



Micro Focus Security ArcSight Connectors

SmartConnector for McAfee ePolicy Orchestrator DB

Configuration Guide

May 17, 2019

Configuration Guide

SmartConnector for McAfee ePolicy Orchestrator DB

May 17, 2019

Copyright © 2004 – 2019 Micro Focus and its affiliates and licensors.

Warranty

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

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
05/17/2019	Updated event mappings for Endpoint Security (ENS) Events with ePO 5.3/5.9 and VirusScan Enterprise 8.8 Events with ePO 5.1/5.3/5.9 sections. Added support for McAfee Application and Change Control (SolidCore) 6.2 with ePO 5.3.
02/19/2019	Updated Endpoint Security (ENS) Events with ePO 5.3/5.9 session event mappings. Added support for Microsoft SQL Server 2016 with ePO 5.9.
11/19/2018	Added McAfee Data Loss Prevention 11.0 support for McAfee ePolicy Orchestrator (ePO) DB 5.9
05/16/2018	Added support for DLP Incident 10000 Removable Storage Protection Events with ePO 5.3. Updated support for DLP Administrative Events with ePO 5.3. Updated support for DLP Discover Events with ePO 5.3. Updated support for DLP Incident Events with ePO 5.3. Updated support for DLP DLP Incident 40102 Removable Storage Protection Events with ePO 5.3.
03/21/2018	Added support for McAfee MOVE AV Agentless 4.5.1 with ePO 5.9. Added support for McAfee Application and Change Control 8.0 with ePO 5.9. Added support Data Exchange Layer module version 4.0 for McAfee ePolicy Orchestrator DB version 5.9. Added Support Policy Auditor module version 6.2.2/6.3 for McAfee Policy Orchestrator DB version 5.9 Added support RSD module version 5.0.5 for McAfee ePolicy Orchestrator DB version 5.9 Added support for SiteAdvisor Enterprise (SAE) 3.5.5 with ePO 5.9 Added support for McAfee Drive Encryption 7.2.3 with ePO 5.9 Added support for MSME 8.5 with ePO 5.9 Added support McAfee Threat Intelligence Exchange module version 2.1 with ePO 5.3.
12/19/2017	Added support for McAfee Host Intrusion Prevention System (HIPS) 8.0 with ePO 5.9.
11/15/2017	Added support for VSE 8.8 and ENS 10.5 with ePO 5.9.

Date	Description
10/20/2017	Added Source Process Name and Old File Path mappings to Endpoint Security mappings table.
10/17/2017	Removed hdlp event type. Added encryption parameters to Global Parameters.
09/15/2017	Added support for RSD v5.0. Removed support for HDLP events with ePO 5.1. Updated DLP events with ePO 5.3 mappings.
08/15/2017	Added support for the Data Exchange Layer (DXL) component.
07/15/2017	Updated JDBC download information. Added support for Orion Audit Log 5.1, and Policy Auditor 6.2 with ePO 5.3.
06/15/2017	Added support for McAfee Data Loss Prevention (DLP) 10.0 with ePO 5.3.
05/15/2017	Added support for McAfee Endpoint Security (ENS) 10.5 with ePO 5.3.
02/15/2017	Added support for McAfee Drive Encryption 7.1 SP3 with ePO 5.3.
11/30/2016	Added support for Application and Change Control 7.0 with ePO 5.3.
09/30/2016	Added support for MOVE AV Agentless 3.6 for ePO 5.3.
08/30/2016	Added support for MSME 8.5 with ePO 5.3.
06/30/2016	Added support for SiteAdvisor Enterprise (SAE) 3.5 with ePO 5.3.

SmartConnector for McAfee ePolicy Orchestrator DB

This guide provides information for installing the SmartConnector for McAfee ePolicy Orchestrator DB and configuring the database for event collection. Microsoft SQL Server versions 2008, 2012, 2014 and 2016 are supported. See "McAfee ePO Products and Versions Supported" for specific support.

Product Overview

The ePolicy Orchestrator software provides a scalable tool for centralized anti-virus and security policy management and enforcement. It includes an ePolicy Orchestrator console, ePolicy Orchestrator agent, and ePolicy Orchestrator server.

The ePolicy Orchestrator agent is installed on target client computers and servers where it gathers and reports data, installs products, enforces policies and tasks, and sends events back to the ePolicy Orchestrator server. (McAfee VirusScan and McAfee Desktop Firewall are examples of ePolicy Orchestrator agents.) The ePolicy Orchestrator server acts as a repository for all data collected from distributed agents.

The ePolicy Orchestrator console lets you manage your entire company's anti-virus and security protection and view client computer properties.

McAfee ePO Products and Versions Supported

Event collection for the following McAfee ePolicy Orchestrator products and versions are supported:

ePO 5.9

- McAfee Data Loss Prevention 11.0
- McAfee Security for Microsoft Exchange (MSME) 8.5
- McAfee Drive Encryption 7.2.3
- McAfee SiteAdvisor Enterprise (SAE) 3.5.5
- McAfee Rogue System Detection (RSD) 5.0
- McAfee Policy Auditor 6.2.2/6.3
- McAfee Data Exchange Layer (DXL) 4.0
- McAfee Application and Change Control 8.0
- McAfee Management for Optimized Virtual Environments (MOVE) 4.5.1

- McAfee Endpoint Security (ENS) 10.5, including Common, Firewall, Threat Prevention, Web Control, Migration Assistant, and Adaptive Threat Protection events
- McAfee VirusScan Enterprise (VSE) 8.8
- McAfee Host Intrusion Prevention System (HIPS) 8.0

ePO 5.3

- McAfee Threat Intelligence Exchange 2.1
- McAfee Application and Change Control 7.0
- McAfee Data Loss Prevention (DLP) 10.0
- McAfee Data Exchange Layer (DXL) 3.0.1
- McAfee Drive Encryption 7.1 SP3
- McAfee Endpoint Security (ENS) 10.5, including Common, Firewall, Threat Prevention, Web Control, Migration Assistant, and Adaptive Threat Protection events
- McAfee Host Intrusion Prevention System (HIPS) 8.0
- McAfee Management for Optimized Virtual Environments (MOVE) 3.6
- McAfee Orion Audit Log 5.1
- McAfee Policy Auditor 6.2
- McAfee Security for Microsoft Exchange (MSME) 8.5
- McAfee Rogue System Detection (RSD) 5.0
- McAfee SiteAdvisor Enterprise (SAE) 3.5
- McAfee VirusScan Enterprise (VSE) 8.8

ePO 5.1

- McAfee Application and Change Control 6.1
- McAfee Host Intrusion Prevention System (HIPS) 8.0
- McAfee Management for Optimized Virtual Environments (MOVE) 3.0
- McAfee Orion Audit Log 5.1
- McAfee Policy Auditor 6.2
- McAfee Rogue System Detection (RSD) 4.7

- McAfee Security for Microsoft Exchange (MSME) 8.0
- McAfee SiteAdvisor Enterprise (SAE) 3.5
- McAfee VirusScan Enterprise (VSE) 8.8

Event Types

The field **Event Types** is used during SmartConnector installation to select the event types the connector is to process. For example, if you want the connector to process ePO VirusScan events, enter 'virusscan' in the Event Type field.

