



ArcSight SmartConnectors

Software Version: CE 24.4.1

Configuration Guide for Microsoft Exchange Message Tracking Log Multiple Server File SmartConnector

Document Release Date: December 2024

Software Release Date: December 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2024 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 Exchange Message Tracking Log Multiple Server File SmartConnector	4
Product overview	5
Configuration	6
Enable message tracking for Exchange 2016	6
Enable message tracking for Exchange 2013 SP1 and earlier	6
Configure for internal to external email traffic	7
Creating shared folder to read logs	8
Installing and configuring the SmartConnector	9
Preparing to install the SmartConnector	9
Installing and configuring the SmartConnector	9
Configuring advanced log processing parameters	11
Device event mapping to ArcSight fields	13
Microsoft Exchange message tracking log 2013, 2013 SP1, and 2016 mappings	13
Microsoft Exchange message tracking log 2007 and 2010 mappings	14
Troubleshooting	16
Send Documentation Feedback	18

Configuration Guide for Microsoft Exchange Message Tracking Log Multiple Server File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Exchange Message Tracking Log 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](#).

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 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

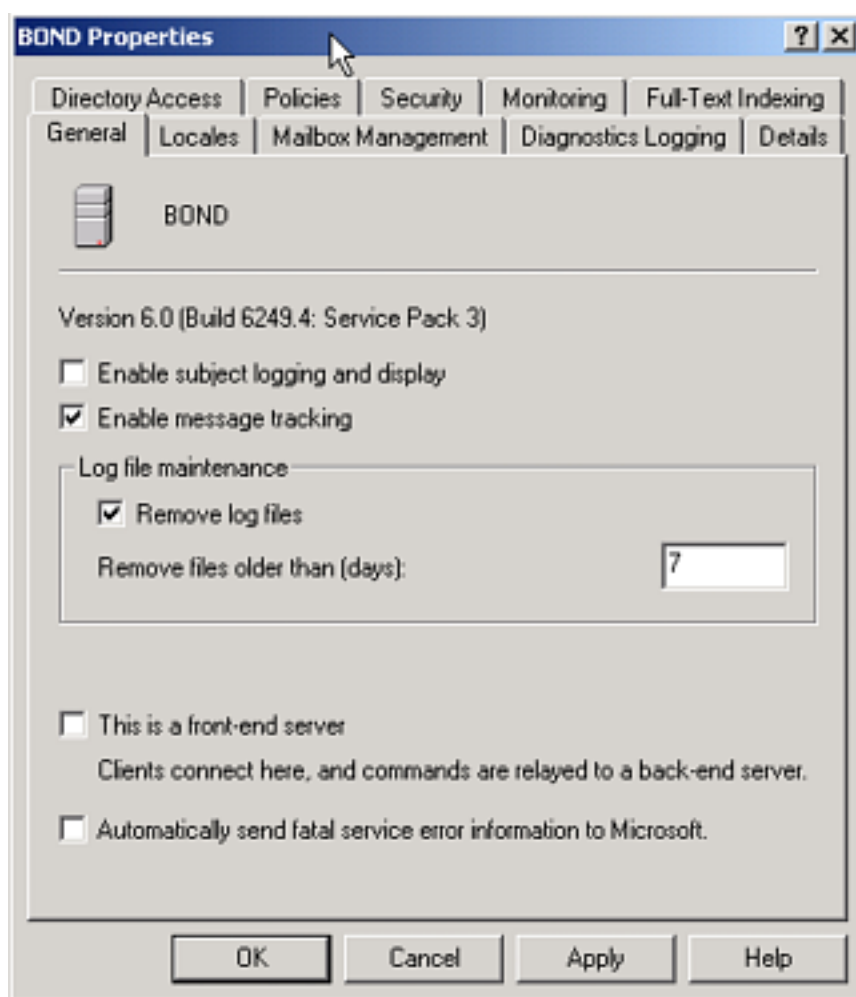
For information on enabling message tracking in Microsoft Exchange 2016, see:

[https://technet.microsoft.com/en-us/library/aa997984\(v=exchg.160\).aspx](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**.



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 email, 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](https://technet.microsoft.com/en-us/library/aa997573(v=exchg.160).aspx)

Creating shared folder to read logs

Many customers do not prefer to install SmartConnectors on their servers in a production environment.

As a best practice, OpenText recommends that you create a shared folder to periodically dump logs. You can configure SmartConnector with a service/user account that has the required privileges to read the log files from this shared folder.

Installing and configuring the SmartConnector

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

Preparing to install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).


If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. In the **Type** list, select **Microsoft Exchange Message Tracking Log Multiple Server File**, then click **Next**.
5. In the **Enter the parameter details** page, select the required value for the following parameters, and then click **Next**:

Parameter	Description
Log Folder	<p>Replace the default file path with the path for each of your Exchange servers.</p> <p>For example:</p> <pre><SmartConnector_installdir>\Logs</pre> <div>  <p>If you have created shared folders, then make sure that this path points to them.</p> </div>
Log File Format	<p>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.</p>

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



If you select **Do not import the certificate to connector from destination**, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. Optionally, configure advanced parameters in the `agent.properties` file to make any changes in the default behavior of the connector.
12. [Run the SmartConnector](#).

For more information about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Configuring advanced log processing parameters

By default, when you run the Exchange Message Tracking Log Multiple Server File SmartConnector for the first time after installation, it reads and processes all the old and present log files in the shared folder and sends the files to the configured destination. The `preservestate` and `startatend` parameters in the `agent.properties` file are set to `false` by default and the connector does not bookmark the old logs. As a result, whenever you restart the connector, it will read, process, and send all the old logs to the configured destination again, leading to duplicate log entries.

To bookmark old logs to avoid duplicate log entries:

1. Configure the following advanced parameters with the specified values in the `agent.properties` file, after installing but before running the connector:
 - `agents[0].foldertable[0].mode=RenameFileInTheSameDirectory`
 - `agents[0].foldertable[0].modeoptions=processed`
 - `agents[0].foldertable[0].preservestate=true`
 - `agents[0].foldertable[0].startatend=true`
 - `agents[0].foldertable[0].usenonlockingwindowsfilereader=true`

2. Run the connector.

The connector will start reading the old log files and bookmark them in the `agentdata` folder located at the following path:

`<connector_HOME>\current\user\agent\agentdata`



The time required to bookmark log files depends on the number of files in each exchange server and the `processinglimit` parameter in the `agent.properties` file. You can increase `processinglimit` if you have a large number of files. The default limit is 256.

3. Stop the connector after it bookmarks all the old log files.



If the `startatend` parameter is set to `true`, then the connector will not read real-time logs.

4. Set the `startatend` parameter to `false` in the `agent.properties` file:
`agents[0].foldertable[0].startatend=false`

5. Restart the connector.

Now, the connector will ignore the old logs as they have been bookmarked and process only the real-time logs, which will be sent to the configured destination.

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
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

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
Device Address	server-ip
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 Windows 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 `logfile` parameter, which should be populated with the local or full UNC path to the log file folder, but not the filename format:

```
agents[0].logfile=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.

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 receive 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 Exchange Message Tracking Log Multiple Server File SmartConnector (SmartConnectors CE 24.4.1)

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!