



ArcSight SmartConnector

Software Version: CE 24.4

Configuration Guide for Trellix ePolicy Orchestrator DB SmartConnector

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

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

Documentation Updates

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

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

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

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

Support

Contact Information

| | |
|--------------------------------|---|
| Phone | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| Support Web Site | https://softwaresupport.softwaregrp.com/ |
| ArcSight Product Documentation | https://www.microfocus.com/documentation/arcsight/ |

Configuration Guide for Trellix ePolicy Orchestrator DB SmartConnector

This guide provides information for installing the SmartConnector for Trellix ePolicy Orchestrator DB and 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](#).

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

Trellix Endpoint Security protects endpoints and empowers the workforce with an integrated security framework. Endpoint Security intercepts threats, monitors overall system health, and

reports detection and status information. The Endpoint Security client is installed on each system to perform these tasks.

The Trellix ePolicy Orchestrator connector is installed on the client computers to connect to the Trellix DB from where it gathers and reports the overall system health, reports detection and status information. For determining how the product features work, install one or more Endpoint Security modules on client systems, manage detections, and configure the settings.

Trellix Endpoint Security Modules Supported

The Trellix Endpoint Security modules that are supported for event collection are as follows:

- Adaptive Threat Protection (ATP) 10.7.0
- Advanced Threat Defense and Intelligent Sandbox 5.2
- Data Loss Prevention 11.10
- Data Loss Prevention Administrative 11.x
- Data Loss Prevention Discover 11.10
- Data Loss Prevention Incident Events 11.10
- Firewall 10.7.0
- Management for Optimized Virtual Environments (MOVE) 4.1
- Policy Auditor 6.5
- Rogue System Detection 5.0
- SolidCore 8.3
- Threat Intelligence Exchange Server 4.0
- Threat Prevention 10.7.0
- Trellix Agent 5.7
- Trellix Security for Microsoft Exchange (MSME) 8.8
- Trellix Security for SharePoint 3.5
- Web Protection 10.7.0

Configuration

For information about configuring your ePolicy Orchestrator agents for event collection, see the appropriate Trellix product documentation.

Configuring the Logging Level of Logs

The following DWORD registry value is used to specify the logging level of the logs that are used for debugging:

HEKY_LOCAL_MACHINES\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL

The LOGLEVEL values are the numbers 1 through 8. The default value is 7, if no value is specified.

- 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).
- 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 Logs

The following DWORD registry value is used to specify the maximum size of the logs that are used for debugging:

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 a log file reaches the maximum size, it is renamed to maximum size, they are renamed to <LOG NAME>_BACKUP.LOG and a new log file is created. If a backup copy of the 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 8.4.0 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](#)).

For more information related to the Microsoft JDBC driver, see the [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`.



Note: While upgrading the connector, you can skip step 4 if the JDBC driver is already present in the path.

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`



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

6. To add JDBC Driver to ArcMC or Connector Appliance, see Adding JDBC Driver to the Connector Appliance/ ArcSight Management Center.
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 **Trellix ePolicy Orchestrator DB** from the **Type** drop-down, then click **Next**.
10. Enter the following parameters, then click **Next**.

| URL | User | Password | Event Types |
|--|------|----------|---------------|
| jdbc:sqlserver://15.214.197.4:1433;DatabaseName=Trellix_ePO510 | sa | ***** | webprotection |

| 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>.</p> <p>Substitute actual values for <code><MS SQL Server Host Name or IP Address></code> and <code><MS SQL Server Database Name></code>.</p> <p>Note: If you are 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 the appropriate privilege. |
| Password | Enter the password assigned to the Database user. |
| Event Types | <p>Select the Event Types to be processed. You can enter a single parameter, or a combined list separated by comma. However, you must not add white space between the parameters.</p> <p>For example, use <code>firewall</code> for processing events only from the Firewall module.</p> <p>Use <code>webprotection, threatprevention</code> for processing events from Web protection and Threat Prevention.</p> <p>Use <code>endpointsecurity</code> if you want to process all different modules of EndPoint Security.</p> |

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

12. 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.
13. Select a [destination and configure parameters](#).
14. Specify a name for the connector.
15. (Conditional) For **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.

