



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for SmartConnector for McAfee ePolicy Orchestrator DB

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2004 – 2023 Open Text.

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

Trademark Notices

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

Documentation Updates

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

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

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

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

Configuration Guide for McAfee ePolicy Orchestrator DB SmartConnector

This guide provides information for installing the SmartConnector for McAfee ePolicy Orchestrator DB and configuring the database for event collection. See [McAfee ePO Products and Versions Supported](#) for specific support.

This guide provides a high level overview of ArcSight SmartConnectors.

Intended Audience

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

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

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

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

Contact Information

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

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

Product Overview

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 5.10

- Advanced Threat Defense 4.12
- McAfee Security for Microsoft SharePoint (MSMS) 3.5
- McAfee Threat Intelligence Exchange 2.1 VirusScan Enterprise (VSE)
- McAfee Host Intrusion Prevention System (HIPS)
- Data Exchange Layer (DXL)
- Data Loss Prevent (DLP) 11.x
- McAfee Endpoint Security (ENS) 10.6
- McAfee Threat Intelligence Exchange Server 2.1
- Drive Encryption (DE)
- Rogue System Detection (RSD)
- Application and Change Control (SolidCore)
- McAfee Agents (ENS) 5.5
- McAfee SiteAdvisor Enterprise (SAE) 3.5/3.5.5
- McAfee Active Response (MAR) 2.3 and 2.4
- Policy Auditor File (PA File) 6.4

- Policy Auditor Rule (PA Rule) 6.4
- Management for Optimized Virtual Environments (MOVE)

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) 3.5/3.5.5
- 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 10.6 and 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

Configuration

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

Configuring 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.

Configuring 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.

Verifying the SQL User Minimum Privileges

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

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

Downloading the JDBC Driver

The SmartConnector installation requires JDBC driver to be present. During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you downloaded to a SmartConnector folder.



Note: Different versions of the JDBC driver are required for different SQL Server database versions. The name of the jar file may be different for some JDBC driver versions. Make sure that you use the correct driver for your database version

Refer to the following information to download the correct jar file depending on the JRE version used by the SmartConnector:

- SmartConnector Version 8.3.0 uses JRE 1.8.0_312 and supports jar files from version mssql-jdbc-6.4.0.jre8.jar ([Download Microsoft JDBC Driver 6.4 for SQL Server](#)) to mssql-jdbc-9.4.0.jre8.jar ([Download Microsoft JDBC Driver 9.4.0 for SQL Server](#)).

- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server).

For more information related to the Microsoft JDBC driver, see [Microsoft Documentation](#).

Installing the SmartConnector

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

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

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. Exit the installation wizard.

4. Copy the jar file associated with the version of the driver that you downloaded earlier to `$ARCSIGHT_HOME/current/user/agent/lib`
5. To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory.

An example of The JDBC driver download path for SQL JDBC driver is:

- For version 4.0 for 32-bit environment is `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll`
- For 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`


To use the latest version of SQL JDBC Driver such as 9.4:

- Copy the `mssql-jdbc-9.4.0.jre8.jar` file associated with the version of the driver that you downloaded earlier to `$ARCSIGHT_HOME/current/user/agent/lib`
- Copy the `mssql-jdbc_auth-9.4.0.x64.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory.



Note: If you are upgrading the SmartConnector, you must copy the authentication file to `$ARCSIGHT_HOME\jre\bin` again after update, as the upgrade process overwrites the `$ARCSIGHT_HOME\jre\bin` directory.

6. Copy certificate and JDBC files to SmartConnector folders as follows:
 - Copy the `jssecacerts` certificate that you installed during the device configuration to the SmartConnector installation folder `$ARCSIGHT_HOME/current/jre/lib/security`.



Note: You must copy this file again to the installation folder after upgrading the SmartConnector as this file gets overwritten during the upgrade process.