Use this parameter:	For this type of event:
dlp	Data Loss Prevention
dlpadministrative	Data Loss Prevention Administrative
dlpdiscover	Data Loss Prevention Discover
dlpincident	Data Loss Prevention Incident
driveencryption	Drive Encryption
dxl	Data Exchange Layer
endpointsecurity	Endpoint Security (ENS)
hips	Host Intrusion Prevention System (HIPS); DesktopFirewall
move	Management for Optimized Virtual Environments
msme	Microsoft Security for Microsoft Exchange
orionaudit	Orion Audit Log
policyauditorfile	Policy Auditor
policyauditorrule	Policy Auditor
rsd	Rogue System Detection
siteadvisor	SiteAdvisor Enterprise
solidcore	Application and Change Control
tie_server	Threat Intelligence Exchange Server
tie_vse	Threat Intelligence Exchange module for VSE
virusscan	VirusScan Enterprise

You can enter a single parameter or a combined list separated by commas.

Configuration

For information about configuring your ePO agents for event collection, see the appropriate McAfee product documentation.

Control the Level of Logging in Debug Logs

The following DWORD registry value controls logging:

```
HEKY_LOCAL_MACHINES\SOFTWARE\NETWORK ASSOCIATES\EPOLICY
ORCHESTRATOR\LOGLEVEL
```

The LOGLEVEL values are the numbers 1 through 8.

- The larger the number, the more messages are logged. For example, level 5 logs the first five levels (message) types e, w, i, x, and E).
- If there is no LOGLEVEL, the default is 7.
- Log level 7 (message types e, w, i, x, E, W, and I) is a good value for normal debugging.
- Log level 8 (message types e, w, i, x, E, W, I, and X) produces extensive output, including every SQL query, whether or not there is an error. Log level 8 also provides all communication details needed to troubleshoot issues related to the network and proxy servers.

Control the Maximum Size of the Debug Logs

The following DWORD registry value controls log size:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY
ORCHESTRATOR\LOGSIZE
```

The value is the size of the log file in megabytes; for example, 1 = 1 MB, 2 = 2 MB, and so on. The default size is 1 MB.

When most log files reach their maximum size, they are renamed to `<LOG NAME>_BACKUP.LOG` and a new log file is created. If a backup copy of a log file already exists, it is overwritten. Be sure to check both logs; if the log file was recently renamed, it might not contain many messages.

Confirm SQL User Minimum Privileges

Confirm with the ePO database administrator that the SQL user authenticating to the database has been granted the following:

- Explicitly assigned permissions for CONNECT
- Explicitly assigned permissions for SELECT
- Public role
- db_datareader role

Download and Install a JDBC Driver

During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you download to a SmartConnector folder. For information about and to download the MS SQL Server JDBC Driver, see:

<http://msdn.microsoft.com/en-us/sqlserver/aa937724>



Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

When you download the JDBC driver, the version of the jar file depends on the version of the JRE the connector uses:

- Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Prior versions, which run JRE 1.6, require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

Install the driver.

For software connectors, copy the jar file appropriate for your SQL Server version from the installation folder for the SQL Server JDBC driver to a temporary location; you will copy this file to `$ARCSIGHT_HOME/current/user/agent/lib`, (where `$ARCSIGHT_HOME` refers to the SmartConnector installation folder, such as `c:\ArcSight\SmartConnectors`) after the core SmartConnector software has been installed at step 3 of Install the SmartConnector. Copy only the jar file associated with the version of the driver to be installed to this location.

Add a JDBC Driver to the Connector Appliance/ArcSight Management Center


After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as described in this section.

- 1 From the Connector Appliance/ArcSight Management Center, select **Setup -> Repositories**.
- 2 Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
- 3 Click **Upload to Repository**.
- 4 From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
- 5 Retain the default selection and click **Next**.
- 6 Click **Upload** and locate and select the `.jar` file you downloaded in step 3 of SmartConnector Installation.
- 7 Click **Submit** to add the specified file to the repository and click **Next** to continue.
- 8 After adding all files you require, click **Next**.

- 9 In the **Name** field, enter a descriptive name for the zip file (`JDBCdriver`, for example). Click **Next**.
- 10 Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
- 11 To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
- 12 Select the container or containers into which the driver is to be uploaded; click **Next**.
- 13 Click **Done** to complete the process.
- 14 Add the connector through the Connector Appliance/ArcSight Management Center interface; see the *Connector Appliance/ArcSight Management Center Online Help* for detailed information. Descriptions of parameters to be entered during connector configuration are provided in the "Install the SmartConnector" section of this guide.


Configure the JDBC Driver and Windows Authentication

This section provides guidance on how to use a JDBC driver with SmartConnectors that connect to Microsoft SQL Servers using Windows Authentication only. As previously described, download the SQL JDBC drivers from Microsoft and install the driver before beginning this procedure.

 The JDBC driver does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

Microsoft Type 4 JDBC drivers (versions 4.0 or later) support integrated authentication. Windows Authentication works only when using one of these drivers. You also will need to add `;integratedSecurity=true` to the JDBC URL entry for the connection to your database.

- 1 Copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory. For example, the JDBC driver download path for SQL JDBC driver version 4.0 for 32-bit environment would be `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll` and, for 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`.

 When upgrading a connector, the `$ARCSIGHT_HOME\jre\bin` directory is overwritten; therefore, you will need to copy the authentication file to this folder again after update.

- 2 Go to `$ARCSIGHT_HOME\current\bin` and double-click `runagentsetup` to continue the SmartConnector installation.

- 3 When entering the connector parameters, in the **JDBC Database URL** field, append `;integratedSecurity=true` to the end of the URL string.

The following is an example; note that the name or instance of the database configured at installation/audit time should be used.