16. Select whether you want to install the connector as a service or in the standalone mode.
17. Complete the installation.



Note: To complete the installation process, you must cancel the wizard and copy the JDBC jar file for executing the agentsetup. This will configure the Trellix Epo database connection string and its event types.

18. [Run the SmartConnector](#).
19. 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 Web Protection events, enter `webprotection` 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 between the parameters.

| Parameter | Used for |
|-------------------|---|
| atd | Advanced Threat Defense and Intelligent Sandbox |
| atp | Adaptive Threat Protection (ATP) |
| dlp | Data Loss Prevention (DLP) |
| dlpadministrative | Data Loss Prevention Administrative |
| dlpdiscover | Data Loss Prevention Discover |
| dlpincident | Data Loss Prevention Incident |
| endpointsecurity | Firewall, Web Protection and Adaptive Threat Protection (ATP) |
| firewall | Firewall |
| move | Management for Optimized Virtual Environments (MOVE) |
| msme | McAfee Security for Microsoft Exchange (MSME) |

| Parameter | Used for |
|-------------------|-------------------------------------|
| msms | Trellix Security for SharePoint |
| policyauditorfile | Policy Auditor File |
| policyauditorrule | Trellix Policy Auditor Rule |
| rsd | Trellix Rogue System Detection |
| threatprevention | Threat Prevention |
| tie_server | Threat Intelligence Exchange Server |
| trellix_agents | Trellix Agents |
| webprotection | Web Protection |

Device Event Mapping to ArcSight Fields

The following table lists the mapping of ArcSight data fields to the device's specific event definitions:

Trellix 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 | DeviceAction |
| Device Custom Date 1 | StartRecordedTime |
| Device Custom Date 1 Label | "First Recorded Time" |
| Device Custom Date 2 | EndRecordedTime |
| Device Custom Date 2 Label | "Last Recorded 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" |

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--|
| Device Custom String 3 | IPV6 |
| Device Custom String 3 Label | "IPv6" |
| Device Custom String 4 | __concatenate(OS," ",OSFamily," ",OSVer) |
| Device Custom String 4 Label | "OS Type" |
| Device Custom String 5 | SourceType |
| Device Custom String 5 Label | "Source Type" |
| Device Custom String 6 | tags |
| Device Custom String 6 Label | "Tags" |
| Device Event Class ID | "Detected Rogue System by RSD" |
| Device Product | ModuleName |
| Device Receipt Time | StartTime |
| Device Vendor | "Trellix" |
| Device Version | ProductVersion |
| End Time | EndTime |
| Name | "Rogue System" |
| Start Time | StartTime |

Trellix Policy Auditor Rule Events with ePO 5.10

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---------------------------|
| Additional Data | HistorySummaryAutoID |
| Additional Data | ManagementType |
| Additional Data | ResultDateAutoID |
| Additional Data | UID |
| Additional Data | Vdi |
| Destination Address | IPAddress |
| Destination Host Name | SystemName |
| Destination MAC Address | NetAddress |
| Device Address | HostIP |
| Device Custom Date 1 | VendorPublicationDate |
| Device Custom Date 1 Label | "Vendor Publication Date" |