 - Copy the `vjdbc.jar` and `commons-logging-1.1.jar` files to the SmartConnector installation folder `$ARCSIGHT_HOME/current/user/agent/lib`. These files are located in the `lib` directory that was created when you downloaded the JDBC driver and unzipped the package.
7. Browse to `$ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup.bat` file to start the SmartConnector Configuration Wizard.
8. Specify the relevant Global Parameters, when prompted.
9. Select **McAfee ePolicy Orchestrator DB** from the **Type** drop-down, then click **Next**
10. Enter the required following parameters, then click **Next**.

Parameter	Description
Database JDBC Driver	Select the <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> driver.
URL	<p>Enter <code>jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name></code>. Substitute actual values for <i><MS SQL Server Host Name or IP Address></i> and <i><MS SQL Server Database Name></i>.</p> <p>Note: If using Windows authentication append <code>;integratedSecurity=true</code> to the end of the URL string. Make sure that you use the name or instance of the database configured during installation or audit. For example: <code>jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true</code></p>
User	Enter the name of the database user with appropriate privilege.
Password	Enter the password assigned to the Database User.
Event Types	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.

Click **Export** to export the host name data you have entered into a CSV file.

Click **Import** to select and import a CSV file that contains host data for multiple hosts. For more information, see the SmartConnector Installation and User Guide.

11. Select a [destination and configure parameters](#).
12. Specify a name for the connector.
13. (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.



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

14. Select whether you want to install the connector as a service or in the standalone mode.
15. Complete the installation.
16. [Run the SmartConnector](#).

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



Note: 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.

Adding 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 required containers, as follows:

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.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all the files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (for example, JDBCdriver). 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 one or more containers into which you want to upload the driver, then click **Next**.
13. Click **Done** to complete the process.
14. Add the connector through the Connector Appliance/ArcSight Management Center interface. For more information, see the *Connector Appliance/ArcSight Management Center Online Help*.

Event Types

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



Note: You can enter a single parameter or a combined list separated by comma. However, you must not add white spaces in between the parameters.

Parameter:	Used For
atd	Advanced Threat Defense
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

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.

Advanced Threat Defense 7.12 Mappings with ePO 5.10

ArcSight ESM Field	Device-Specific Field
Device Vendor	McAfee
Device Product	Advanced Threat Defense

ArcSight ESM Field	Device-Specific Field
External Id	AutoID
Name	name
Message	Description
Device Receipt Time	ReceivedTime (Received UTC)
Device Mac Address	DetectingProductMAC
Device Host Name	DetectingProductHostName
Device Address	DetectingProductIPv4 (AnalyzerIPV4)
Device Severity	ThreatSeverity
Device Action	ThreatAction
Source Host Name	ThreatSourceHostName (SourceHostName)
Source Address	ThreatSourceIPv4 (SourceIPV4)
Source Mac Address	ThreatSourceMAC (SourceMAC)
Source User Name	ThreatSourceUserName (SourceUserName)
Request Url	ThreatSourceURL (SourceURL)
Source Process Name	ThreatSourceProcessName (SourceProcessName)
Transport Protocol	NetworkProtocol
Destination Host Name	HostName
Destination Address	IPv4
Destination Mac Address	MAC
Destination User Name	UserName
Destination Port	PortNumber
Destination Process Name	ProcessName
Device Custom String 1	ThreatName
Device Custom String 1 Label	"Threat Name"
Device Custom String 2	productFamily
Device Custom String 2 Label	"Product Family"
Device Custom String 4	DetectingProductID
Device Custom String 4 Label	Detecting Product ID
Device Custom String 5	AgentGUID
Device Custom String 5 Label	__stringConstant(Agent GUID)
Device Custom String 6	ThreatType

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	Threat Type
Device Custom Date 1	DetectTime (DetectedUTC)
Device Custom Date1 Label	"Detect Time"
Event Outcome	ThreatHandled
File Hash	MD5
File Size	size
File Create Time	FileUploadTime (Timestamp)
File Path	FilePath

