Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft Exchange Message Tracking Log Multiple Server File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Microsoft Exchange Message Tracking Log Multiple Server File

October 17, 2017

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
03/15/2017	Added support for Microsoft Exchange Server 2016. Updated the information about enabling message tracking for Exchange 2016 and about the configuration for internal to external email traffic.
02/15/2017	Removed Device Version parameter. Removed event mappings for 2000 and 2003 due to end of support. Combined the event mappings for log 2007 and 2010 mappings.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
03/31/2015	Added support for Microsoft Exchange Server 2013 SP1.
08/15/2014	Removed the incorrect statement that this connector is supported for installation only on Windows platforms.
05/15/2014	Added support for Microsoft Exchange Server 2013.

SmartConnector for Microsoft Exchange Message Tracking Log Multiple Server File

This guide provides information for installing the SmartConnector for Microsoft Exchange Message Tracking Log Multiple Server File and configuring the device for event collection. Microsoft Exchange Servers 2007, 2010, 2013, 2013 SP1 and 2016 are supported.

Product Overview

Microsoft Exchange Server helps you manage a reliable messaging system with built-in protection against spam and viruses, while providing people throughout your organization with anywhere access to e-mail, voicemail, calendars, and contacts from a wide variety of devices.

Configuration

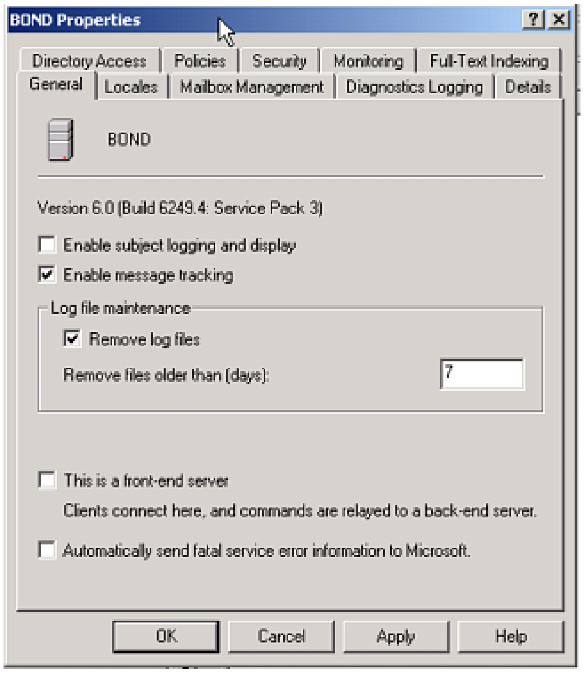
Enable Message Tracking for Exchange 2016

For information on enabling message tracking in Microsoft Exchange 2016, see:
https://technet.microsoft.com/en-us/library/aa997984(v=exchg.160).aspx

Enable Message Tracking for Exchange 2013 SP1 and earlier

To enable message tracking:

1 In the **Exchange System Manager**, right-click an Exchange server, then select **Properties**.



Version 6.0 (Build 6249.4: Service Pack 3)

☐ Enable subject logging and display

☑ Enable message tracking

Log file maintenance

☑ Remove log files

Remove files older than (days): 7

☐ This is a front-end server

Clients connect here, and commands are relayed to a back-end server.

☐ Automatically send fatal service error information to Microsoft.

2 On the **General** tab, select the **Enable message tracking** check box.

If the **Enable message tracking** check box is unavailable or appears dimmed, there is a server policy object applied to this server. You must either enable message tracking on the policy or remove the server from this policy.

3 In the **Remove files older than (days)** text box, enter the number of days that you want the files to remain on the server before being deleted.

Configure for Internal to External Email Traffic

When the Microsoft Exchange server sends an e-mail, the action initiates numerous internal events that include all the queuing stages between when the message is sent and when it is received. Each of these internal events generates an event class ID, and all these events are sent to the ArcSight Manager by the Exchange Message Tracking Log SmartConnector. Unless you need to troubleshoot the internal workings of the Exchange server, the only two events that are relevant to security monitoring are the send (outgoing) and receive (incoming) events.

The EventId parameter of the Get-MessageTrackingLog cmdlet can be used to filter the message tracking log entries by the value of the EventId field, which classifies each message event. Include only Send and Receive eventIds.

For more information, see Get-MessageTrackingLog at the following location:
https://technet.microsoft.com/en-us/library/aa997573(v=exchg.160).aspx

Install the SmartConnector

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

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 HPE SSO and Protect 724 sites.