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--|
| Device Custom Date 2 | ExpirationDate |
| Device Custom Date 2 Label | "Expiration Date" |
| Device Custom Number 1 | TenantID |
| Device Custom Number 1 Label | "Tenant ID" |
| Device Custom Number 2 | ManagedState |
| Device Custom Number 2 Label | "Managed State" |
| Device Custom Number 3 | CheckVersion |
| Device Custom Number 3 Label | "Check Version" |
| Device Custom String 1 | ClassType |
| Device Custom String 1 Label | "Class Type" |
| Device Custom String 2 | CheckID |
| Device Custom String 2 Label | "Check ID" |
| Device Custom String 3 | __regexTokenNoWarning(Title,"(MS\\d+\\ \\d+)\\s*.*)") |
| Device Custom String 3 Label | "Vulnerability Reference ID" |
| Device Custom String 4 | RuleID |
| Device Custom String 4 Label | "Rule ID" |
| Device Custom String 5 | __concatenate(BenchmarkID," ",BenchmarkVersion) |
| Device Custom String 5 Label | "Benchmark" |
| Device Custom String 6 | AuditName |
| Device Custom String 6 Label | "Audit Name" |
| Device Domain | Domain |
| Device Event Category | "PARule" |
| Device Event Class ID | __concatenate(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 | "Trellix" |
| Event Outcome | RuleResult |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|--|
| Message | CheckDescription |
| Name | __stringTrim(__oneOf(__regexTokenNoWarning(Title,"(?:\\S+, \\d+)?(?: (.*)\\s*\\(\\..*\\) (.*)"),Title)) |
| Old File Id | __concatenate("Platform ID: ",PlatformID) |
| Source User ID | EmailAddress |

Policy Auditor File Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|-------------------------|-------------------------------------|
| Additional Data | isSystem |
| Additional Data | action |
| Additional Data | isArchive |
| Additional Data | isHidden |
| Additional Data | isReadOnly |
| Additional Data | vdi |
| Additional Data | managementType |
| Additional Data | isBaseline |
| Destination Address | HostIP |
| Destination Host Name | HostName |
| Destination MAC Address | __getLongMACAddressByHexString(MAC) |
| Destination User Name | FileOwner |
| Destination User ID | AcceptedByUserID |
| 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 5 | FileGroup |
| Device Custom String 6 | Tags |
| Device Domain | Domain |
| Device Event Category | "PAFile" |
| Device Event Class ID | Type |
| Device Host Name | HostName |
| Device MAC Address | __getLongMACAddressByHexString(MAC) |
| Device Product | "Policy Auditor" |
| Device Receipt Time | ReportedTime |
| Device Time Zone | TimeZone |
| Device Vendor | "Trellix" |
| File Create Time | CreatedTime |
| File Hash | __oneOf(SHA2,fileMD5Hash,fileSHA1Hash) |
| File Modification Time | ModifiedTime |
| File Name | __regexToken(filePath,".*\\\\\\(.*\$)") |
| File Path | __regexToken(filePath,"(.*\\\\\\).*\$") |
| File Size | Size |
| Name | Type |
| Old File ID | __ifThenElse(PlatformID, "", __concatenate("Platform ID: ", PlatformID)) |
| Old File Name | __ifThenElse(AllowedIPs, "", __concatenate("Allowed IPs: ", AllowedIPs)) |
| Reason | ErrorCode |
| Source User ID | EmailAddress |

Trellix Agents Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|-----------------------|
| Destination Host Name | HostName |
| Destination User Name | UserName |
| Device Action | Type |
| Device Custom Date 1 | GeneratedTime |
| 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 Custom String 5 | Tags |
| Device Custom String 5 Label | Tags |
| Device Event Class ID | TVDEventID |
| Device Receipt Time | ReceivedUTC |
| Device Severity | TVDSeriverty |
| Device Version | One of (DetectingProductVersion,DetectingAgentVersion) |
| End Time | DetectedUTC |
| External ID | AutoID |
| Message | Description |
| Name | Name |
| Start Time | ReceivedUTC |