```
jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;i  
ntegratedSecurity=true
```

- 4 Complete the remaining connector wizard configuration steps.
- 5 After completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should login to the database. The Connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Install the SmartConnector

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

ArcSight recommends you do not install database connectors on the database server or any mission critical servers as this could cause performance issues.

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

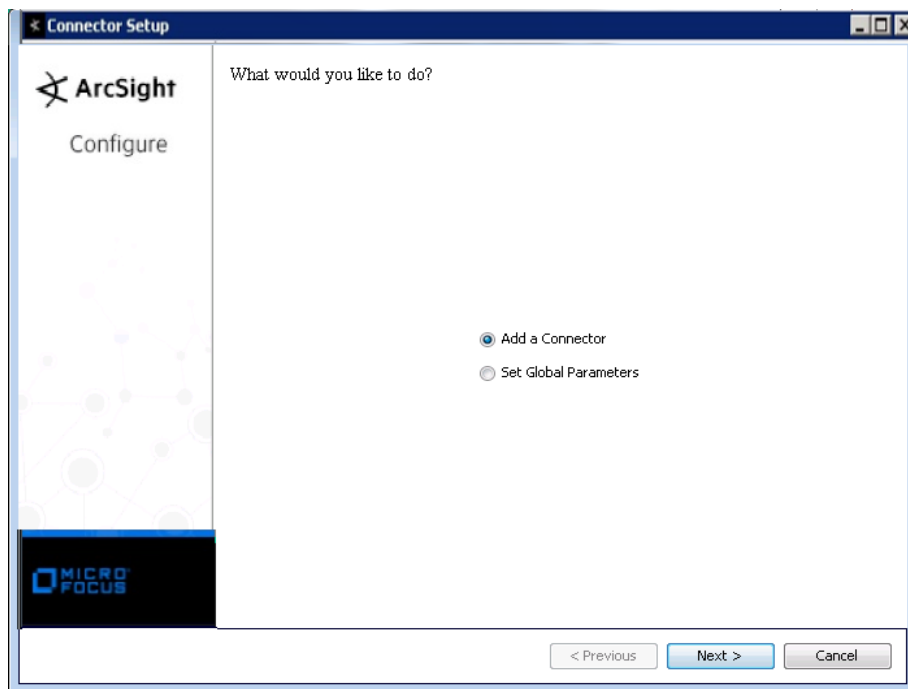
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus 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:



Download SQL Server JDBC Driver

To download a Microsoft SQL Server JDBC driver, click **Cancel** to leave the configuration wizard at this point and copy the jar file you downloaded earlier (see "Download and Install a JDBC Driver") to `$ARCSIGHT_HOME/current/user/agent/lib`.

From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

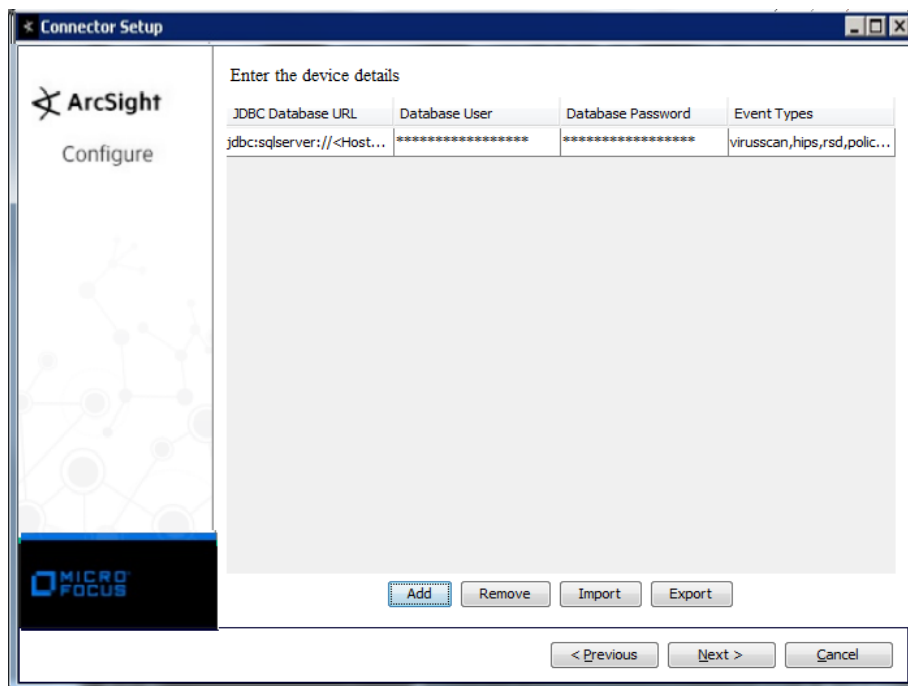
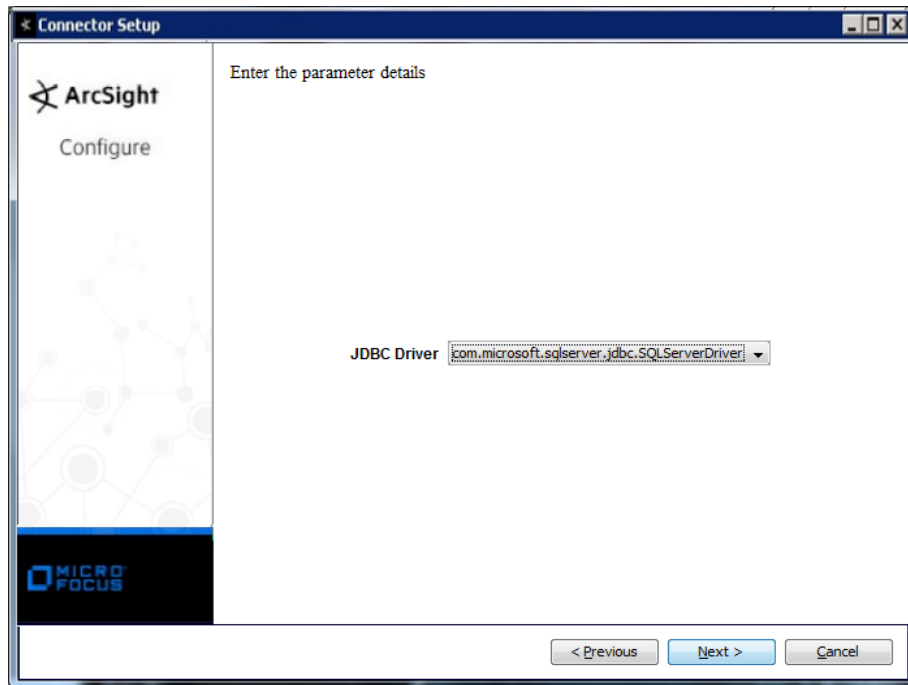
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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 **McAfee ePolicy Orchestrator DB** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



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.

Parameter	Description
Database JDBC Driver	On the first parameter entry screen, select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver (shown in screen shot). Restart the connector setup after installing the JDBC driver. For more information, see "Download and Install a JDBC Driver" and "Add a JDBC Driver to the Connector Appliance/ArcSight Management Center".
URL	Click 'Add' on the next parameter entry screen to have the wizard display a table row with default values already entered. The following default value is shown for the JDBC driver: 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>;1433;DatabaseName=<MS SQL Server Database Name>'. Substitute actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>. If you are configuring additional databases, click 'Add' each time you want to enter a new row for each new database or instance. Change the URL for the database driver and the other values as appropriate.
User	Enter the login name of the database user with appropriate privilege.
Password	Enter the password assigned to the Database User.
Event Types	This field is used to select the event types to be processed. Enter an individual type or a comma-separated list. Remove any uninstalled components from the default list for this parameter as needed. See "Event Types" earlier in this guide for a list of event types.

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*.



When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

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.

Application and Change Control 7.0/8.0 Mappings with ePO 5.3/5.9

ArcSight ESM Field	Device-Specific Field
Additional data	evt_error

ArcSight ESM Field	Device-Specific Field
Additional data	evt_file_sha1
Additional data	evt_process_md5
Additional data	evt_process_sha1
Agent (Connector) Severity	0, 1, 2 = High; 3, 4 = Medium; 5, 6, 7 = Low
Destination Address	targetipv4
Destination Host Name	host_name
Destination Mac Address	targetmac
Destination Port	targetport
Destination Process Name	evt_prog_name
Device Action	threatactiontaken
Device Custom Date 1	detectedutc (Detect Time)
Device Custom Number 1	tenantid (Tenant ID)
Device Custom Number 2	managedstate (Managed State)
Device Custom Number 3	evt_reputation_score (Reputation Score)
Device Custom String 1	analyzeripv6 (Device IPv6 Address)
Device Custom String 2	sourceipv6 (Source IPv6 Address)
Device Custom String 3	productid (Detecting Product ID)
Device Custom String 4	agentguid (Agent GUID)
Device Custom String 5	targetipv6 (Destination IPv6 Address)
Device Event Category	threatcategory
Device Event Class ID	threateventid
Device Host Name	analyzerhostname
Device Mac Address	analyzermac
Device Product	'SolidCore'
Device Receipt Time	receivedutc
Device Severity	threatseverity
Device Vendor	'McAfee'
Device Version	Both ('solidcore', productversion)
External ID	autoid
File Hash	evt_file_md5
File Name	evt_file_name
File Path	evt_object
Message	evt_display_key
Name	evt_display_key
Reason	evt_deny_reason
Request URL	sourceurl
Source Address	sourceipv4
Source Host Name	sourcehostname
Source Mac Address	sourcemac
Source Process Name	sourceprocessname
Source User Name	evt_user_name
Transport Protocol	targetprotocol

Application and Change Control 6.1/6.2 Mappings with ePO 5.1/5.3

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 0, 1, 2; Medium = 3, 4; Low = 5, 6, 7
Destination Address	targetipv4
Destination Host Name	host_name
Destination MAC Address	targetmac
Destination Port	targetport
Destination Process Name	evt_prog_name
Device Action	threatactiontaken
Device Custom Date 1	detectedutc (Detect Time)
Device Custom IPv6 Address 1	analyzeripv6 (Device IPv6 Address)
Device Custom IPv6 Address 2	sourceipv6 (Source IPv6 Address)
Device Custom IPv6 Address 3	targetipv6 (Destination IPv6 Address)
Device Custom Number 1	tenantid
Device Custom Number 2	managedstate
Device Custom String 3	productid (Detecting Product ID)
Device Custom String 4	agentguid
Device Event Category	threatcategory
Device Event Class ID	threateventid
Device Host Name	analyzerhostname
Device MAC Address	analyzermac
Device Product	'SolidCore'
Device Receipt Time	receivedutc
Device Severity	threatseverity
Device Vendor	'McAfee'
Device Version	All of ('solidcore', productversion, '/epo5.1' or All of ('solidcore', productversion, '/epo5.3')
External ID	autoid
File Name	evt_file_name
File Path	evt_object
Name	evt_display_key
Reason	evt_error
Request URL	sourceurl
Source Address	sourceipv4
Source Host Name	sourcehostname
Source MAC Address	sourcemac
Source Process Name	sourceprocessname
Source User Name	evt_user_name
