



# ArcSight SmartConnectors

Software Version: 8.4.3

## Configuration Guide for Symantec Endpoint Protection DB SmartConnector

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 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>

## Support

### Contact Information

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

# Contents

Configuration Guide for Symantec Endpoint Protection DB SmartConnector .....	5
Product Overview .....	6
Prerequisites .....	7
Downloading the JDBC Driver .....	7
Configuration .....	8
Configuring an SQL Account with Minimal Privileges .....	8
Configuring Log Preferences .....	8
Installing the SmartConnector .....	10
Preparing to Install the SmartConnector .....	10
Installing and Configuring the SmartConnector .....	10
Adding a JDBC Driver to the Connector Appliance/ArcSight Management Center ..	13
Device Event Mapping to ArcSight Fields .....	15
Agent Mappings .....	15
Agent Behavior Event Mappings .....	16
Agent Packet Mappings .....	17
Agent Packet 14 Mappings .....	18
Agent Security Event Mappings .....	19
Agent Traffic Event Mappings .....	20
Alerts Mappings v14.2 .....	21
Alerts Mappings v14.x .....	23
Alerts Mappings v12.x .....	25
NAC Client Mappings .....	26
NAC System Mappings .....	27
NAC Traffic Mappings .....	28
Notification Alert Mappings .....	29
Scans Mappings .....	29
Server Mappings .....	31

- Server-Admin Mappings ..... 31
- Server Client Mappings .....32
- Server Policy Mappings .....33
- Virus Category Mappings .....33
  
- Actions ..... 35
  
- Alerts ..... 37
  
- Categories .....38
  
- Troubleshooting .....39
  
- Send Documentation Feedback ..... 41

# Configuration Guide for Symantec Endpoint Protection DB SmartConnector

This guide provides information for installing the SmartConnector for Symantec Endpoint Protection DB and configuring the device for event collection.

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](mailto:MFI-Documentation-Feedback@opentext.com).

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

## Product Overview

Symantec Endpoint Protection combines Symantec AntiVirus with advanced threat prevention for defense against malware for laptops, desktops, and servers. It integrates its security technologies in a single agent and management console.

Symantec Endpoint Protection version 12.1 (for Anti-Virus, Anti-Spyware, Network Threat Protection (including firewall events), Network Access Control, and Behavior events) and 14.0 (for Scan, Server Admin Log, Network Threat Protection, Behavior, System Anti-Virus and Anti-Spyware Protection, Virus, and Server Policy events) are supported. The Symantec Endpoint Protection Small Business Edition v12.1 is also supported. Symantec Endpoint Protection components relate to mapping tables for this connector as follows:

Symantec Endpoint Protection Component	Parser/Mappings
Scan Events (SEP 12, 14)	scans
Server Admin. Log Events (SEP 12, 14)	server-admin
Network Threat Protection Events (SEP 12, 14)	agent-security, agent-traffic
Behavior Events (SEP 12, 14)	agent-behavior
System Events (SEP 12, 14)	agent, server
Anti-Virus and Anti-Spyware Protection Events (SEP 12, 14)	alerts
Network Access Control (SEP 12)	nac-client, nac-system, nac-traffic
Notification Alerts (SEP 14)	notificationalerts
Agent Packet Events (SEP 12)	agent-packet
Virus Category (SEP 12, 14)	virus-category
Server Policy Events (SEP 12, 14)	server-policy

# Prerequisites

## 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).

# Configuration

Symantec Endpoint Protection collects and reads events that occur in your network from the management server logs stored in the database. The database can be an existing Microsoft SQL database in your network, with the privilege to connect to and select from the database.

## Configuring an SQL Account with Minimal Privileges

To configure an SQL account to connect with the minimum permissions/tables required for Connector to access files from DB:

1. Open MS SQL Server Management Studio.
2. Create a new user in the MSSQL database (local or AD).
3. Change the default database to the SEPM database.
4. Apply the user to the public server for the SEPM database at **User Mapping > Select SEPM db**.
5. In MS SQL Server Management Studio, verify that the user is permitted to connect to the database at **SEPM DB > Properties > Permissions > Connect / Grant**.
6. Add the `db_datareader` role to the SEPM database at **SEPM DB > Security > Users > User Properties > role members > db\_datareader**.