Data Loss Prevention Administrative Event Mappings

| 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 Number 2 | PolicyRevision |
| Device Custom String 1 | PolicyName |
| Device Custom String 5 | PolicyUid |
| Device Custom String 6 | UserGroups |
| Device Event Category | 'Administrative event' |
| Device Product | 'Data Loss Prevention' |
| Device Receipt Time | EndpointTime |
| Device Severity | Severity (0=Info, 1=Warning, 2=Minor, 3=Major, 4=Critical) |
| Device Vendor | 'Trellix' |
| Device Version | 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 |
| Reason | ReplicationFailedError |
| Device Custom Number 2 | ReleaseCodeAttempts |
| Device Custom Number 3 | ReleaseCodeDuration |

McAfee Security for Microsoft Exchange (MSME) Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | 0,1,2 = High; 3,4 = Medium; 5,6,7 = Low |
| Destination Address | __integerToAddressMcAfee(__safeToInteger(IPV4)) |
| Destination Host Name | HostName |

| | |
|------------------------------------|--|
| Destination Mac Address | __getLongMACAddressByHexString(MAC) |
| Destination Port | __safeToInteger(PortNumber) |
| Destination Process Name | ProcessName |
| Destination User Name | UserName |
| Device Action | ThreatAction |
| Device Custom Date 1 | __toLocalTimeStamp(GeneratedTime) |
| Device Custom Date 1 Label | __stringConstant("Detect Time") |
| Device Custom IPv6 Address 1 | __byteArrayToIPv6(DetectingProductIPv6) |
| Device Custom IPv6 Address 1 Label | __stringConstant("Device IPv6 Address") |
| Device Custom IPv6 Address 2 | __byteArrayToIPv6(ThreatSourceIPv6) |
| Device Custom IPv6 Address 2 Label | __stringConstant("Source IPv6 Address") |
| Device Custom IPv6 Address 3 | __byteArrayToIPv6(IPv6) |
| Device Custom IPv6 Address 3 Label | __stringConstant("Destination IPv6 Address") |
| Device Custom Number 2 | ManagedState |
| Device Custom Number 2 Label | __stringConstant("Managed State") |
| Device Custom String 3 | ThreatName |
| Device Custom String 3 Label | __stringConstant("Threat Name") |
| Device Custom String 4 | DetectingProductID |
| Device Custom String 4 Label | __stringConstant("Detecting Product ID") |
| Device Custom String 5 | AgentGUID |
| Device Custom String 5 Label | __stringConstant("Agent GUID") |
| Device Custom String 6 | Tags |
| Device Custom String 6 Label | __stringConstant("Tags") |
| Device Event Category | ThreatCategory |
| Device Event Class ID | ThreatEventID |

| | |
|---------------------|---|
| Device Host Name | DetectingProductHostName |
| Device Mac Address | __getLongMACAddressByHexString(DetectingProductMAC) |
| Device Product | DetectingProductName |
| Device Receipt Time | __toLocalTimeStamp(__longToTimeStamp(ReceivedTime)) |
| Device Severity | ThreatSeverity |
| Device Vendor | __stringConstant("Trellix") |
| Device Version | DetectingProductVersion |
| External Id | AutoID |
| File Name | FileName |
| Message | ThreatType |
| Name | EventName |
| Request Url | ThreatSourceURL |
| Source Address | __integerToAddressMcAfee(__safeToInteger(ThreatSourceIPv4)) |
| Source Host Name | ThreatSourceHostName |
| Source Mac Address | __getLongMACAddressByHexString(ThreatSourceMAC) |
| Source Process Name | ThreatSourceProcessName |
| Source User Name | ThreatSourceUserName |
| Transport Protocol | NetworkProtocol |