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
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	targetip4
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	analyzerip6 (Device IPv6 Address)
Device Custom String 2	sourceip6 (Source IPv6 Address)
Device Custom String 3	productid (Detecting Product ID)
Device Custom String 4	agentguid (Agent GUID)

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
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	sourcceipv4
Source Host Name	sourcehostname
Source MAC Address	sourcemac

ArcSight ESM Field	Device-Specific Field
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
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)

ArcSight ESM Field	Device-Specific Field
External ID	autoid
File Path	One of (sourceurl, targetfilename)
Message	All of ('Threat:', one of (threatname, threatype))
Name	All of ('Threat:', one of (threatname, threatype))
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
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

ArcSight ESM Field	Device-Specific Field
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 5.10

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical, Major = High; Minor, Warning = Medium; Info = Low
Bytes In	TotalContentSize
Destination NT Domain	UserPrincipalName
Destination User Name	UserAccount
Destination User Privilege	UserGroups
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'

ArcSight ESM Field	Device-Specific Field
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 Hash	SHA1
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 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'

ArcSight ESM Field	Device-Specific Field
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 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'

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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 Events with ePO 5.10

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Critical, Major = High; Minor, Warning = Medium; Info = Low
Bytes In	TotalContentSize
Destination Nt Domain	UserPrincipalName
Destination Process Name	destination
Destination User Id	DestinationUserID
Destination User Name	UserAccount

ArcSight ESM Field	Device-Specific Field
Destination User Privilege	UserGroups
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 Hash	SHA1
File Name	FileName
File Path	FilePath
File Permission	Copy Direction
File Size	FileSize
File Type	FileType
Old File Hash	ActualActionOther
Reason	FailureReason
Request Context	ItemType
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 Date 2	PluginLocalTime
Device Custom Number 2	FileSystemAccess
Device Custom Number 3	DeviceFileSystemType
Device Custom String 4	Both ('DeviceName:', DeviceName, 'DeviceDescription:', DeviceDescription, 'USBVendorId:', USBVendorId, 'USBProductId:', USBProductId, 'USBSerialNumber:', USBSerialNumber)
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 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

ArcSight ESM Field	Device-Specific Field
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
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 5.3/5.9/5.10

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
Flex String 2	Tags
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
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, or 5.10

ArcSight ESM Field	Device-Specific Field
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	TargetAccessTime
Device Custom Date 1 Label	"Target Access Time"
Device Custom Date 2	SourceAccessTime
Device Custom Date 2 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)

ArcSight ESM Field	Device-Specific Field
Device Host Name	DetectingProductHostName
Device MAC Address	DetectingProductMAC
Device Product	'Endpoint Security'
Device Receipt Time	ReceivedTime
Device Severity	ThreatSeverity
Device Vendor	'McAfee'
Device Version	Both ('ENS', DetectingProductVersion)
End Time	Mapped properly by ESM Console
External ID	ThreatEventID
File Create Time	Target Create Time
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

ArcSight ESM Field	Device-Specific Field
Source MAC Address	ThreatSourceMAC
Source Port	SourcePort
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
Source User Privileges	concatenate("Source Signed: ",SourceSigned)
Start Time	GeneratedTime
Transport Protocol	NetworkProtocol

HIPS 8.0 Events with ePO 5.10

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

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	AppVersion
Device Direction	Direction
Device Event Category	One of ('ThreatNameIsSignature', 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 Hash	DetailedEventInfo
Old File ID	Both ('EventID', EventID)
Old File Name	Both ('DestinationFile:', DestinationFile)
Old File Path	Both ('Files:', Files)
Old File Permission	Both ('EventUserName:', EventUserName)
Old File Type	ApiName
Request URL	ThreatSourceURL
Source Address	ThreatSourceIPv4
Source Host Name	ThreatSourceHostName
Source Mac Address	ThreatSourceMAC
Source Port	LocalPort

ArcSight ESM Field	Device-Specific Field
Source Process Name	ThreatSourceProcessName
Source User Name	ThreatSourceUserName
Transport Protocol	One of (NetworkProtocol, Protocol)

