



ArcSight SmartConnector

Software Version: CE 24.1

Configuration Guide for Trellix ePolicy Orchestrator DB SmartConnector

Document Release Date: January 2024

Software Release Date: January 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
- Firewall 10.7.0
- Threat Prevention 10.7.0
- Web Protection 10.7.0
- Threat Intelligence Exchange Server 4.0
- Trellix Security for SharePoint 3.5
- SolidCore 8.3

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: 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.

5. (Optional) 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. 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 because this file gets overwritten during the upgrade process.

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

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

13. 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.
14. Select a [destination and configure parameters](#).
15. Specify a name for the connector.
16. (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.

17. Select whether you want to install the connector as a service or in the standalone mode.
18. 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.

19. [Run the SmartConnector](#).
20. 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
atp	Adaptive Threat Protection (ATP)
firewall	Firewall
threatprevention	Threat Prevention
webprotection	Web Protection
endpointsecurity	Firewall, Web Protection and Adaptive Threat Protection (ATP)
tie_server	Threat Intelligence Exchange Server
msms	Trellix Security for SharePoint

Device Event Mapping to ArcSight Fields

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

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 24.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!