Trellix MOVE Antivirus Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | Critical, Major = High; Minor, Warning = Medium; Info = Low |
| Destination Address | __integerToAddressMcAfee(__safeToInteger(IPv4)) |
| Destination Host Name | HostName |
| Destination Mac Address | __getLongMACAddressByHexString(MAC) |
| Destination Port | __safeToInteger(PortNumber) |
| Destination Process Name | ProcessName |

| | |
|------------------------------------|---|
| Destination User Name | UserName |
| Device Action | ThreatAction |
| Device Custom Date 1 | __toLocalTimeStamp(GeneratedTime) |
| Device Custom Date 1 Label | __stringConstant("Detected Time") |
| Device Custom IPv6 Address 1 | __byteArrayToIPv6(DetectingProductIPv6) |
| Device Custom IPv6 Address 1 Label | __stringConstant("Device IPv6 Address") |
| Device Custom IPv6 Address 2 | __byteArrayToIPv6(ThreatSourceIPv6) |
| Device Custom IPv6 Address 2 Label | __stringConstant("Source IPv6 Address") |
| Device Custom IPv6 Address 3 | __byteArrayToIPv6(IPv6) |
| Device Custom IPv6 Address 3 Label | __stringConstant("Destination IPv6 Address") |
| Device Custom Number 2 | ManagedState |
| Device Custom Number 2 Label | __stringConstant("Managed State") |
| Device Custom String 1 | ThreatName |
| Device Custom String 1 Label | __stringConstant("Threat Name") |
| Device Custom String 4 | DetectingProductID |
| Device Custom String 4 Label | __stringConstant("Detecting Product ID") |
| Device Custom String 5 | AgentGUID |
| Device Custom String 5 Label | __stringConstant("Agent GUID") |
| Device Custom String 6 | Tags |
| Device Custom String 6 Label | __stringConstant("Tags") |
| Device Event Category | ThreatCategory |
| Device Event Class ID | ThreatEventID |
| Device Host Name | DetectingProductHostName |
| Device Mac Address | __getLongMACAddressByHexString(DetectingProductMAC) |
| Device Product | __stringConstant("MOVE Antivirus") |
| Device Receipt Time | __toLocalTimeStamp(__longToTimeStamp(ReceivedTime)) |
| Device Severity | __simpleMap (ThreatSeverity,"0=Info","1=Warning","Minor","3=Major","4=Critical") |
| Device Vendor | __stringConstant("Trellix") |
| Device Version | DetectingProductVersion |
| External ID | AutoID |
| File Name | FileName |

| | |
|---------------------|---|
| File Type | ThreatType |
| Message | ThreatType |
| Request Url | ThreatSourceURL |
| Source Address | __integerToAddressMcAfee(__safeToInteger(ThreatSourceIPv4)) |
| Source Host Name | ThreatSourceHostName |
| Source Mac Address | __getLongMACAddressByHexString(ThreatSourceMAC) |
| Source Process Name | ThreatSourceProcessName |
| Source User Name | ThreatSourceUserName |
| Transport Protocol | NetworkProtocol |

Data Loss Prevention Discover Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|---|
| Agent (Connector) Severity | Critical, Major = High, Minor, Warning = Medium, Info = Low |
| Bytes In | TotalContentSize |
| Destination Nt Domain | __extractNTDomain(UserPrincipalName) |
| Destination User Name | __extractNTUser(UserAccount) |
| Destination User Privileges | UserGroups |
| Device Action | ActualAction("0=No action", "1=Block", "2=Encrypt", "3=Request Justification", "4=RM Protect", "5=Quarantine", "6=Read-only", "7=Block", "8=Delete", "9=Tag", "10=Copy", "11=Move", "12=Remove Sharing", "13=Remove All Sharing", "17=Classify File", "19=Request Justification", "22=Remove Automatic Classification") |
| Device Custom Date 1 | ViolationUTCTime |
| Device Custom Date 1 Label | "Violation UTC Time" |
| Device Custom Number 1 | EvidenceCount |
| Device Custom Number 1 Label | "Evidence Count" |
| Device Custom Number 2 | PolicyRevision |
| Device Custom Number 2 Label | "Policy Revision" |
| Device Custom Number 3 | IncidentId |
| Device Custom Number 3 Label | "Incident ID" |
| Device Custom Sting 2 | Both(Status: StatusKey Resolution: ResolutionKey) |
| Device Custom Sting 2 Label | "Status and Resolution" |