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
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 ('ThreatNameIsSignature', ThreatCategory, ThreatType)
Device Event Class ID	One of (SignatureID, ThreatEventID, both (ThreatCategory, ThreatType))

ArcSight ESM Field	Device-Specific Field
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 ('ThreatNameIsSignature', 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)

ArcSight ESM Field	Device-Specific Field
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 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 5.1/5.3/5.9/5.10

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

ArcSight ESM Field	Device-Specific Field
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)
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

Active Response (MAR) with ePO 5.10

ArcSight ESM Field	Device-Specific Field
Analyzer Version	__concatenate("MAR ", Device Version)
Description	__oneOf(Description,Name)
Destination Address	TargetIPV4
Destination Host Name	TargetHostName
Destination Mac Address	TargetMAC
Destination Port	TargetPort
Destination Process Name	TargetProcessName
Destination User Name	TargetUserName
Device Action	ThreatActionTaken
Device Address	AnalyzerIPV4
Device Custom Date 1	DetectedUTC
Device Custom Date 1 Label	"Generated Time"
Device Custom IPv6 Address 1	AnalyzerIPV6
Device Custom IPv6 Address 1 Label	"Device IPv6 Address"
Device Custom IPv6 Address 2	SourceIPV6
Device Custom IPv6 Address 2 Label	"Source IPv6 Address"
Device Custom IPv6 Address 3	TargetIPV6
Device Custom IPv6 Address 3 Label	"Destination IPv6 Address"
Device Custom Number 1	ManagedState
Device Custom Number 1 Label	"Managed State"
Device Custom Number 2	ThreatHandled
Device Custom Number 2 Label	"Threat Handled"
Device Custom String 1	ThreatName
Device Custom String 1 Label	"Threat Name"
Device Custom String 2	AgentPlatform
Device Custom String 2 Label	"Agent Platform"

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	Analyzer
Device Custom String 4 Label	"Detect Product ID"
Device Custom String 5	AgentGUID
Device Custom String 5 Label	AgentGUID
Device Custom String 6	ThreatType
Device Custom String 6 Label	"Threat Type"
Device Event Category	ThreatCategory
Device Event Class ID	ThreatEventID
Device Host Name	AnalyzerHostName
Device Mac Address	AnalyzerMAC
Device Product	"Active Response"
Device Receipt Time	ReceivedUTC
Device Severity	ThreatSeverity
External ID	AutoID
File Name	TargetFileName
Flex String 2	Tags
Name	name
Request Url	SourceURL
Source Address	SourceIPV4
Source Host Name	SourceHostName
Source Mac Address	SourceMAC
Source Process Name	SourceProcessName
Source User Name	SourceUserName
Transport Protocol	TargetProtocol

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

ArcSight ESM Field	Device-Specific Field
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	AutoID
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
Source Mac Address	ThreatSourceMAC

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

McAfee Agents events with ePO 5.10

ArcSight ESM Field	Device-Specific Field
Destination Host Name	HostName
Destination User Name	UserName
Device Action	Type
Device Custom Date 1	DetectedUTC
Device Custom Date 1 Label	Detected Time
Device Custom IPv6 Address 3	IPV6
Device Custom IPv6 Address 3 Label	Destination IPv6 Address
Device Custom Number 1	ManagedState
Device Custom Number 1 Label	Managed State
Device Custom Number 2	Error
Device Custom Number 2 Label	Error Code
Device Custom String 1	InitiatorType
Device Custom String 1 Label	Initiator Type
Device Custom String 3	SiteName
Device Custom String 3 Label	Site Name
Device Custom String 4	ProductCode
Device Custom String 4 Label	Product Code
Device Custom String 5	AgentGUID
Device Custom String 5 Label	Agent GUID
Device Event Class ID	TVDEventID
Device Receipt Time	ReceivedUTC
Device Severity	TVDSerivity
Device Version	Version