Transport Protocol	targetprotocol

Data Loss Prevention (DLP) Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	2, 1, 0 = High; 4, 3 = Medium; 5, 6, 7 = Low

ArcSight ESM Field	Device-Specific Field
Destination Address	targetipaddress
Destination Host Name	targethostname
Destination Mac Address	targetmac
Destination Port	targetport
Destination Process Name	targetprocessname
Destination User Name	targetusername
Device Action	threataction
Device Custom Date 1	detecttime
Device Custom IPv6 Address 2	sourceIPv6
Device Custom IPv6 Address 3	targetIPv6
Device Custom String 1	threatname
Device Custom String 2	sourceIPv6
Device Custom String 3	targetIPv6
Device Custom String 4	detectingproductid
Device Custom String 5	agentguid
Device Event Class ID	threateventid
Device Host Name	producthostname
Device Mac Address	productmac
Device Product	'ePolicy Orchestrator'
Device Receipt Time	receivedtime
Device Severity	threatseverity
Device Vendor	'McAfee'
Device Version	Both ('dlp', productversion)
External ID	autoid
File Path	One of (sourceurl, targetfilename)
Message	All of ('Threat:', one of (threatname, threattype))
Name	All of ('Threat:', one of (threatname, threattype))
Request URL	sourceurl
Source Address	sourceaddress
Source Host Name	sourcehostname
Source Mac Address	sourcemac
Source Process Name	sourceprocessname
Source User Name	sourceusername
Transport Protocol	targetprotocol

DLP Administrative Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical, Major = High; Minor, Warning = Medium; Info = Low
Device Custom Date 1	UTCTime (Local Time)
Device Custom String 1	PolicyName
Device Custom String 3	PolicyRevision
Device Custom String 5	PolicyUid

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	UserGroups
Device Product	'Data Loss Prevention'
Device Receipt Time	EndpointTime
Device Severity	Severity (0=Info, 1=Warning, 2=Minor, 3=Major, 4=Critical)
Device Vendor	'McAfee'
Device Version	Both ('dlp', AgentVersion)
End Time	InsertionTime
External ID	EventType
Source Address	IP
Source FQDN	FQDN
Source Host Name	Name
Source NT Domain	Username_NTLM
Source User ID	One of (SID, UID)
Source User Name	Username_NTLM

DLP Administrative 402 Evidence Replication Failed Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Reason	ReplicationFailedError

DLP Administrative 405 Release Code Locked Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	ReleaseCodeAttempts
Device Custom Number 3	ReleaseCodeDuration

DLP Discover Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical, Major = High; Minor, Warning = Medium; Info = Low
Bytes In	TotalContentSize
Device Action	ActualAction (0=No action, 1=Block)
Device Custom Date 1	ViolationUTCTime (Violation Time)
Device Custom Number 1	EvidenceCount
Device Custom String 1	RulesToDisplay
Device Custom String 3	PolicyRevision
Device Custom String 4	FileName
Device Product	'Data Loss Prevention'
Device Receipt Time	ViolationLocalTime
Device Severity	Severity (0=Info, 1=Warning, 2=Minor, 3=Major, 4=Critical)
Device Vendor	'McAfee'
Device Version	Both ('dlp', DlpAgentVersion)

ArcSight ESM Field	Device-Specific Field
End Time	InsertionTime
External ID	IncidentType
File Name	FileName
File Path	FilePath
File Size	FileSize
File Type	FileType
Reason	FailureReason
Source Address	IP
Source FQDN	FQDN
Source Host Name	Name
Source NT Domain	Username_NTLM
Source User ID	One of (SID, UID)
Source User Name	Username_NTLM

DLP Incident Events with ePO 5.3

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical, Major = High; Minor, Warning = Medium; Info = Low
Bytes In	TotalContentSize
Destination Process Name	destination
Device Action	ActualAction (0=No action, 1=Block)
Device Custom Date 1	ViolationUTCTime (Violation Time)
Device Custom Number 1	EvidenceCount
Device Custom String 1	RulesToDisplay (Rule Name)
Device Custom String 3	PolicyRevision
Device Custom String 4	FileName (Evidence Value)
Device Product	'Data Loss Prevention'
Device Receipt Time	ViolationLocalTime
Device Severity	Severity (0=Info, 1=Warning, 2=Minor, 3=Major, 4=Critical)
Device Vendor	'McAfee'
Device Version	Both ('dlp', DlpAgentVersion)
End Time	InsertionTime
External ID	IncidentType
File Name	FileName
File Path	FilePath
File Size	FileSize
File Type	FileType
Reason	FailureReason
Source Address	IP
Source FQDN	FQDN
Source Host Name	Name
Source NT Domain	Username_NTLM
Source Process Name	ApplicationFileName

ArcSight ESM Field	Device-Specific Field
Source User ID	One of (SID, UID)
Source User Name	Username_NTLM

DLP Incident Events with ePO 5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical, Major = High; Minor, Warning = Medium; Info = Low
Bytes In	TotalContentSize
Destination Process Name	destination
Destination User Id	DestinationUserID
Device Action	ActualAction (0=No action, 1=Block)
Device Custom Date 1	ViolationUTCTime (Violation Time)
Device Custom Number 1	EvidenceCount
Device Custom String 1	RulesToDisplay (Rule Name)
Device Custom String 3	PolicyRevision
Device Custom String 4	FileName (Evidence Value)
Device Product	'Data Loss Prevention'
Device Receipt Time	ViolationLocalTime
Device Severity	Severity (0=Info, 1=Warning, 2=Minor, 3=Major, 4=Critical)
Device Vendor	'McAfee'
Device Version	Both ('dlp', DlpAgentVersion)
End Time	InsertionTime
External ID	IncidentType
File Name	FileName
File Path	FilePath
File Permission	Copy Direction
File Size	FileSize
File Type	FileType
Reason	FailureReason
Source Address	IP
Source FQDN	FQDN
Source Host Name	Name
Source NT Domain	Username_NTLM
Source Process Name	ApplicationFileName
Source User ID	One of (SID, UID)
Source User Name	Username_NTLM

DLP Incident 10000 Removable Storage Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Device Custom Date2	PluginLocalTime
Device Custom Number2	FileSystemAccess
Device Custom Number3	DeviceFileSystemType

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	Both ('DeviceName:', DeviceName, 'DeviceDescription:', DeviceDescription, 'USBVendorId:', USBVendorId, 'USBProductId:', USBProductId, 'USBSerialNumber:', USBSerialNumber)
Device Custom String6	VolumeSerialNumber