| | |
|------------------------------|---|
| Device Custom String1 | RulesToDisplay |
| Device Custom String 1 Label | "Rules To Display" |
| Device Custom String 3 | PolicyName |
| Device Custom String 3 Label | "Policy Name" |
| Device Event Category | "Discover Event" |
| Device Product | "Data Loss Prevention" |
| Device Receipt Time | ViolationLocalTime |
| Device Severity | Severity("0=Info","1=Warning","2=Minor","3=Major","4=Critical") |
| Device Vendor | Trellix |
| Device Version | DlpAgentVersion |
| End Time | InsertionTime |
| External ID | IncidentType |
| File Hash | SHA1 |
| File Name | FileName |
| File Path | FilePath |
| File Size | FileSize |
| Reason | FailureReason |
| Request Context | ItemType |
| Source Address | IP |
| Source FQDN | FQDN |
| Source Host Name | Name |
| Source User Name | __extractNTUser(UserAccount) |
| Source Nt Domain | __extractNTDomain(Username_NTLM) |

Advanced Threat Defense and Intelligent Sandbox Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | Critical, Major = High; Minor, Warning = Medium; 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 Address | DetectingProductIPv4 |
| Device Custom Date 1 | DetectTime |
| 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 String 1 | ThreatType |
| Device Custom String 2 | ProductFamily |
| Device Custom String 4 | DetectingProductID |
| Device Custom String 5 | AgentGUID |
| Device Custom String 6 | ThreatName |
| Device Event Category | ThreatCategory |
| Device Event Class ID | ThreatEventID |
| Device Host Name | DetectingProductHostName |
| Device Mac Address | DetectingProductMAC |
| Device Product | DetectingProductName |
| Device Receipt Time | ReceivedTime |
| Device Severity | ThreatSeverity |
| Device Vendor | Trellix |
| Device Version | ATDProductVersion |
| External ID | AutoID |
| File Create Time | FileUploadTime |
| File Hash | MD5 |
| File Path | FilePath |
| File Size | size |
| Message | Description |
| Name | Name |

| | |
|---------------------|-------------------------|
| Outcome | ThreatHandled |
| 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 |

Data Loss Prevention Incident Event Mappings

| 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 |
| Destination User Privileges | UserGroups |
| Device Action | ActualAction ("0=No action", "1=Block", "2=Encrypt", "3=Request Justification", "4=RM Protect", "5=Quarantine", "6=Read-only", "7=Block", "8=Delete", "9=Tag", "10=Copy", "11=Move", "12=Remove Sharing", "13=Remove All Sharing", "17=Classify File", "19=Request Justification", "22=Remove Automatic Classification") |
| Device Custom Date 1 | ViolationUTCTime (Violation UTC Time) |
| Device Custom Number 1 | EvidenceCount |
| Device Custom Number 2 | PolicyRevision |
| Device Event Category | Incident Event |

| | |
|---------------------|---|
| Device Product | Data Loss Prevention |
| Device Receipt Time | ViolationLocalTime |
| Device Severity | Severity (0=Info, 1=Warning, 2=Minor, 3=Major, 4=Critical) |
| Device Vendor | Trellix |
| Device Version | DlpAgentVersion |
| End Time | InsertionTime |
| External ID | IncidentType |
| File Hash | SHA1 |
| File Name | FileName |
| File Path | FilePath |
| File Permission | __concatenate("Copy Direction: ",copyDirection) |
| File Size | FileSize |
| File Type | FileType |
| Name | RulesToDisplay |
| Old File Type | (BusType,"0=0","1=USB","2=PCI","3=FireWire (IEEE1394)","4=PCMCIA","5=Bluetooth","6=IDE/SATA","7=SCSI","8=SD","9=Thunderbolt") |
| 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 |

