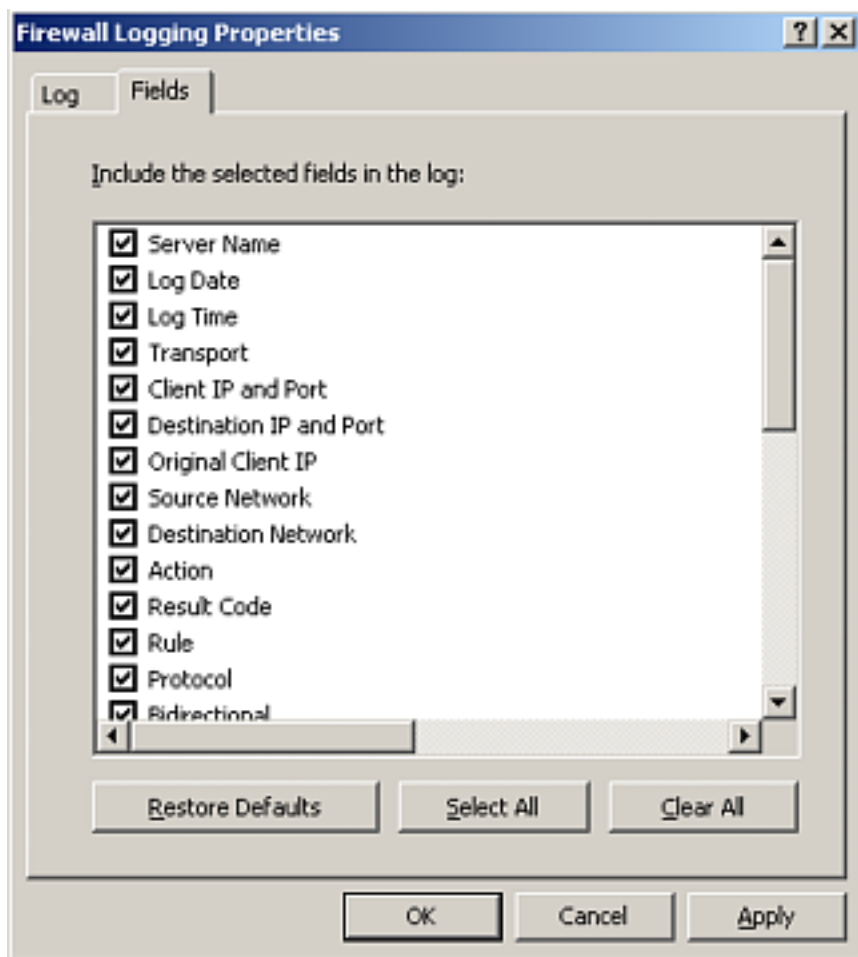
- 1 In the Management Console, expand the computer name in the left pane of the console and click the **Monitoring** node.
- 2 Click the **Logging** tab in the **Details** pane. Expose the **Task** pane if it is not already open. In the **Task** pane, click the **Tasks** tab and **Configure Firewall Logging**.



- 3 Select the **WC3 extended log file format** from the **Format** list. Confirm that a checkmark appears in the **Enable logging for this service** check box.