File Id	Both('Device Class GUID:',DeviceClassGUID)
Old File Id	Both('DeviceInstanceId:',DeviceInstanceId)
Old File Name	Both('VolumeLabel:',VolumeLabel)
Old File Path	Both('Unplugged Time:',UnpluggedLocalTime)
Old File Permission	Both('Device Compatible ID:',DeviceCompatibleID)
Old File Type	Both('Bus Type:',BusType)

DLP Incident 40101 Network File System Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	DestinationPath

DLP Incident 40102 Removable Storage Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Device Custom Date 2	PluginLocalTime
Device Custom Number 3	DeviceFileSystemType
Device Custom String 2	SourcePath
Device Custom String 4	Both ('DeviceName:', DeviceName, 'DeviceDescription:', DeviceDescription, 'USBVendorId:', USBVendorId, 'USBProductId:', USBProductId, 'USBSerialNumber:', USBSerialNumber)
Device Custom String 5	DestPath
Device Custom String 6	VolumeSerialNumber
File Id	Both('Device Class GUID:',DeviceClassGUID)
Old File Id	Both('DeviceInstanceId:',DeviceInstanceId)
Old File Name	Both('VolumeLabel:',VolumeLabel)
Old File Path	Both('Unplugged Time:',UnpluggedLocalTime)
Old File Permission	Both('Device Compatible ID:',DeviceCompatibleID)
Old File Type	Both('Bus Type:',BusType)

DLP Incident 40200 Email Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Sender
Device Custom String 5	All of ('Recipients:', Recipients, 'Recipients Cc:', RecipientsCc, 'Recipients Bcc:', RecipientsBcc)
Device Custom String 6	Subject

DLP Incident 40301 Printing Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	PrinterName

DLP Incident 40400 Network Protection Events with ePO 5.3

ArcSight ESM Field	Device-Specific Field
Destination Address	DestIP
Destination Port	DestPort
Device Direction	ConnectionDirection (0=Inbound, 1=Outbound)
Source Port	SourcePort

DLP Incident 40400 Network Protection Events with ePO 5.9

ArcSight ESM Field	Device-Specific Field
Destination Address	DestIP
Destination Port	DestPort
Device Custom String 2	NetworkTransport
Device Direction	ConnectionDirection (0=Inbound, 1=Outbound)
Source Port	SourcePort
Transport Protocol	NetworkProtocol

DLP Incident 40500 Web Post Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Request URL	DestinationURL

DLP Incident 40601 Application File Access Protection Events with 3PO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Source Process ID	ProcessId

DLP Incident 40603 Screen Capture Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	VisibleApplications

DLP Incident 40700 Cloud Protection Events with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Destination Service Name	CloudService

Drive Encryption 7.1 SP3 and 7.2.3 Mappings with ePO 5.3/5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	4 = Very High; 3 = High; 1, 2 = Medium; 0 = Low
Destination Host Name	HostName
Destination User Name	UserName
Device Action	Type
Device Custom Date 1	Generated Time (Detected Time)
Device Custom IPv6 Address 3	IPv6 (Destination IPv6 Address)
Device Custom Number 1	ManagedState (Managed State)
Device Custom Number 2	Error (Error Code)
Device Custom String 3	SiteName (Site Name)
Device Custom String 4	ProductCode (Product Code)
Device Custom String 5	AgentGUID (Agent GUID)
Device Event Class ID	Both (EventID, Severity)
Device Product	'Drive Encryption'
Device Receipt Time	ReceivedTime
Device Severity	Severity
Device Vendor	'McAfee'
Device Version	One of (Version, both ('Drive Encryption', Version))
External ID	AutoID
Message	Description
Name	Name

Data Exchange Layer Mappings with ePO 5.3 to Data Exchange Layer Mappings with ePO 5.3/ePO 5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	4 = Very High; 3 = High; 1, 2 = Medium; 0 = Low
Destination Host Name	HostName
Destination User Name	UserName
Device Action	Type
Device Custom Date 1	Generated Time (Detected Time)
Device Custom IPv6 Address 3	IPv6 (Destination IPv6 Address)
Device Custom Number 1	ManagedState (Managed State)
Device Custom Number 2	TenantId (Tenant Id)
Device Custom String 1	FamilyDispName (Product Family)
Device Custom String 2	Tags (Tags)
Device Custom String 3	AgentPlatform (Agent Platform)
Device Custom String 5	AgentGUID (Agent GUID)
Device Custom String 6	AgentVersion (Agent Version)
Device Event Class ID	EventID
Device Facility	SiteName
Device Product	'Data Exchange Layer'
Device Receipt Time	ReceivedTime
Device Severity	Severity

ArcSight ESM Field	Device-Specific Field
Device Vendor	'McAfee'
Device Version	One of (both ('Data Exchange Layer', Version), Unknown)
External ID	AutoID
Message	Description
Name	Name
Reason	Error

Endpoint Security (ENS) Events with ePO 5.3/5.9

ArcSight ESM Field	Device-Specific Field
device Custom Date2	SourceAccessTime
Agent (Connector) Severity	2, 1, 0 = High; 4, 3 = Medium; 5, 6, 7 = Low
Destination Address	IPv4
Destination Host Name	HostName
Destination MAC Address	MAC
Destination Port	PortNumber
Destination Process Name	DestProcessName
Destination User Name	UserName
Device Action	ThreatAction
Device Custom Date 1	GeneratedTime (Generated Time)
Device Custom Date 2	SourceAccessTime
device Custom Date2 Label	"Source Access Time"
Device Custom IPv6 Address 2	ThreatSourceIPv6 (Source IPv6 Address)
Device Custom IPv6 Address 3	IPv6 (Destination IPv6 Address)
Device Custom Number 1	AttackVectorType
Device Custom Number 1 Label	"Attack Vector Type"
Device Custom Number 2	FirstActionStatus
Device Custom Number 2 Label	"First Action Status"
Device Custom Number 3	SecondActionStatus
Device Custom Number 3 Label	"Second Action Status"
Device Custom String 1	ThreatName
Device Custom String 2	FamilyName
Device Custom String 3	Name (Event Name)
Device Custom String 4	DetectingProductID
Device Custom String 5	AgentGUID
Device Custom String 6	ThreatType
Device Event Category	ThreatCategory
Device Event Class ID	Both (ThreadEventID, Name)
Device Host Name	DetectingProductHostName
Device MAC Address	DetectingProductMAC
Device Product	'Endpoint Security'
Device Receipt Time	ReceivedTime
Device Severity	ThreatSeverity

ArcSight ESM Field	Device-Specific Field
Device Vendor	'McAfee'