## Configuring Log Preferences

You can configure the options used for logs and reports. For information about the reporting options you can set, click **Help** on the **Logs and Reports** tab in the **Preferences** dialog box.

To configure preferences:

1. From the console, on the Home page, click **Preferences**.
2. Click the **Logs and Reports** tab.
3. Set the values for the options you want to change.
4. Click **OK**.



For a description of each configurable option, you can click **Tell me more** for that type of log on the Symantec Endpoint Protection Manager Console. **Tell me more** displays the context-sensitive Help.

See Symantec's *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* for complete logging and reporting information.

# 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. Browse to `$ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup` file to start the SmartConnector Configuration Wizard.

7. Browse to `$ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup` file to start the SmartConnector Configuration Wizard.
8. Specify the relevant Global Parameters, when prompted.
9. Select **Symantec Endpoint Protection DB Type** drop-down, then click **Next**.
10. Enter the following parameters to configure the SmartConnector, then click **Next**:

Parameter	Description
JDBC Driver	Select the <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> driver.
Database URL	<p>Enter: <code>jdbc:sqlserver://&lt;MS SQL Server Host Name or IP Address&gt;:1433;DatabaseName=&lt;MS SQL Server Database Name&gt;</code>. Replace with the actual values for &lt;MS SQL Server Host Name or IP Address&gt; and &lt;MS SQL Server Database Name&gt;.</p> <p>To configure JDBC Driver and Windows Authentication, add <code>;integratedSecurity=true</code> to the JDBC URL entry for the connection to your database.</p> <p><b>Note:</b> The name or instance of the database configured at installation or audit time must be used. For example, <code>jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true</code></p>
Database User	Enter the name of a database user with adequate permissions to access the database.
Database Password	Enter the password for the Database User.
Event Types	<p>Enter the types of events the connector is to collect: alerts, agent-security, agent-traffic, nac-client, nac-system, nac-traffic, agent-behavior, agent, server, server-admin, scans, agent-packet, server-client, server-policy, notificationalerts, virus-category. All event types are selected by default, except agent-packet, server-client, server-policy, and notificationalerts.</p> <p><b>Note:</b> If an event type for which no data exists is entered, the error message "Database version could not be detected" is displayed.</p>

- Click **Export** export the host name data you have entered into the table into a CSV file.
- Click **Import** to select a CSV file to import data into the table rather than manually entering it. See the SmartConnector Installation and User's Guide for more information.
- Select a [destination and configure parameters](#).
- Specify a name for the connector.
- (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.

16. Select whether you want to install the connector as a service or in the standalone mode.
17. Complete the installation.
18. [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 a JDBC Driver to the Connector Appliance/ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the 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*.

# 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.

## Agent Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = FATAL; High = ERROR; Medium = WARNING; Low = INFO
Destination Address	IP_ADDR1
Destination Host Name	HOST_NAME
Destination NT Domain	COMPUTER_NAME or concatenate(COMPUTER_NAME,".", COMPUTER_DOMAIN_NAME)
Device Address	SERVER_IP
Device Custom String 6	GROUP_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device NT Domain	SERVER_DOMAIN_NAME, SERVER_NAME or concatenate(SERVER_NAME,".",SERVER_DOMAIN_NAME)
Device Process Name	EVENT_SOURCE
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP
Device Severity	SEVERITY (0=INFO, 1=WARNING, 2=ERROR, 3=FATAL)
Device Vendor	'Symantec'
Device Version	null
End Time	EVENT_TIME
External ID	LOG_IDX
Message	EVENT_DESC
Name	One of (EVENT_DESC, EVENT_SOURCE)
Old File Name	GROUP_NAME

ArcSight ESM Field	Device-Specific Field
Old File Permission	agent
Old File Type	GROUP_TYPE
Start Time	EVENT_TIME

## Agent Behavior Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Device Severity 0-3; High = Device Severity 4-7; Medium = Device Severity 8-11; Low = Device Severity 12-15
Destination Address	IP_ADDR
Destination Host Name	HOST_NAME
Destination Process Id	CALLER_PROCESS_ID
Destination Process Name	CALLER_PROCESS_NAME
Destination User Name	USER_NAME
Device Action	__simpleMap (ACTION,"0=Allow","1=Blocked","2=Ask","3=Continue","4=Terminate")
Device Custom String 1	RULE_NAME
Device Custom String 2	SITE_NAME
Device Custom String 6	GROUP_NAME
Device Domain	DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	_DB_HOST
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP
Device Severity	SEVERITY
Device Vendor	'Symantec'
Device Version	Unknown
End Time	END_TIME
External ID	LOG_IDX
File Path	PARAMETER