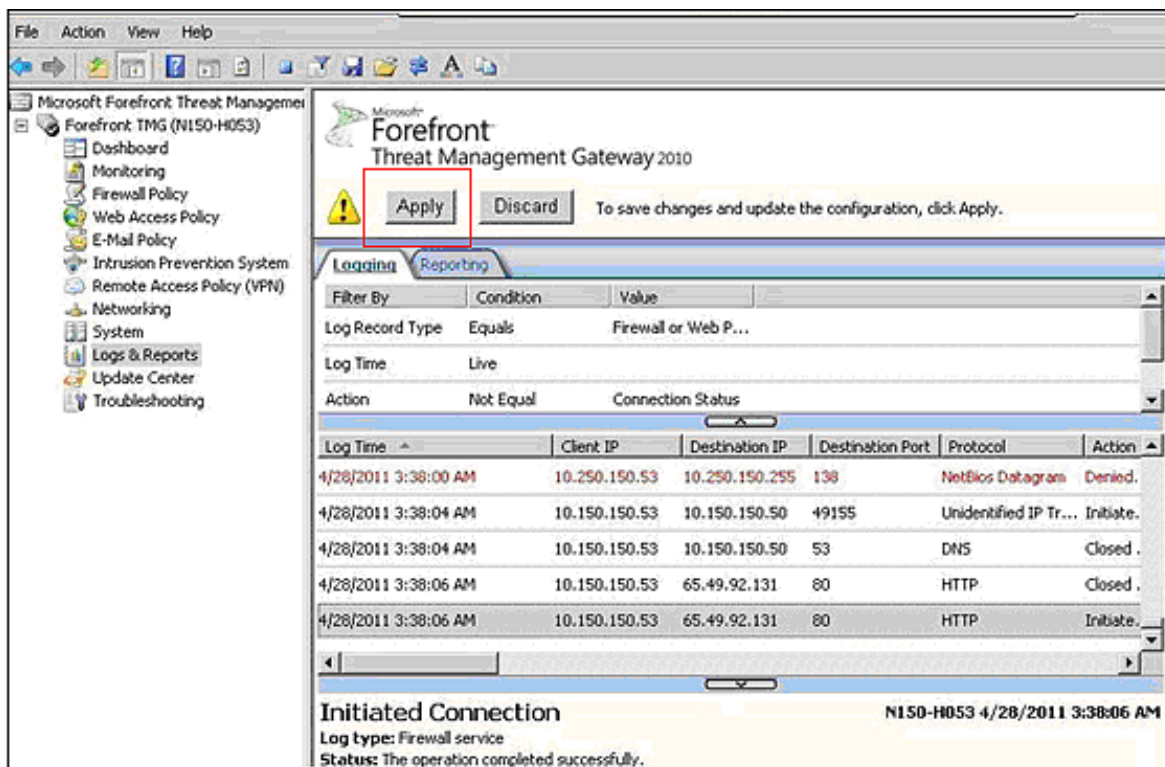


- 4 Click the **Fields** tab. Confirm that all fields are selected.



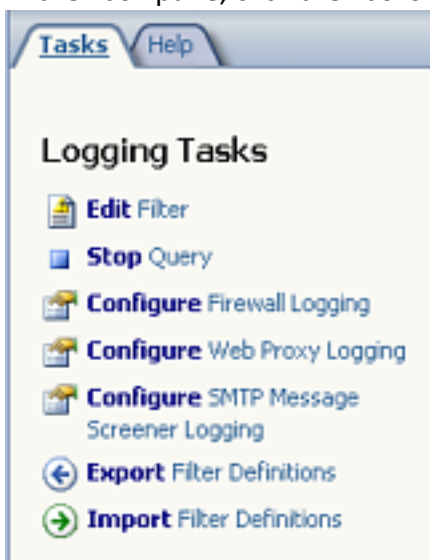
ArcSight recommends that you select all fields. Each field that appears in an event is mapped to an ArcSight field for correlation purposes; for example, Log Date and Log Time are mapped to Device Receipt Time, Transport is mapped to Transport Protocol, Protocol is mapped to Application Protocol, and so on. Any field that is not selected for logging cannot be processed.

- 5 Click **Apply** and then click **OK** in the Firewall Logging Properties dialog box.
- 6 Click **Apply** to save changes and update the firewall policy, as shown in the following image:

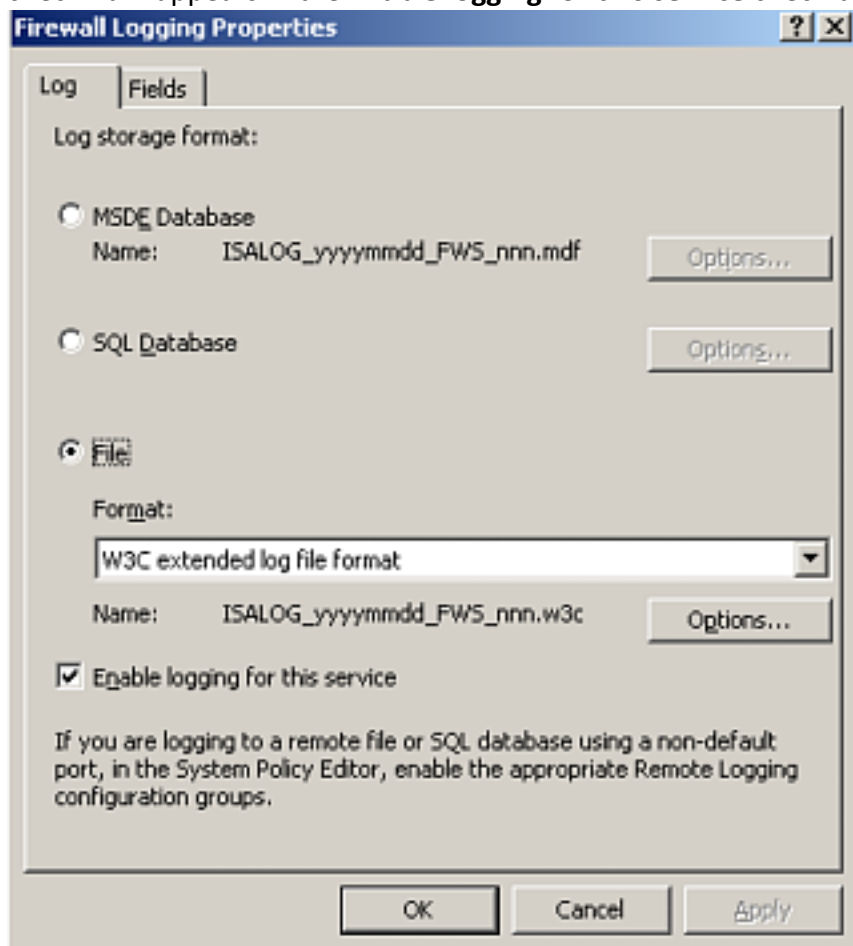


Threat Management Gateway 2004/2006

- 1 In the Management Console, expand the computer name in the left pane of the console and click the **Monitoring** node.
- 2 Click the **Logging** tab in the **Details** pane. Expose the **Task** pane if it is not already open. In the **Task** pane, click the **Tasks** tab and **Configure Firewall Logging**.

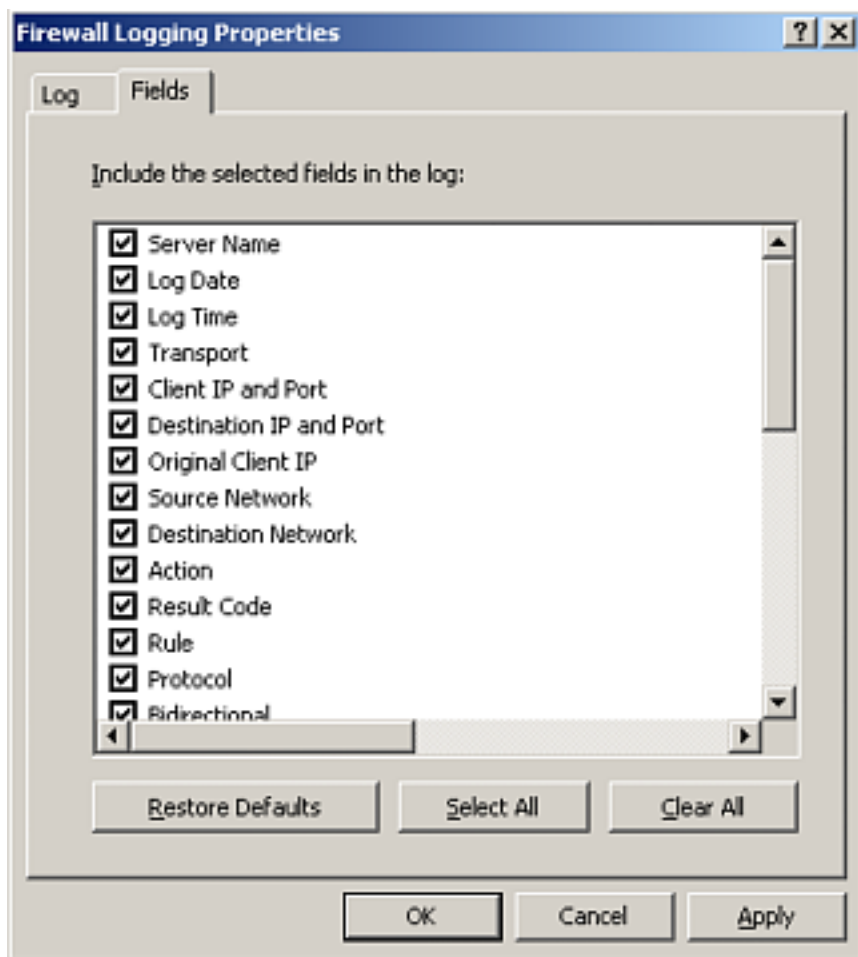


- 3 Select the **WC3 extended log file format** from the **Format** list. Confirm that a checkmark appears in the **Enable logging for this service** check box.



- 4 Click the **Fields** tab. Confirm that all fields are selected.

