



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Windows Event Log –
Unified: Microsoft Exchange Access Auditing

Supplemental Configuration Guide

July 15, 2017

Supplemental Configuration Guide

SmartConnector for Microsoft Exchange Access Auditing Windows Event Log Unified

July 15, 2017

Copyright © 2010 – 2017 Hewlett Packard Enterprise Development LP

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
07/15/2017	Removed platform support for Windows 2003.
02/14/2014	Added recommendation to use the SmartConnector for Microsoft Exchange PowerShell for Exchange 2010 and later versions.
09/30/2013	Updated "Collect Events from the Event Log" procedure.
05/15/2012	Updated for new installation procedure.
03/30/2012	Added configuration information for application logs.
02/15/2012	Added IPv6 mapping support.
11/15/2011	Updated configuration information.
09/24/2010	First edition of this configuration guide, for initial support of Microsoft Exchange Mailbox Access Auditing events 10100, 10102, 10104, and 10106 with Microsoft Exchange 2007 SP2..

Contents

Product Overview.....	4
Enable Mailbox Access Auditing.....	4
Access the Audited Information	7
Change Default Properties.....	7
Exclude Service Accounts.....	8
Connector Installation and Configuration	8
Collect Events from the Event Log.....	8
Device Event Mapping to ArcSight Fields	9
Exchange Event 10100 Mappings	9
Exchange Event 10102 Mappings	9
Exchange Event 10104 Mappings	10
Exchange Event 10106 Mappings	10

SmartConnector for Microsoft Exchange Mailbox Access Auditing Windows Event Log Unified

This guide provides information about the SmartConnector for Microsoft Exchange Access Auditing Windows Event Log Unified and its event mappings to ArcSight data fields. This connector supports Microsoft Exchange Server 2007 audit application events for Windows Server 2008 and Windows Server 2008 R2 versions only.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is very difficult due to the potential number of mailboxes and the vast amount of data they may contain, and Windows Event Log integration for this will not work.

Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP2 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

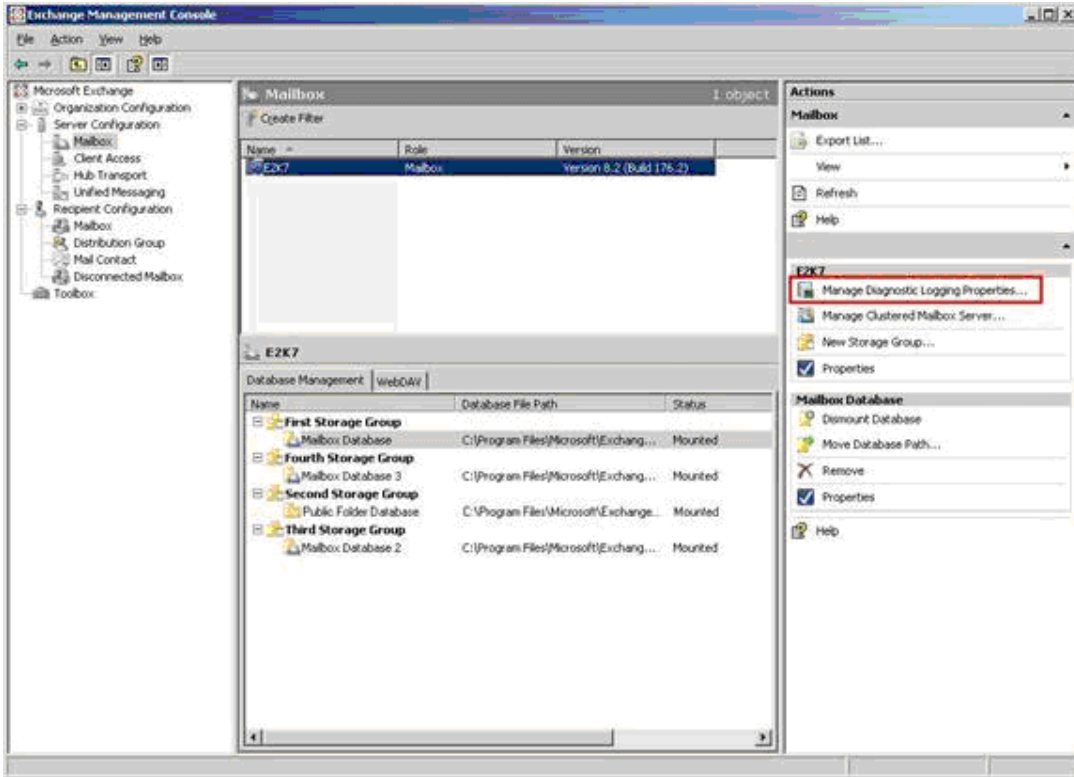
The *ArcSight SmartConnector Mappings to Windows Security Events* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Unified: Microsoft Exchange Audit. .