ArcSight ESM Field	Device-Specific Field
File Size	FILE_SIZE
Name	DESCRIPTION
Old File Name	GROUP_NAME
Old File Permission	agent-behavior
Old File Type	GROUP_TYPE
Source Host Name	PARENT_SERVER_NAME
Start Time	BEGIN_TIME

## Agent Packet Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	One of(REMOTE_HOST_IP, LOCAL_HOST_IP)(Ignore Zero IP)
Destination Host Name	REMOTE_HOST_NAME   HOST_NAME
Destination Mac Address	One of(REMOTE_HOST_MAC,LOCAL_HOST_MAC)(Ignore Zero IP)
Destination Port	REMOTE_PORT   LOCAL_PORT
Destination User Name	USER_NAME
Device Action	BLOCKED (0=Not blocked, 1=Blocked)
Device Custom String 1	RULE_NAME
Device Custom String 2	SITE_NAME
Device Custom String 6	GROUP_NAME
Device Direction	TRAFFIC_DIRECTION (0=Unknown, 1=Inbound, 2=Outbound)
Device Domain	DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP
Device Vendor	'Symantec'
End Time	EVENT_TIME
File Path	APP_NAME
Message	EVENT_DESC

ArcSight ESM Field	Device-Specific Field
Name	EVENT_ID (401-Raw Ethernet)
Old File Name	GROUP_NAME
Old File Permission	agent-packet
Old File Type	GROUP_TYPE
Source Address	LOCAL_HOST_IP   REMOTE_HOST_IP
Source Host Name	HOST_NAME   REMOTE_HOST_NAME
Source Mac Address	LOCAL_HOST_MAC   REMOTE_HOST_MAC
Source Port	LOCAL_PORT   REMOTE_PORT
Source User Name	USER_NAME

## Agent Packet 14 Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	One of(REMOTE_HOST_IP, LOCAL_HOST_IP)(Ignore Zero IP)
Destination Host Name	REMOTE_HOST_NAME   HOST_NAME
Destination Mac Address	One of(REMOTE_HOST_MAC,LOCAL_HOST_MAC)(Ignore Zero IP)
Destination Port	REMOTE_PORT   LOCAL_PORT
Destination User Name	USER_NAME
Device Action	BLOCKED (0=Not blocked, 1=Blocked)
Device Custom Date1	TIME_STAMP_CHANGED
Device Custom Date1 Label	"TIME STAMP CHANGED"
Device Custom String 1	RULE_NAME
Device Custom String 2	SITE_NAME
Device Custom String 6	GROUP_NAME
Device Direction	TRAFFIC_DIRECTION (0=Unknown, 1=Inbound, 2=Outbound)
Device Domain	DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Symantec'
End Time	EVENT_TIME
File Path	APP_NAME
Message	EVENT_DESC
Name	EVENT_ID (401-Raw Ethernet)
Old File Name	GROUP_NAME
Old File Permission	agent-packet
Old File Type	GROUP_TYPE
Source Address	LOCAL_HOST_IP   REMOTE_HOST_IP
Source Host Name	HOST_NAME   REMOTE_HOST_NAME
Source Mac Address	LOCAL_HOST_MAC   REMOTE_HOST_MAC
Source Port	LOCAL_PORT   REMOTE_PORT
Source User Name	USER_NAME

## Agent Security Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 0..3; High = 4..7; Medium = 8..11; Low = 12..15
Base Event Count	REPETITION
Device Action	EVENT_DESC
Device Custom Date 1	TIME_STAMP_CHANGED (Changed Time)
Device Custom Number 1	HACK_TYPE (Hack Type)
Device Custom Number 2	EVENT_DESC (SID)
Device Custom Number 3	SEQ_ID (Sequence ID)
Device Custom String 2	SITE_NAME (Site Name)
Device Custom String 3	INTRUSION_PAYLOAD_URL ('Intrusion Payload URL')
Device Custom String 4	HOST_NAME (Host Name)
Device Custom String 5	LOCATION_NAME (Location Name)
Device Custom String 6	GROUP_NAME (Group Name)
Device Direction	TRAFFIC_DIRECTION (One of (0=Unknown, 1=Inbound, 2=Outbound))