Data Loss Prevention (DLP) Event Mappings

| 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 | threattype |
| Device Custom String 2 | detectingproductid |
| Device Custom String 4 | tags |
| Device Custom String 5 | agentguid |
| Device Event Class ID | threateventid |
| Device Host Name | producthostname |
| Device Mac Address | productmac |
| Device Product | Data Loss Prevention |
| Device Receipt Time | receivedtime |
| Device Severity | threatseverity |
| Device Vendor | Trellix |
| Device Version | productversion |
| External ID | autoid |
| File Path | One of (sourceurl, targetfilename) |
| Name | threatname |
| 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 |

SolidCore Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|---|
| Agent (Connector) Severity | 1 = Very High; 2,3 = High; 4,5 = Medium; 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 |
| Device Custom Date 1 Label | Detected Time |
| Device Custom IPv6 1 | AnalyzerIPv6 |
| Device Custom IPv6 1 Label | Device IpV6 Address |
| Device Custom IPv6 2 | SourceIPv6 |
| Device Custom IPv6 2 Label | Source IpV6 Address |
| Device Custom IPv6 3 | TargetIPv6 |
| Device Custom IPv6 3 Label | Target IpV6 Address |
| Device Custom Number 1 | TenantId |
| Device Custom Number 1 Label | Tenant ID |
| Device Custom Number 2 | ManagedState |
| Device Custom Number 2 Label | Managed State |
| Device Custom Number 3 | EVT_REPUTATION_SCORE |
| Device Custom Number 3 Label | Reputation Score |
| Device Custom String 1 | Analyzer |
| Device Custom String 1 Label | Detecting Product ID |
| Device Custom String 4 | AGENTGUID |
| Device Custom String 4 Label | Agent GUID |
| Device Custom String 5 | EVT_CMD_LINE |
| Device Custom String 5 Label | Command Line |
| Device Custom String 6 | Tags |

| | |
|------------------------------|-------------------|
| Device Custom String 6 Label | Tags |
| Device Event Category | ThreatCategory |
| Device Event Class Id | THREATEVENTID |
| Device Event String 3 | EVT_CMD_USER_NAME |
| Device Event String 3 Label | Command User Name |
| Device Host Name | AnalyzerHostName |
| Device Mac Address | AnalyzerMAC |
| Device Product | SolidCore |
| Device Receipt Time | RECEIVEDUTC |
| Device Severity | THREATSEVERITY |
| Device Vendor | Trellix |
| Device Version | AnalyzerVersion |
| External Id | AUTOID |
| File Hash | EVT_FILE_MD5 |
| File Name | EVT_FILE_NAME |
| File Path | EVT_OBJECT |
| File Type | EVT_FILE_TYPE |
| Name | EVT_DISPLAY_KEY |
| Old File Name | EVT_CMD_STATUS |
| Reason | EVT_DENY_REASON |
| Request URI | SourceURL |
| Source Host Name | SourceHostName |
| Source IPI | SourceIPV4 |
| Source Mac Address | SourceMac |
| Source Process Name | SourceProcessname |
| Source User Name | EVT_USER_NAME |
| Transport Protocol | TargetProtocol |

Threat Intelligence Exchange Server Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------------|---|
| Agent (Connector) Severity | 1 = Very High; 2,3 = High; 4,5 = Medium; 6, 7 = Low |
| 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 | TenantId |
| Device Custom Number 1 Label | Tenant Id |
| Device Custom Number 2 | ManagedState |
| Device Custom Number 2 Label | Managed State |
| Device Custom String 2 | ProductFamily |
| Device Custom String 2 Label | Product Family |
| Device Custom String 3 | AgentPlatform |
| Device Custom String 3 Label | Agent Platform |
| Device Custom String 4 | AgentGUID |
| Device Custom String 4 Label | Agent GUID |
| Device Custom String 5 Label | Agent Version |
| Device Custom String 6 | Tags |
| Device Custom String 6 Label | Tags |
| Device Event Class ID | ThreatEventID |
| Device Facility | SiteName |
| Device Product | FamilyDispName |
| Device Receipt Time | ReceivedTime |
| Device Severity | ThreatSeverity |
| Device Vendor | Trellix |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|-----------------------|
| Device Version | CatalogProductVersion |
| External ID | AutoID |
| Message | Description |
| Name | Name |
| Reason | Error |