ArcSight ESM Field	Device-Specific Field
Device Version	Both (DetectingProductVersion,DetectingAgentVersion)
End Time	DetectedUTC
External ID	AutoID
Flex String 2	Tags
Message	Description
Name	Name
Start Time	ReceivedUTC

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	AutoID
Message	Message
Name	CmdName
Start Time	StartTime

Orion Audit Log 5.1 Mappings with ePO DB 5.10

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'
Device Version	'Unknown'
End Time	EndTime
Event Outcome	One of (Success, '1', 'Success', 'Failed')
External ID	AutoID
Message	Message
Name	CmdName
Reason	DetailMessage
Request Method	AdditionalDetailsURI
Source Address	LocalAddress
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

ArcSight ESM Field	Device-Specific Field
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'
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'
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

ArcSight ESM Field	Device-Specific Field
File Name	filePath
File Path	filePath
File Size	Size
File Type	filePath
Name	Type
Old File Name	
Reason	ErrorCode

Policy Auditor File (PA File) 6.4

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

ArcSight ESM Field	Device-Specific Field
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
Old File ID	PlatformID
Old File Name	
Reason	ErrorCode
Source User ID	EmailAddress

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

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

Policy Auditor Rule (PA Rule) 6.4

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

ArcSight ESM Field	Device-Specific Field
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 Severity	VendorSeverity
Device Time Zone	TimeZone
Device Vendor	'McAfee'
Device Version	'Unknown'
Event Outcome	RuleResult
Message	CheckDescription
Name	Title
Old File ID	PlatformID
Source User ID	EmailAddress

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	DeviceAction
Device Custom Date 1	StartRecordedTime
Device Custom Date 2	EndRecordedTime

ArcSight ESM Field	Device-Specific Field
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	StartTime
Device Vendor	'McAfee'
Device Version	'Unknown'
End Time	EndTime
Name	'Rogue System'
Start Time	StartTime

Rogue System Detection events with ePO 5.10

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	StartRecordedTime
Device Custom Date 2	EndRecordedTime
Device Custom IPv6 Address 3	IPv6
Device Custom Number 1	ManagedState
Device Custom Number 1 Label	Managed State
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'

ArcSight ESM Field	Device-Specific Field
Device Product	'Rogue System Sensor'
Device Receipt Time	StartTime
Device Vendor	'McAfee'
Device Version	'Unknown'
End Time	End Time
Name	'Rogue System'
Start Time	Start Time

Security for Microsoft SharePoint Events with ePO 5.10

ArcSight ESM Field	Device-Specific Field
Destination Address	TargetIPv4
Destination Host Name	TargetHostName
Destination Mac Address	TargetMAC
Destination Port	TargetPort
Destination Process Name	TargetProcessName
Destination User Name	TargetUserName
Detect Time	DetectedUTC
Device Action	ThreatActionTaken
Device Address	AnalyzerIPv4
Device Custom Date 1	DetectedUTC
Device Custom Date 1 Label	Generated Time
Device Custom IPv6 Address 1	AnalyzerIPv6
Device Custom IPv6 Address 1 Label	Device IPv6 Address
Device Custom IPv6 Address 2	SourceIPv6
Device Custom IPv6 Address 2 Label	Source IPV6 Address
Device Custom IPv6 Address 3	TargetIPv6
Device Custom IPv6 Address 3 Label	Destination IPv6 Address
Device Custom Number 1	ManagedState

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1 Label	Managed State
Device Custom Number 2	ThreatHandled
Device Custom Number 2 Label	Threat Handled
Device Custom String 1	ThreatName
Device Custom String 1 Label	Threat Name
Device Custom String 2	AgentPlatform
Device Custom String 2 Label	Agent Platform
Device Custom String 3	Name
Device Custom String 3 Label	Event Name
Device Custom String 4	Analyzer
Device Custom String 4 Label	Detect Product ID
Device Custom String 5	AgentGUID
Device Custom String 5 Label	Agent GUID
Device Custom String 6	ThreatType
Device Custom String 6 Label	Threat Type
Device Event Category	ThreatCategory
Device Event Class ID	ThreatEventID
Device Host Name	AnalyzerHostName
Device Mac Address	AnalyzerMAC
Device Product	AnalyzerName
Device Receipt Time	ReceivedUTC
Device Severity	ThreatSeverity
Device Version	MSMS, AnalyzerVersion
End Time	DetectedUTC
External ID	ThreatEventID
File Name	TargetFileName
Flex String2	Tags
Message	Description
Name	Name
Request Url	SourceURL
Source Address	SourceIPV4