Product Overview

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions. Microsoft Exchange 2007 Service Pack 2 is supported by this SmartConnector.

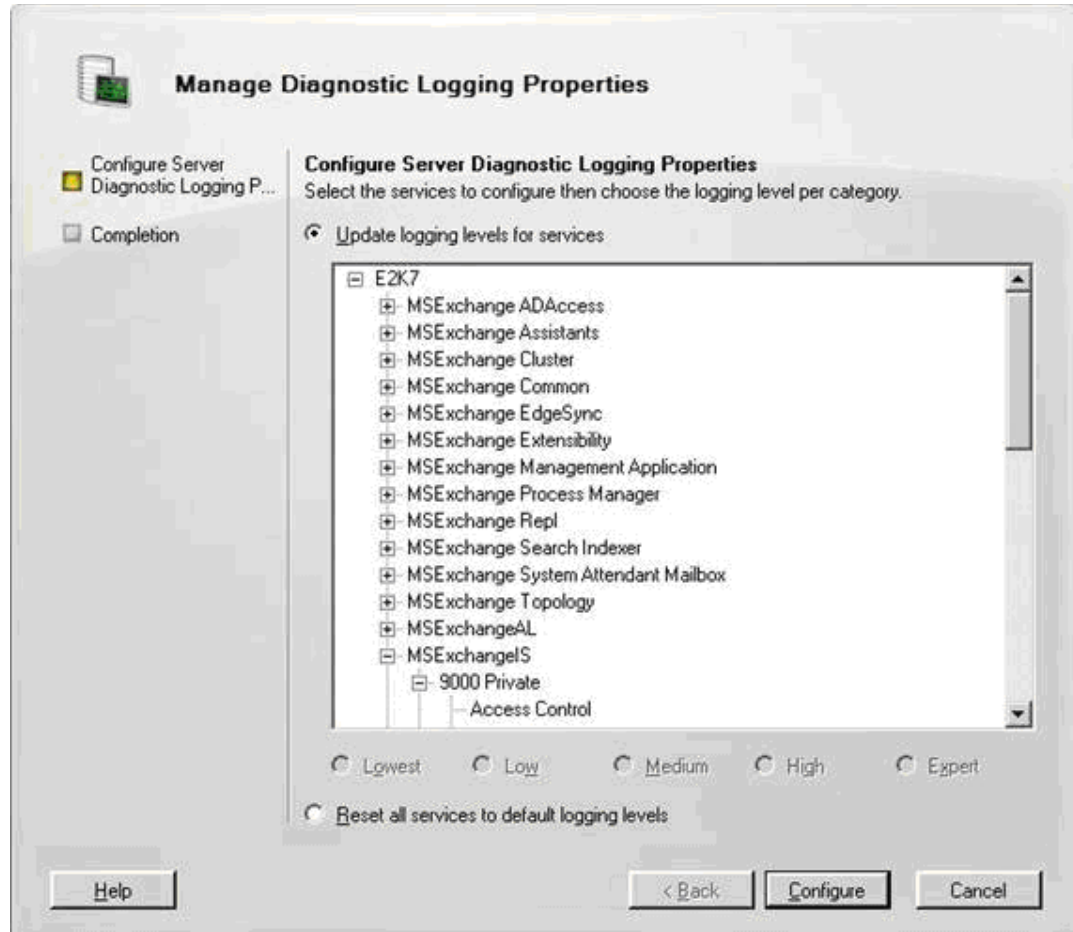
Enable Mailbox Access Auditing

To access the configuration area for mailbox access auditing, use the Exchange Management Console. The following figure shows the new **Manage Diagnostic Logging Properties** menu option.