ArcSight recommends that you select all fields. Each field that appears in an event is mapped to an ArcSight field for correlation purposes; for example, Log Date and Log Time are mapped to Device Receipt Time, Transport is mapped to Transport Protocol, Protocol is mapped to Application Protocol, and so on. Any field that is not selected for logging cannot be processed.



5 Click **Apply** to save the changes and update the firewall policy.

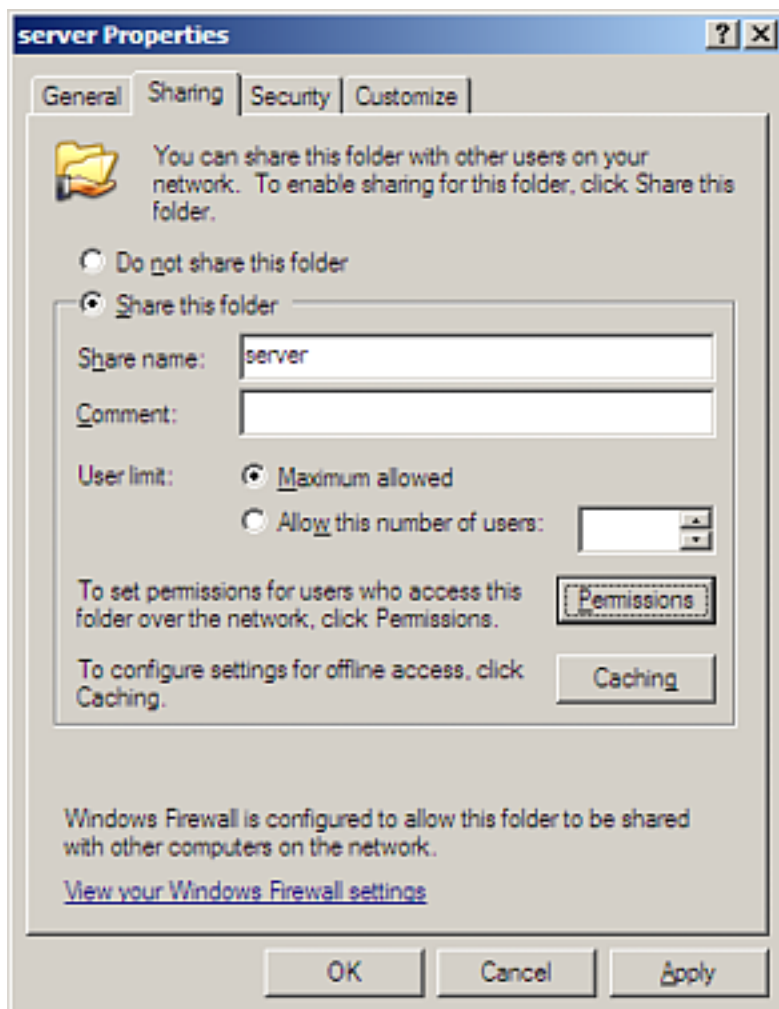
6 Click **OK** in the **Apply New Configuration** dialog box.

7 Click **OK** in the Firewall Logging Properties dialog box.

Grant Access Privilege for Network Share

To allow the SmartConnector to access the Server log folder, grant access as follows:

- 1 On each server, select the folder containing the logs. Right-click on the folder name and select **Properties**.
- 2 Click the **Sharing** tab.



3 Select **Share this folder**.

4 Click the **Permissions** tab to give the logon user of the SmartConnector machine the right to access the share you created.

5 Click **Add** and add the object type and location from the **Select Users, Computers, or Groups** dialog box. Click **OK** when you are finished adding the user; click **OK** to exit the **Permissions** window; click **OK** again to exit the **Properties** window.

If the SmartConnector is to read logs from a remote machine through a network share:

1 Use a UNC name for the folder to be shared (for example, \\computername\sharename) rather than a drive letter (such as F:).

2 Grant access privilege to the user who is to access this share.



If you run the SmartConnector as a Windows service, use the **Log on** tab to enter the name and password for the user to whom access permission is to be granted.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the OpenText SSO site.