ArcSight ESM Field	Device-Specific Field
Source Host Name	SourceHostName
Source Mac Address	SourceMAC
Source Process Name	SourceProcessName
Source User Name	SourceUserName
Start Time	ReceivedUTC
Transport Protocol	TargetProtocol

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	agentGUID
Device Event Class ID	Both (EventTypeId, eventName)
Device Product	'SiteAdvisor Enterprise'
Device Receipt Time	detectedTime
Device Severity	ratingId
Device Vendor	'McAfee'
Device Version	'Unknown'
External ID	autold
Message	reasonType
Name	eventName
Request URL	url

ArcSight ESM Field	Device-Specific Field
Source NT Domain	userId
Source User ID	userId
Source User Name	userName

SiteAdvisor Enterprise 3.5/3.5.5 Mappings with ePO 5.10

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 Number 3	managedState
Device Custom String 2	listType
Device Custom String 3	ratingName
Device Custom String 4	observerMode(0=off,1=on)
Device Custom String 5	agentGuid
Device Event Class ID	Both(EventTypeld, eventName)
Device Product	'SiteAdvisor Enterprise'
Device Receipt Time	detectedTime
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 2.1/2.3 Events with ePO 5.3/5.10

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	AutoID
Flex String2	tags
Message	Description
Name	Name
Reason	Error

TIE_VSE 1.0 Events with ePO 5.3/5.10

ArcSight ESM Field	Device-Specific Field
Destination Address	targetipaddress
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)

ArcSight ESM Field	Device-Specific Field
Flex String 2	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
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	virusype
Device Custom String 3	All of ('ProductName: ', productname, ',ProductVersion: ', productversion)
Device Custom String 4	scantype (Analyzer Detection Method)

ArcSight ESM Field	Device-Specific Field
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

VirusScan Enterprise 8.8 Events with ePO DB 5.10

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	5, 6 = Very High; 4 = High; 2, 3 = Medium, 1 = Low
Base Event Count	counter
Destination Address	agentipaddress
Destination Host Name	agenthostname
Destination Mac Address	agentmac
Destination NT Domain	agentdomainname

ArcSight ESM Field	Device-Specific Field
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	virusype
Device Custom String 3	All of ('ProductName: ', productname, ',ProductVersion: ', productversion)
Device Custom String 4	scantype (Analyzer Detection Method)
Device Custom String 5	engine version
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
Old File ID	__ifThenElse(SystemSerialNumber,,,__concatenate("System Serial Number : ",SystemSerialNumber))
Old File Name	__ifThenElse(EmailAddress,,,__concatenate("Email Address : ",EmailAddress))
Old File Path	__ifThenElse(PlatformID,,,__concatenate("Platform ID : ",PlatformID))

ArcSight ESM Field	Device-Specific Field
Old File Permission	<code>__ifThenElse(SystemManufacturer,__,__concatenate("System Manufacturer : ",SystemManufacturer))</code>
Old File Type	<code>__ifThenElse(SystemModel,__,__concatenate("System Model : ",SystemModel))</code>
Source Address	<code>sourceaddress</code>
Source HostName	<code>source</code>
Source Mac Address	<code>sourcemac</code>
Source Port	<code>LoadBalancerHttpsPort</code>
Source Process Name	<code>sourceprocessname</code>
Source User Name	<code>sourceusername</code>

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`.

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 SmartConnector for McAfee ePolicy Orchestrator DB (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

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

We appreciate your feedback!