Trellix Security for SharePoint Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------------|---|
| Agent (Connector) Severity | 1 = Very High; 2,3 = High; 4,5 = Medium; 6, 7 = 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 | DetectedUTC |
| Device Custom Date 1 Label | Detected Time |
| Device Custom IPv6 Address 1 | DetectingProductIPv6 |
| Device Custom IPv6 Address 1 Label | Device IPv6 Address |
| Device Custom IPv6 Address 2 | ThreatSourceIPv6 |
| Device Custom IPv6 Address 2 Label | Source IPv6 Address |
| Device Custom IPv6 Address 3 | IPv6 |
| Device Custom IPv6 Address 3 Label | Destination IPv6 Address |
| Device Custom Number 1 | ThreatHandled |
| Device Custom Number 1 Label | Threat Handled |
| Device Custom Number 2 Label | ManagedState |
| Device Custom String 1 | ThreatName |
| Device Custom String 1 Label | Threat Name |
| Device Custom String 2 | ThreatType |

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--------------------------|
| Device Custom String 2 Label | Threat Type |
| Device Custom String 4 | AgentGUID |
| Device Custom String 4 Label | Agent GUID |
| Device Custom String 5 | AgentPlatform |
| Device Custom String 5 Label | Agent Platform |
| Device Custom String 6 | Tags |
| Device Custom String 6 Label | Tags |
| Device Event Category | ThreatCategory |
| Device Event Class ID | ThreatEventID |
| Device Host Name | DetectingProductHostName |
| Device MAC Address | DetectingProductMAC |
| Device Product | ProductName |
| Device Receipt Time | ReceivedTime |
| Device Severity | ThreatSeverity |
| Device Vendor | Trellix |
| Device Version | DetectingProductVersion |
| External ID | AutoID |
| Message | Description |
| Name | Name |
| 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 |

Trellix Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--|
| Agent (Connector) Severity | 2, 1, 0 = High; 4, 3 = Medium; 5, 6, 7 = Low |
| 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 | ServerIPAddress |
| Device Custom Number 1 | TenantID |
| Device Custom Number 1 Label | TenantId |
| Device Custom Number 2 | AnalyzerDATVersion |
| Device Custom Number 2 Label | Analyzer DAT Version |
| Device Custom String 1 | ThreatName |
| Device Custom String 2 | ThreatType |
| Device Custom String 3 | CatalogProductName |
| Device Custom String 4 | AnalyzerDetectionMethod |
| Device Custom String 5 | AnalyzerEngineVersion |
| Device Event Category | ThreatCategory |
| Device Event Class ID | ThreatEventID |
| Device Host Name | ServerHostName |
| Device Product | Analyzer Name |
| Device Receipt Time | DetectedUTC |
| Device Severity | ThreatSeverity |
| Device Vendor | Trellix |
| Device Version | AnalyzerVersion |
| End Time | Mapped properly by ESM Console |

| ArcSight ESM Field | Device-Specific Field |
|---------------------|-----------------------|
| External ID | AutoID |
| File Hash | Target Hash |
| File Name | TargetFileName |
| Name | Name |
| Old File ID | SystemSerialNumber |
| Old File Name | EmailAddress |
| Old File Path | PlatformID |
| Old File Permission | SystemManufacturer |
| Old File Type | SystemModel |
| Source Address | SourceIPV4 |
| Source Host Name | SourceHostName |
| Source MAC Address | SourceMacAddress |
| Source Port | LoadBalanceHttpPort |
| Source Process Name | SourceProcessName |
| Source User Name | SourceUserName |
| Start Time | GeneratedTime |

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 Trellix ePolicy Orchestrator DB SmartConnector (SmartConnector CE 24.4)

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!