ArcSight ESM Field	Device-Specific Field
Device Domain	DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	EVENT_TIME
Device Severity	SEVERITY
Device Vendor	'Symantec'
Device Version	AGENT_VERSION
End Time	END_TIME
External Id	AGENT_SECURITY_LOG_IDX
File Name	APP_NAME
Message	EVENT_DESC
Name	EVENT_ID
Old File Name	GROUP_NAME
Old File Permission	agent-security
Old File Type	GROUP_TYPE
Protocol	One of (NETWORK_PROTOCOL (One of (2=TCP, 3=UDP, 4=ICMP)), 'OTHERS')
Request Url	INTRUSION_URL
Start Time	BEGIN_TIME

## Agent Traffic Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 0..3; High = 4..7; Medium = 8..11; Low = 12..15
Base Event Count	REPETITION
Device Custom Date 1	Device Custom Date 1
Device Custom String 1	RULE_NAME (Rule Name)
Device Custom String 2	SITE_NAME (Site Name)
Device Custom String 6	GROUP_NAME
Device Direction	TRAFFIC_DIRECTION (0=Unknown, 1=Inbound, 2=Outbound)

ArcSight ESM Field	Device-Specific Field
Device Domain	DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	EVENT_TIME
Device Severity	SEVERITY
Device Vendor	'Symantec'
Device Version	AGENT_VERSION
End Time	END_TIME
File Name	APP_NAME
Message	BLOCKED (All of (one of '1', 'Blocked', 'Passed'), 'traffic per rule', RULE_NAME)
Name	BLOCKED (All of (one of '1', 'Blocked', 'Passed'), 'traffic')
Old File Name	GROUP_NAME
Old File Permission	agent-traffic
Old File Type	GROUP_TYPE
Protocol	NETWORK_PROTOCOL (One of 2=TCP, 3=UPD, 4=ICMP, OTHERS)
Start Time	BEGIN_TIME

## Alerts Mappings v14.2

ArcSight ESM Field	Device-Specific Field
additionaldata.LOCATION_NAME	LOCATION_NAME
Destination Address	IP_ADDR1
Destination Host Name	COMPUTER_NAME
Destination Mac Address	MAC_ADDR
Destination NtDomain	COMPUTER_DOMAIN_NAME
Destination User Name	CURRENT_LOGIN_USER
Device Action	ACTUALACTION

# Configuration Guide for Symantec Endpoint Protection DB SmartConnector

## Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	TIME_STAMP_CHANGED
Device Custom Number 1	NOOFVIRUSES
Device Custom Number 2	THREATS
Device Custom Number 3	INFECTED
Device Custom String 1	VIRUSNAME
Device Custom String 2	REQUESTEDACTION
Device Custom String 3	SECONDARYACTION
Device Custom String 4	MESSAGE2
Device Custom String 5	BOTH(HPP_APP_NAME,HPP_APP_TYPE)(TruScan Detected Application)
Device Event Category	SOURCE
Device Event Class ID	ALERT_IDX
Device Host Name	PARENT_SERVER_NAME
Device Product	Endpoint Protection'
Device Receipt Time	ALERTINSERTTIME
Device Severity	HID_LEVEL
Device Vendor	Symantec'
Device Version	14.2
External ID	SCAN_ID
File Hash	HPP_APP_HASH
File ID	DOMAIN_ID
File Name	FILEPATH
File Path	FILEPATH
File Permission	USER_DOMAIN_NAME
File Type	CLIENT_TYPE
Message	DESCRIPTION
Name	ALERT
Old File Hash	KERNEL
Old File ID	STATUS
Old File Name	CLIENT_GROUP
Old File Path	Both (OPERATION_SYSTEM, SERVICE_PACK)

ArcSight ESM Field	Device-Specific Field
Old File Permission	Alerts
Old File Permission	alerts
Old File Type	CLIENT_TYPE
Request Context	GROUP_ID
Request Cookies	DOWNLOADER
Request Method	CLIENT_GROUP
Source User ID	UUID
Source Address	SOURCE_COMPUTER_IP
Source Host Name	SOURCE_COMPUTER_NAME
Source User Name	USER_NAME