Device Version	Both ('ENS', DetectingProductVersion)
endTime	TargetCreateTime
External ID	ThreatEventID
File Hash	SourceHash
file Modification Time	TargetModifyTime
File Path	One of (ThreatSourceURL, FilePath)
File Permission	SourceParentProcessHash
file Size	TargetFileSize
File Type	Both ('_DB_NAME:', '_DB_NAME')
Message	Description
Name	Name
Old File Create Time	SourceCreateTime
Old File Hash	TargetHash
Old File Id	SourceProcessHash
Old File Modification Time	SourceModifyTime
Old File Path	ThreatSourceFilePath
Old File Size	__ifThenElse(AccessRequested,, "", __concatenate("Access Requested: ", AccessRequested))
request Client Application	concatenate("Target Signed: ", TargetSigned)
request Context	concatenate("Target Signer: ", TargetSigner)
Request Cookies	TargetParentProcessHash
Request URL	ThreatSourceURL
Source Address	ThreatSourceIPv4
Source Host Name	ThreatSourceHostName
Source MAC Address	ThreatSourceMAC
Source Port	SourcePort
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
source User Privileges	concatenate("Source Signed: ", SourceSigned)
startTime	TargetAccessTime
Transport Protocol	NetworkProtocol

HIPS 8.0 Events with ePO 5.9

ArcSight ESM Field	Device-Specific Field
Additional data	DetectingProductIPv6
Agent (Connector) Severity	High = Device Severity 2, 1, 0; Medium = Device Severity 4, 3; Low = Device Severity 5, 6, 7
Destination Address	One of (Local IP Address, IPv4)
Destination Host Name	HostName
Destination Mac Address	MAC
Destination Port	One of (PortNumber, RemotePort)
Destination User Name	UserName

ArcSight ESM Field	Device-Specific Field
Device Action	ThreatAction (Blocked, Permitted, or Block)
Device Custom Date 1	GeneratedTime
Device Custom IPv6 Address 1	LocalIPAddress
Device Custom IPv6 Address 2	ThreatSourceIPv6 (Source IPv6 Address)
Device Custom IPv6 Address 3	IPv6
Device Custom Number 1	Signature
Device Custom Number 2	EventPolicyType
Device Custom String 1	ThreatName
Device Custom String 2	ThreatSourceIPv6
Device Custom String 3	IPv6 (Target IPv6)
Device Custom String 4	DetectingProductID
Device Custom String 5	AgentGUID
Device Custom String 6	AppVersion
Device Direction	Direction
Device Event Category	One of ('ThreatNameSignature', ThreatCategory, ThreatType)
Device Event Class ID	One of (SignatureID, ThreatEventID, both (ThreatCategory, ThreatType))
Device Host Name	DetectingProductHostName
Device MAC Address	DetectingProductMAC
Device Product	DetectingProductName
Device Receipt Time	ReceivedTime
Device Severity	ThreatSeverity (0 – 7)
Device Vendor	'McAfee'
Device Version	All of ('hips', DetectingProductVersion)
External ID	ThreatEventID
File Hash	Both ('AppHash:', AppHash)
File Name	Both ('AppDesc:', AppDesc)
File Path	One of (files, ThreatSourceURL, FilePath)
File Permission	Both ('AppSigner:', AppSigner)
File Type	SigRuleClass
Message	One of (both (ThreatName, 'Blocked'), both ('Threat', ThreatName))
Name	One of (SignatureName, 'Application Blocked', both ('Threat', ThreatName))
Old File ID	Both ('EventID', EventID)
Old File Name	Both ('DestinationFile:', DestinationFile)
Old File Path	Both ('Files:', Files)
Old File Permission	Both ('EventUserName:', EventUserName)
Request URL	ThreatSourceURL
Source Address	ThreatSourceIPv4
Source Host Name	ThreatSourceHostName
Source Mac Address	ThreatSourceMAC
Source Port	LocalPort
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
Transport Protocol	One of (NetworkProtocol, Protocol)

HIPS 8.0 Events with ePO 5.1/5.3

ArcSight ESM Field	Device-Specific Field
Additional data	DetectingProductIPv6
Agent (Connector) Severity	High = Device Severity 2, 1, 0; Medium = Device Severity 4, 3; Low = Device Severity 5, 6, 7
Destination Address	One of (Local IP Address, IPv4)
Destination Host Name	HostName
Destination Mac Address	MAC
Destination Port	One of (PortNumber, RemotePort)
Destination User Name	UserName
Device Action	ThreatAction (Blocked, Permitted, or Block)
Device Custom Date 1	GeneratedTime
Device Custom IPv6 Address 1	LocalIPAddress
Device Custom IPv6 Address 2	ThreatSourceIPv6 (Source IPv6 Address)
Device Custom IPv6 Address 3	IPv6
Device Custom Number 1	Signature
Device Custom Number 2	EventPolicyType
Device Custom String 1	ThreatName
Device Custom String 2	ThreatSourceIPv6
Device Custom String 3	IPv6 (Target IPv6)
Device Custom String 4	DetectingProductID
Device Custom String 5	AgentGUID
Device Custom String 6	AppVersion
Device Direction	Direction
Device Event Category	One of ('ThreatNameSignature', ThreatCategory, ThreatType)
Device Event Class ID	One of (SignatureID, ThreatEventID, both (ThreatCategory, ThreatType))
Device Host Name	DetectingProductHostName
Device MAC Address	DetectingProductMAC
Device Product	DetectingProductName
Device Receipt Time	ReceivedTime
Device Severity	ThreatSeverity (0 – 7)
Device Vendor	'McAfee'
Device Version	All of ('hips', DetectingProductVersion)
External ID	ThreatEventID
File Hash	Both ('AppHash:', AppHash)
File Name	Both ('AppDesc:', AppDesc)
File Path	One of (files, ThreatSourceURL, FilePath)
File Permission	Both ('AppSigner:', AppSigner)
File Type	SigRuleClass
Message	One of (both (ThreatName, 'Blocked'), both ('Threat', ThreatName))
Name	One of (SignatureName, 'Application Blocked', both ('Threat', ThreatName))
Old File ID	Both ('EventID', EventID)

ArcSight ESM Field	Device-Specific Field
Old File Permission	Both ('EventUserName:', EventUserName)
Request URL	ThreatSourceURL
Source Address	ThreatSourceIPv4
Source Host Name	ThreatSourceHostName
Source Mac Address	ThreatSourceMAC
Source Port	LocalPort
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
Transport Protocol	One of (NetworkProtocol, Protocol)

MOVE 3.0/3.6/4.5.1 Mappings with ePO 5.1/5.3/5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Critical; High = High, Major; Medium = Warning, Medium; Low = Informational, Info, Low
Destination Address	IPv4
Destination Host Name	HostName
Destination MAC Address	MAC
Destination Port	PortNumber
Destination Process Name	ProcessName
Destination User Name	UserName
Device Action	ThreatAction
Device Custom Date 1	GeneratedTime (Detected Time)