To configure mailbox access auditing on a particular mailbox server:

- 1 Select that server in the Exchange Management Console and then select the **Manage Diagnostics Logging Properties** menu option from the action pane; the **Manage Diagnostics Logging Properties** window is displayed.



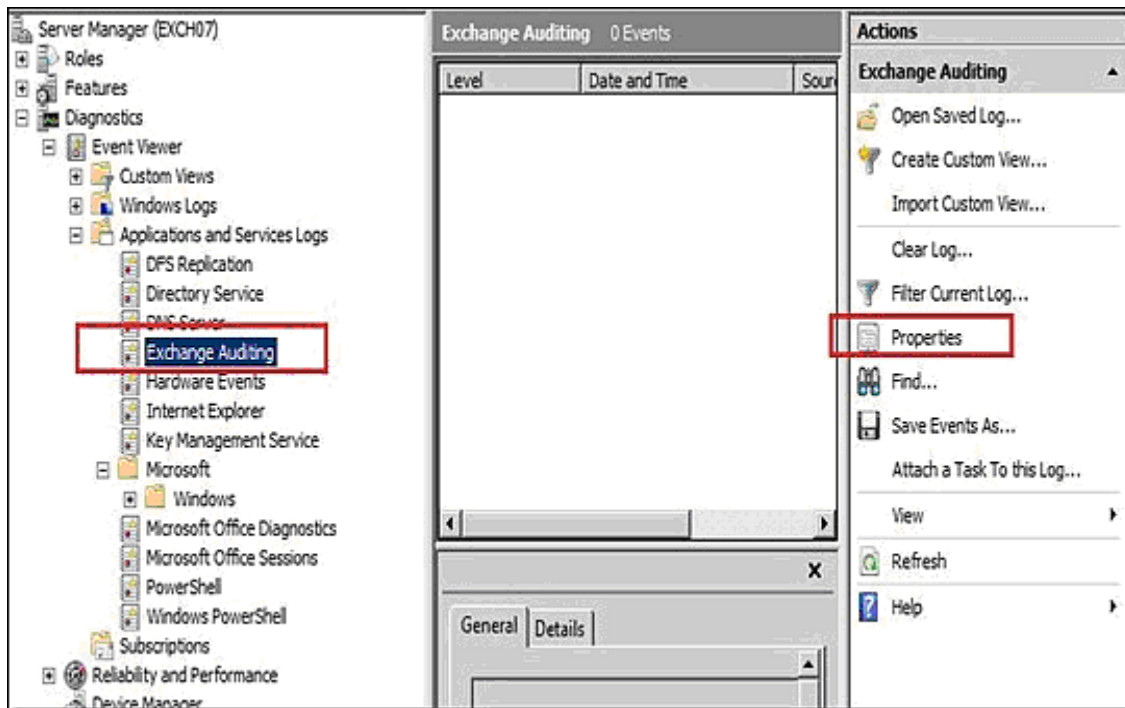
- 2 In this window, expand the **MExchangeIS** category and then expand the **9000 Private** category.
- 3 Under the **MExchangeIS\9000 Private** category, configure auditing for any or all of the four possible actions:
 - ◆ Folder Access, to log events that correspond to opening folders, such as the Inbox, Outbox, or Sent Items folders
 - ◆ Message Access, to log events that correspond to explicitly opening messages
 - ◆ Extended Send As, to log events that correspond to sending a message as a mailbox-enabled user
 - ◆ Extended Send On Behalf Of, to log events that correspond to sending a message on behalf of a mailbox-enabled user.
- 4 When you have finished configuring the auditing levels, click **Configure**.

For more information about Exchange mailbox access auditing, see http://www.msexchange.org/articles_tutorials/exchange-server-2007/compliance-policies-archiving/exchange-2007-mailbox-access-auditing-part1.html

For examples of configuring Exchange mailbox access auditing, see <http://www.howexchangeworks.com/2009/09/mailbox-access-auditing-in-exchange.html>