- 1 Download the SmartConnector executable for your operating system from the OpenText SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

- Introduction
- Choose Install Folder

Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

| Parameter | Setting |
|---------------------------------|--|
| FIPS mode | Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'. |
| Remote Management | Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'. |
| Remote Management Listener Port | The remote management device will listen to the port specified in this field. The default port number is 9001. |
| Preferred IP Version | When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4. |

The following parameters should be configured only if you are using OpenText SecureData solutions to provide encryption. See the *OpenText SecureData Architecture Guide* for more information.

| Parameter | Setting |
|------------------------------|--|
| Format Preserving Encryption | Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector. |
| Format Preserving Policy URL | Enter the URL where the OpenText SecureData Server is installed. |
| Proxy Server (https) | Enter the proxy host for https connection if any proxy is enabled for this machine. |
| Proxy Port | Enter the proxy port for https connection if any proxy is enabled for this machine. |

| Parameter | Setting |
|----------------------------|--|
| Format Preserving Identity | The OpenText SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for OpenText SecureData. |
| Format Preserving Secret | Enter the secret configured for OpenText SecureData to use for encryption. |
| Event Fields to Encrypt | Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited. |

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Microsoft Forefront Threat Management Gateway File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

| Parameter | Description |
|-------------------|--|
| Server Log Folder | For each server, enter the log file home directory for your server log files. |
| Log Types | Enter the log file types to be collected (FWS, WEB, or both) from each server in the corresponding column. |

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

Select a Destination

- 1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

- 2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
- 3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

- 1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
- 3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
- 4 Click **Next** on the summary window.
- 5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter Ctrl+C in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Threat Management Gateway 2010 Web Proxy Service Log Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | High = 400 – 599; Medium = 300 – 399; Low = 100 – 299 |
| Application Protocol | cs-protocol |
| Bytes In | cs-bytes |
| Bytes Out | sc-bytes |
| Destination Address | r-ip |
| Destination Host Name | r-host |
| Destination Port | r-port |
| Destination Service Name | s-svcname |
| Device Action | action |
| Device Custom Number 3 | time-taken |
| Device Custom String 1 | c-agent |
| Device Custom String 2 | FilterInfo |
| Device Custom String 3 | sc-authenticated |
| Device Custom String 4 | rule |
| Device Custom String 5 | One of (cs-Network, cs-network) |
| Device Custom String 6 | One of (sc-Network, sc-network) |
| Device Event Class ID | sc-status |
| Device Host Name | s-computername |
| Device Process Name | s-object-source |
| Device Product | 'ISA Server' |
| Device Receipt Time | date, time |

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|-------------------------|
| Device Severity | sc-status |
| Device Translated Address | NAT address |
| Device Vendor | 'Microsoft' |
| Name | 'Web Proxy Service Log' |
| Reason | UrlCategorizationReason |
| Request Client Application | c-agent |
| Request Method | s-operation |
| Request URL | cs-uri |
| Source Address | c-ip |
| Source Port | s-port |
| Source User Name | cs-username |
| Transport Protocol | cs-transport |

Threat Management Gateway Firewall Service Log Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|---|
| Agent (Connector) Severity | High = 1 – 99, 400 – 999, 10000 – 11004, 13301, 20002; Medium = 300 – 399, 20001; Low = 0, 100 – 299, 20000 |
| Application Protocol | application protocol |
| Bytes In | bytes received |
| Bytes Out | bytes sent |
| Destination Address | First part of destination |
| Destination Port | Second part of destination |
| Destination User Name | username |
| Device Action | action |
| Device Custom IPv6 Address 2 | original client IP (Source IPv6 address) |
| Device Custom IPv6 Address 3 | destination (destination IPv6 address) |
| Device Custom Number 1 | bytes received intermediate |
| Device Custom Number 2 | bytes sent intermediate |
| Device Custom Number 3 | connection time |

Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector Device Event Mapping to ArcSight Fields

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|------------------------|
| Device Custom String 1 | agent |
| Device Custom String 2 | session ID |
| Device Custom String 3 | connection ID |
| Device Custom String 4 | rule |
| Device Custom String 5 | source network |
| Device Custom String 6 | destination network |
| Device Event Class ID | status |
| Device Host Name | computer |
| Device Payload ID | protocol payload |
| Device Product | 'ISA Server' |
| Device Receipt Time | date, time |
| Device Severity | status |
| Device Translated Address | NAT Address |
| Device Vendor | 'Microsoft' |
| Name | 'Firewall Service Log' |
| Request Client Application | agent |
| Source Address | First part of source |
| Source Port | Second part of source |
| Transport Protocol | IP protocol |

Troubleshooting

How do I specify the file rotation time zone when it is different from the connector host time zone?

The connector misses processing of events in realtime when the connector and file server are in different time zones. The `isalogfiletimezoneid` property has been added for specifying the log file rotation time zone.

To set this parameter, after connector installation, edit the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Locate the `isalogfiletimezoneid` parameter and set its value to the time zone for file rotation. Save the file and restart the connector for your changes to take effect.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!