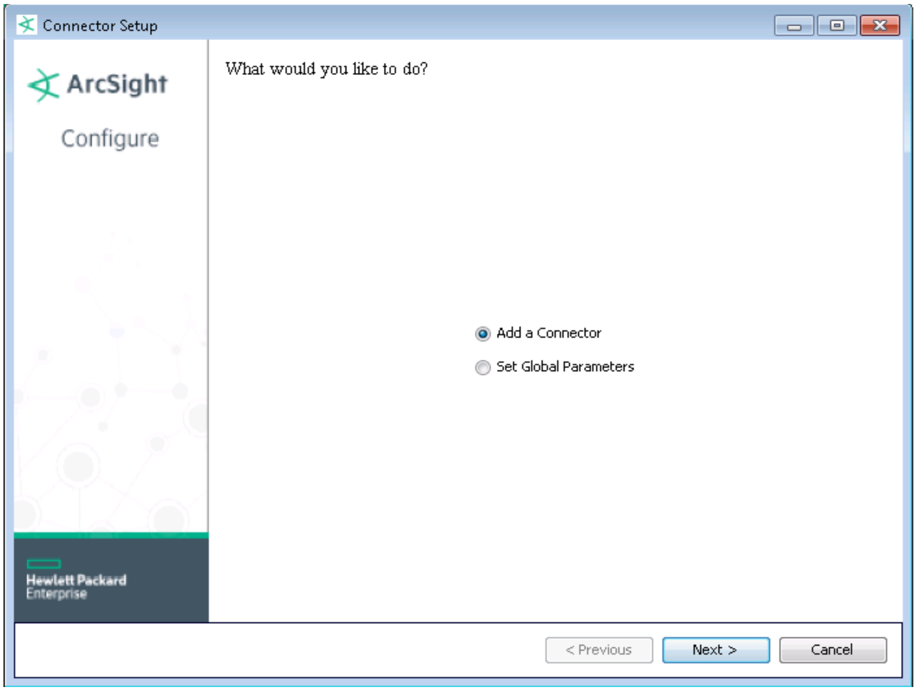
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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:



What would you like to do?

● Add a Connector
○ Set Global Parameters

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 HPE SecureData solutions to provide encryption. See the *HPE 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 HPE 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.
Format Preserving Identity	The HPE 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 HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE 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.

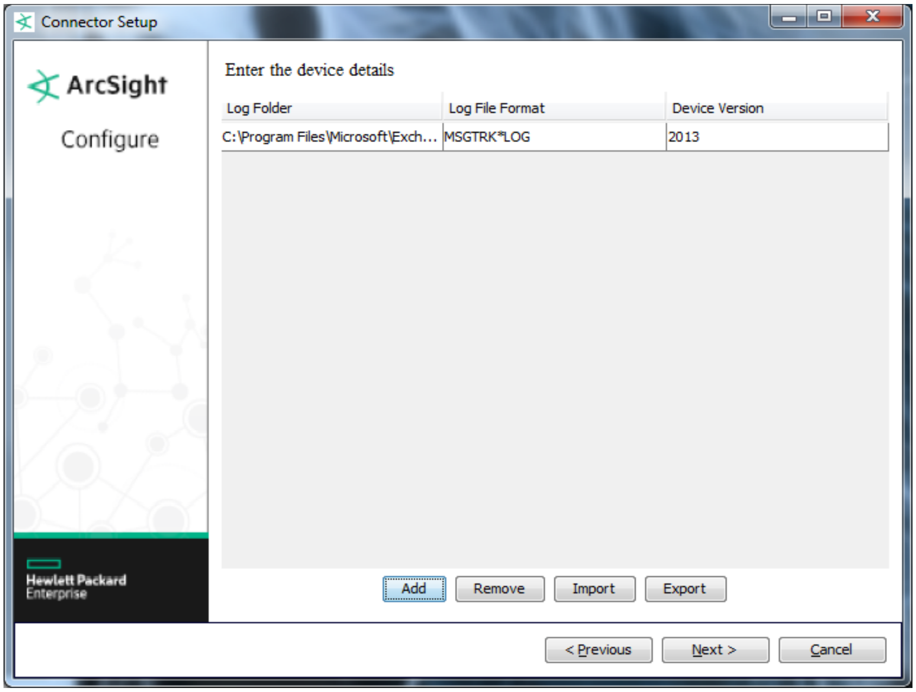
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 Exchange Message Tracking Log Multiple Server File** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Enter the device details

Log Folder	Log File Format	Device Version
C:\Program Files\Microsoft\Exch...	MSGTRK*LOG	2013

Parameter	Description
Log Folder	Replace the default file path with the path for each of your Exchange servers.
Log File Format	The default value of MSGTRK*LOG lets the connector locate all message logs starting with MSGTRK and ending with .LOG, regardless of the date format used for individual log files. The format uses a wildcard and not a regular expression. This connector does not support regular expressions for file format. Accept this default value, or enter a specific alternative value.

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.