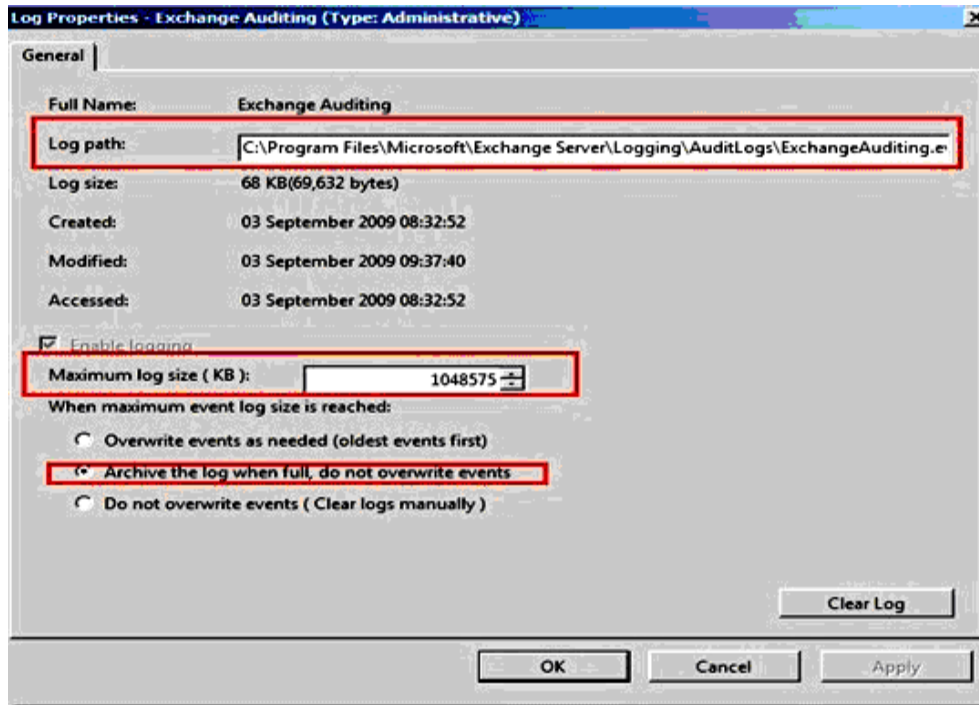
Access the Audited Information

Now that mailbox access auditing is enabled, you can view the information logged by navigating to **Event Viewer -> Applications & Services Log -> Exchange Auditing**.



Change Default Properties

By default, the location for storing the logs is in the Exchange Server installation directory (`Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs`). The default behavior is to archive the logs when it gets full; therefore, the location of the logs should be changed to a drive that has enough free space. You can do this by selecting the properties for the Exchange Auditing log and changing the options.



Exclude Service Accounts

To keep from filling up your mailbox access log with events for service accounts that have full access to the mailboxes, you can run the following command to exclude service accounts from being audited.

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -User
"service account" -ExtendedRights ms-Exch-Store-Bypass-Access-Auditing -
InheritanceType All
```

Connector Installation and Configuration

Follow the installation and configuration procedures in the [SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified](#), selecting **Microsoft Windows Event Log – Unified** as the connector to be configured.

Collect Events from the Event Log

To set up the connector to collect application events:

- 1 From \$ARCSIGHT_HOME\current\bin, double-click **runagentsetup.bat**.
- 2 Select **Modify Connector** on the window displayed and click **Next**.
- 3 Select **Modify connector parameters** and click **Next**.
- 4 Select **Navigate to the Modify table parameters** window.
- 5 To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **Exchange Auditing** in the **Custom Log Names** field.

You can specify multiple Custom Log Names in a comma-separated format; for example:

```
Oracle Audit, Exchange Auditing
```

- 6 Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
- 7 Select **Exit** and click **Next** to exit the configuration wizard.
- 8 Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified*.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Exchange Event 10100 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name depending upon event
File Path	Folder path (when relevant)
Name	A folder in mailbox was opened by user.
Source Host Name	Machine Name
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address

Exchange Event 10102 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name, depending upon event
File Path	Folder path (when relevant)
Name	A message in mailbox was opened by user.
Source Host Name	Machine Name

ArcSight ESM Field	Device-Specific Field
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address

Exchange Event 10104 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name, depending upon event
Name	User sent a message on behalf of another user.
Source Host Name	Machine Name
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address
Target User ID	full ID of user being impersonated

Exchange Event 10106 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name, depending upon event
Name	User sent a message as another user.
Source Host Name	Machine Name
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address
Target User ID	full ID of user being impersonated