Device Custom IPv6 Address 1	DetectingProductIPv6 (Device IPv6 Address)
Device Custom IPv6 Address 2	ThreatSourceIPv6 (Source IPv6 Address)
Device Custom IPv6 Address 3	IPv6 (Destination IPv6 Address)
Device Custom Number 2	ManagedState
Device Custom String 1	ThreatName
Device Custom String 4	DetectingProductID
Device Custom String 5	AgentGUID
Device Event Category	ThreatCategory
Device Event Class ID	ThreatEventID
Device Host Name	DetectingProductHostName
Device MAC Address	DetectingProductMAC
Device Product	'MOVE Antivirus'
Device Receipt Time	ReceivedTime
Device Vendor	'McAfee'
Device Version	Both (DetectingProductName, DetectingProductVersion)
External ID	AutoID
File Name	FileName
File Type	ThreatType
Message	ThreatType
Name	Message (dependent on ThreatEventID)

ArcSight ESM Field	Device-Specific Field
Request URL	ThreatSourceURL
Source Address	ThreatSourceIPv4
Source Host Name	ThreatSourceHostName
Source MAC Address	ThreatSourceMAC
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
Transport Protocol	NetworkProtocol

MSME 8.0 and 8.5 with ePO 5.1/5.3/5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 2, 1, 0; Medium = 4, 3; Low = 5, 6, 7
Destination Address	IPV4
Destination Host Name	HostName
Destination Mac Address	MAC
Destination Port	PortNumber
Destination Process Name	ProcessName
Destination User Name	UserName
Device Action	ThreatAction
Device Custom Date 1	GeneratedTime
Device Custom IPv6 Address 1	DetectingProductIPv6 (Device IPv6 Address)
Device Custom IPv6 Address 2	ThreatSourceIPv6 (Source IPv6 Address)
Device Custom IPv6 Address 3	IPv6 (Destination IPv6 Address)
Device Custom Number 2	ManagedState
Device Custom String 1	ThreatName
Device Custom String 4	DetectingProductID (Detecting Product ID)
Device Custom String 5	AgentGUID (Agent GUID)
Device Event Category	ThreatCategory
Device Event Class ID	ThreatEventID
Device Host Name	DetectingProductHostName
Device Mac Address	DetectingProductMAC
Device Product	'MSME'
Device Receipt Time	ReceivedTime
Device Severity	ThreatSeverity
Device Vendor	'McAfee'
Device Version	('msme',' ', DetectingProductVersion)
External ID	AutolD
File Name	FileName
Message	Both ('Threat:', ThreatType)
Name	Both ('Threat:', one of(ThreatName,'On Demand Scan'))
Request URL	ThreatSourceURL
Source Address	ThreatSourceIPv4
Source Host Name	ThreatSourceHostName

ArcSight ESM Field	Device-Specific Field
Source Mac Address	ThreatSourceMAC
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
Transport Protocol	NetworkProtocol

Orion Audit Log 5.1 Mappings with ePO DB 5.1/5.3

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 1, 5; Medium = 2, 6; Low = 3, 4, 7, 8
Destination Address	RemoteAddress
Destination User ID	UserID
Destination User Name	UserName
Device Custom Number 1	TenantId
Device Event Class ID	CmdName
Device Product	'ePolicy Orchestrator'
Device Severity	Priority
Device Vendor	'McAfee'
End Time	EndTime
Event Outcome	One of (Success, '1', 'Success', 'Failed')
External ID	AutolD
Message	Message
Name	CmdName
Start Time	StartTime

Policy Auditor File 6.2 with ePO 5.1/5.3

ArcSight ESM Field	Device-Specific Field
Destination Address	HostIP
Destination Host Name	HostName
Destination Mac Address	MAC
Destination User ID	AcceptedByUserID
Destination User Name	FileOwner
Device Address	HostIP
Device Custom Date 1	AcceptedTime
Device Custom Date 2	BaselineDate
Device Custom Number 1	FVID
Device Custom Number 2	TenantID
Device Custom Number 3	ManagedState
Device Custom String 2	SystemID
Device Custom String 3	UsersSHA1Hash
Device Custom String 4	IsBaseline
Device Custom String 6	FileGroup (Group Name)
Device Domain	Domain

ArcSight ESM Field	Device-Specific Field
Device Event Category	'PAFile'
Device Event Class ID	Type
Device Host Name	HostName
Device Mac Address	MAC
Device Product	'Policy Auditor'
Device Receipt Time	ReportedTime
Device Time Zone	TimeZone
Device Vendor	'McAfee'
Device Version	'Unknown'
File Create Time	CreatedTime
File Hash	One of (SHA2, fileMD5Hash, fileSHA1Hash)
File Modification Time	ModifiedTime
File Name	filePath
File Path	filePath
File Size	Size
File Type	filePath
Name	Type
Reason	ErrorCode

Policy Auditor File 6.2.2/6.3 with ePO 5.9

ArcSight ESM Field	Device-Specific Field
Destination Address	HostIP
Destination Host Name	HostName
Destination Mac Address	MAC
Destination User ID	AcceptedByUserID
Destination User Name	FileOwner
Device Address	HostIP
Device Custom Date 1	AcceptedTime
Device Custom Date 2	BaselineDate
Device Custom Number 1	FVID
Device Custom Number 2	TenantID
Device Custom Number 3	ManagedState
Device Custom String 2	SystemID
Device Custom String 3	UsersSHA1Hash
Device Custom String 4	IsBaseline
Device Custom String 6	FileGroup (Group Name)
Device Domain	Domain
Device Event Category	'PAFile'
Device Event Class ID	Type
Device Host Name	HostName
Device Mac Address	MAC
Device Product	'Policy Auditor'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	ReportedTime
Device Time Zone	TimeZone
Device Vendor	'McAfee'
Device Version	'Unknown'
File Create Time	CreatedTime
File Hash	One of(SHA2, fileMD5Hash, fileSHA1Hash)
File Modification Time	ModifiedTime
File Name	filePath
File Path	filePath
File Size	Size
File Type	filePath
Name	Type
Old File Name	
Reason	ErrorCode

Policy Auditor Rule 6.2 with ePO 5.1/5.3 and Policy Auditor Rule 6.2.2/6.3 with ePO5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical = Very High; Important = High; Moderate = Medium; Low = Low
Destination Address	HostIP
Destination Host Name	SystemName
Destination MAC Address	MAC
Device Address	HostIP
Device Custom Date 1	VendorPublicationDate
Device Custom Number 1	TenantID
Device Custom Number 2	ManagedState
Device Custom String 1	ClassType
Device Custom String 2	CheckID
Device Custom String 3	CheckVersion
Device Custom String 4	RuleID
Device Custom String 5	Both (BenchmarkIDk, BenchmarkVersion)
Device Custom String 6	AuditName
Device Domain	Domain
Device Event Class ID	Both (ClassType, RuleResult)
Device Host Name	HostName
Device MAC Address	MAC
Device Product	'Policy Auditor'
Device Receipt Time	EndTime