Microsoft Exchange Message Tracking Log 2013, 2013 SP1, and 2016 Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	custom-data
Additional data	message-info
Additional data	network-message-id
Additional data	recipient-status
Additional data	related-recipient-address

ArcSight ESM Field	Device-Specific Field
Additional data	tenant-id
Additional data	transport-traffic-type
Bytes In	total-bytes (RECEIVE)
Bytes Out	total-bytes (except for RECEIVE)
Destination Address	client-ip
Destination Host Name	client-hostname
Destination User Name	recipient-address
Device Address	server-ip
Device Custom IPv6 Address 1	server-ip (Device IPv6 Address)
Device Custom IPv6 Address 3	client-ip (Destination IPv6 Address)
Device Custom Number 1	recipient-count
Device Custom String 1	internal-message-id
Device Custom String 2	message-id
Device Custom String 3	reference
Device Custom String 4	connector-id
Device Custom String 5	source-context
Device Custom String 6	return-path
Device Event Category	source
Device Event Class ID	event-id
Device Host Name	server-hostname
Device Product	''Exchange Server'
Device Receipt Time	date-time, 'GMT'
Device Vendor	'Microsoft'
Flex String 1	directionality
Message	message-subject
Name	event-id
Source Address	original-client-ip
Source Service Name	source
Source User Name	sender-address

Microsoft Exchange Message Tracking Log 2007 and 2010 Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	custom-data
Additional data	message-info
Additional data	original-client-ip
Additional data	original-server-ip
Additional data	recipient-status
Additional data	related-recipient-address
Additional data	tenant-id
Bytes In	total-bytes (RECEIVE)
Bytes Out	total-bytes (except for RECEIVE)
Destination User Name	recipient-address
Device Address	server-ip

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 1	server-ip
Device Custom IPv6 Address 2	client-ip
Device Custom Number 1	recipient-count
Device Custom String 1	internal-message-id
Device Custom String 2	message-id
Device Custom String 3	reference
Device Custom String 4	connector-id
Device Custom String 5	source-context
Device Custom String 6	return-path
Device Event Category	source
Device Event Class ID	event-id
Device Host Name	server-hostname
Device Product	'Exchange Server'
Device Receipt Time	date-time, 'GMT'
Device Vendor	'Microsoft'
Flex String 1	directionality
Message	message-subject
Name	event-id
Source Address	client-ip
Source Host Name	client-hostname
Source Service Name	source
Source User Name	sender-address

Troubleshooting

What do we need to do if the connector is to read logs from a remote machine through network share

You should have a good knowledge of UNC/network share and understand their limitations to make it possible for the Exchange SmartConnector to work from a remote machine.

There are three things to consider:

1 Use UNC name for such a share (for example, `\computername\sharename`) instead of the driver name (such as `F:`.

2 Giving access privilege to the user you use to access such share. (If you run the connector as a Winodws service, use the 'Log on' tab to enter user name and password for the user to which the file share gives access permission.)

3 If you have to use a drive letter, call the following code piece in your connector initialization method:

```
Process_process=Runtime.getRuntime().exec("net use I:
10.0.80.233\ShareTest/user:XXXXX-T40\ShareTest ShareTestPassword");
```

I configured the connector, but it never receives events. What is the problem?

Verify that the user configured to start the connector service has the necessary permissions to view and open the log files you want the connector to read, particularly if the files will be read from a shared folder on another host. Write access is not required.

One or more of the following errors may appear in `agent.log`.

```
[2007-11-06 15:06:03,486][FATAL]
[default.com.arcsight.agent.loadable.agent._ExchangeTrackingLogFileAgent]
[mainLoop] com.arcsight.common.InitializationException: Exception
initializing 'com.arcsight.agent.db.a.o': Log filename pattern must be
[prefix,],
```

When this error is observed, the problem usually lies in the syntax of the `rotationschemeparams` setting. This parameter is a list of the various parameters used in the naming of the log files. The default for Exchange is `yyyyMMdd,.log`, based upon the current day and rotated daily. The way to specify these parameters is with a comma:

```
agents[0].rotationschemeparams=yyyyMMdd,.log
[2007-11-07 13:13:39,111][WARN][default.com.arcsight.agent.db.a.v]
[startNewThread] Agent Started, but the file[C:\Testing\exch1.log\]
did not appear yet...will retry after [5] seconds.
```

The second parameter, which is commonly misconfigured, is the `logfilename` parameter, which should be populated with the local or full UNC path to the log file folder, but not the filename format:

```
agents[0].logfilename=C\:\\Testing\\
```

The last key parameters are `rotationscheme` and `followexternalrotation`, which together define the rotation method used by the application to move to the next file. Neither of these are configurable through the standard installation wizard, and these values are not the default values.

```
agents[0].rotationscheme=Daily
agents[0].followexternalrotation=false
```

To adjust these settings, open `agent.properties` (located under the connector's `/current/user/agent directory)` in a text editor and edit the values. Save the file and restart the connector.