Device Severity	VendorSeverity
Device Time Zone	TimeZone
Device Vendor	'McAfee'
Device Version	'Unknown'

ArcSight ESM Field	Device-Specific Field
Event Outcome	RuleResult
Message	CheckDescription
Name	Title

RSD 4.7/5.0 Events with ePO 5.1/5.3/5.9

ArcSight ESM Field	Device-Specific Field
Destination Address	IPv4
Destination DNS Domain	DnsName
Destination Host Name	HostName
Destination Mac Address	MAC
Destination NT Domain	Domain
Device Action	Device Action
Device Custom Date 1	Start Recorded Time
Device Custom Date 2	End Recorded Time
Device Custom IPv6 Address 3	IPv6
Device Custom String 3	IPV6
Device Custom String 4	All of (OS, OSFamily, OSVer)
Device Custom String 6	SourceType
Device Event Class ID	'Detected Rogue System by RSD'
Device Product	'Rogue System Sensor'
Device Receipt Time	Start Time
Device Vendor	'McAfee'
Device Version	'Unknown'
End Time	End Time
Name	'Rogue System'
Start Time	Start Time

SiteAdvisor Enterprise 3.5/3.5.5 Mappings with ePO 5.1/5.3/5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 3; Medium = 2; Low = 1, 4, 5, 6
Destination NT Domain	domainName
Device Action	actionName
Device Custom Number 1	eventCount
Device Custom Number 2	contentId
Device Custom String 2	listType
Device Custom String 3	ratingName
Device Custom String 4	observerMode (0=off, 1=on)
Device Custom String 5	agentGuld
Device Event Class ID	Both (EventTypeId, eventName)
Device Product	'SiteAdvisor Enterprise'
Device Receipt Time	detectedTime

ArcSight ESM Field	Device-Specific Field
Device Severity	ratingId
Device Vendor	'McAfee'
Device Version	'Unknown'
External ID	autold
Message	reasonType
Name	eventName
Request URL	url
Source NT Domain	userId
Source User Id	userId
Source User Name	userName

TIE_SERVER 2.1 Events with ePO 5.3

ArcSight ESM Field	Device-Specific Field
Destination Host Name	HostName
Destination User Name	UserName
Device Action	Type
Device Custom Date 1	GeneratedTime
Device Custom IPv6 Address3	IPV6
Device Custom Number 1	ManagedState
Device Custom Number 2	TenantId
Device Custom String 1	FamilyDispName
Device Custom String 2	ProductFamily
Device Custom String 3	AgentPlatform
Device Custom String 5	AgentGUID
Device Custom String 6	AgentVersion
Device Event Class ID	EventID
Device Facility	SiteName
Device Product	'Threat Intelligence Exchange Server'
Device Receipt Time	ReceivedTime
Device Severity	Severity
Device Vendor	'McAfee'
Device Version	one of (Unknown,both("TIE Server ",Version))
External ID	Autold
Flex String2	tags
Message	Description
Name	Name
Reason	Error

TIE_VSE 1.0 Events with ePO 5.3

ArcSight ESM Field	Device-Specific Field
Destination Address	targetipaddress

ArcSight ESM Field	Device-Specific Field
Destination HostName	targethostname
Destination Mac Address	targetmac
Destination Port	targetport
Destination Process Name	targetprocessname
Destination User Name	targetusername
Device Action	threataction
Device Custom Date 1	detecttime
Device Custom IPv6 Address2	sourceIPv6
Device Custom IPv6 Address3	targetIPv6
Device Custom Number 1	managedstate
Device Custom Number 2	tenantid
Device Custom String 1	threatname
Device Custom String 2	threattype
Device Custom String 4	detectingproductid
Device Custom String 5	agentguid
Device Custom String 6	productname
Device Event Category	threatcategory
Device Event Class ID	threateventid
Device Host Name	producthostname
Device Mac Address	productmac
Device Product	'Threat Intelligence Exchange module for VSE'
Device Receipt Time	receivedtime
Device Severity	threatseverity
Device Vendor	'McAfee'
Device Version	Both("TIE for VSE ",productversion)
External ID	autoid
File Path	One of (sourceurl,targetfilename)
Flex String2	tags
Message	Description
Name	name
Request Url	sourceurl
Source Address	sourceaddress
Source Host Name	sourcehostname
Source Mac Address	sourcemac
Source Process Name	sourceprocessname
Source UserName	sourceusername
Transport Protocol	targetprotocol

VirusScan Enterprise 8.8 Events with ePO 5.1/5.3/5.9

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	5, 6 = Very High; 4 = High; 2, 3 = Medium, 1 = Low
Base Event Count	counter

ArcSight ESM Field	Device-Specific Field
Destination Address	agentipaddress
Destination Host Name	agenthostname
Destination Mac Address	agentmac
Destination NT Domain	agentdomainname
Destination Port	agentport
Destination Process Name	processname
Destination User Name	One of (username, agentusername)
Device Action	ActionName
Device Address	serveripaddress
Device Custom Date 1	detecttime
Device Custom Number 2	datversion
Device Custom String 1	virusname
Device Custom String 2	virustype
Device Custom String 3	All of ('ProductName: ', productname, 'ProductVersion: ', productversion)
Device Custom String 4	scantype (Analyzer Detection Method)
Device Custom String 5	engineversion
Device Custom String 6	datversion
Device Event Category	threatcateg
Device Event Class ID	tvdeventid
Device Host Name	serverhostname
Device Product	'ePolicy Orchestrator'
Device Receipt Time	datetime
Device Severity	eventseverity
Device Time Zone	agenttimezone
Device Vendor	'McAfee'
Device Version	Both ('virusscan', productversion)
Event Name	One of (eventname, virusname, 'ePO AntiVirus Scan Event')
External ID	autoid
File Hash	MD5
File Name	filename
Source Address	sourceaddress
Source HostName	source
Source Mac Address	sourcemac
Source Port	LoadBalancerHttpsPort
Source Process Name	sourceprocessname
Source User Name	sourceusername

Troubleshooting

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection.'"

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The `preservestate` parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting `preservestate` to disabled (false) in the `agent.properties` file allows the connector to skip the old events and start from real time. The `agent.properties` file is located in the `$ARCSIGHT_HOME\current\user\agent` folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the connector uses. Versions 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar. Versions 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.