## Alerts Mappings v14.x

ArcSight ESM Field	Device-Specific Field
Destination Address	IP_ADDR1
Destination Host Name	COMPUTER_NAME
Destination NtDomain	COMPUTER_DOMAIN_NAME
Destination User Name	CURRENT_LOGIN_USER
Device Action	ACTUALACTION
Device Custom Date 1	TIME_STAMP_CHANGED
Device Custom Number 1	NOOFVIRUSES
Device Custom Number 2	THREATS
Device Custom Number 3	INFECTED
Device Custom String 1	VIRUSNAME
Device Custom String 2	REQUESTEDACTION
Device Custom String 3	SECONDARYACTION
Device Custom String 4	MESSAGE2
Device Custom String 5	Both(HPP_APP_NAME,HPP_APP_TYPE) (TruScan Detected Application)
Device Event Category	SOURCE
Device Event Class ID	ALERT_IDX

# Configuration Guide for Symantec Endpoint Protection DB SmartConnector

## Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Host Name	PARENT_SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	ALERTINSERTTIME
Device Vendor	'Symantec'
Device Version	14
Event.oldFilePermission	Alerts
External ID	SCAN_ID
File Hash	HPP_APP_HASH
File Id	DOMAIN_ID
File Name	FILEPATH
File Path	FILEPATH
File Permission	USER_DOMAIN_NAME
File Type	CLIENT_TYPE
Message	DESCRIPTION
Name	ALERT
Old File Hash	KERNEL
Old File ID	STATUS
Old File Name	CLIENT_GROUP
Old File Path	Both (OPERATION_SYSTEM, SERVICE_PACK)
Old File Permission	alerts
Old File Type	CLIENT_TYPE
Request Context	GROUP_ID
Request Cookies	DOWNLOADER
Request Method	CLIENT_GROUP
Source Address	SOURCE_COMPUTER_IP
Source Host Name	SOURCE_COMPUTER_NAME
Source User ID	UUID
Source User Name	USER_NAME



## Alerts Mappings v12.x

ArcSight ESM Field	Device-Specific Field
Destination Address	IP_ADDR1
Destination Host Name	COMPUTER_NAME
Destination User Name	CURRENT_LOGIN_USER
Device Action	ACTUALACTION
Device Custom Number 1	NOOFVIRUSES
Device Custom Number 2	THREATS
Device Custom Number 2	THREATS
Device Custom Number 3	INFECTED
Device Custom String 1	VIRUSNAME
Device Custom String 2	REQUESTEDACTION
Device Custom String 3	SECONDARYACTION
Device Custom String 4	MESSAGE2
Device Custom String 5	Both(HPP_APP_NAME,HPP_APP_TYPE)
Device Custom String 6	CATEGORY_DESC when ALERT_IDX is 1 or 2
Device Event Category	SOURCE
Device Event Class ID	One of (ALERT_IDX, both (ALERT_IDX VIRUS_TYPE) when ALERT_IDX is 1 or 2)
Device Host Name	PARENT_SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	ALERTINSERTTIME
Device Vendor	'Symantec'
Device Version	12
External ID	SCAN_ID
File Hash	HPP_APP_HASH
File Id	DOMAIN_ID
File Name	FILEPATH
File Path	FILEPATH

ArcSight ESM Field	Device-Specific Field
File Type	CLIENT_TYPE
Message	DESCRIPTION
Name	ALERT
Old File	GROUP_NAME
Old File Path	Both (OPERATION_SYSTEM, SERVICE_PACK)
Old File Permission	alerts
Old File Type	GROUP_TYPE
Request Method	CLIENT_GROUP
Source Address	SOURCE_COMPUTER_IP
Source Host Name	SOURCE_COMPUTER_NAME
Source User Name	USER_NAME

## NAC Client Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	ACTION
Device Custom Number 1	TIME_STAMP
Device Custom Number 2	PERIOD
Device Custom String 1	ENFORCER_ID
Device Custom String 2	ENFORCER_TYPE
Device Custom String 3	SITE_NAME
Device Custom String 4	SITE_ID
Device Custom String 5	CLIENT_ID
Device Custom String 6	DOMAIN_ID
Device Event Class ID	EVENT_ID
Device Product	'Network Access Control'
Device Receipt Time	EVENT_TIME
Device Vendor	'Symantec'
Message	EVENT_DESC
Name	EVENT_DESC

ArcSight ESM Field	Device-Specific Field
Old File Name	GROUP_NAME
Old File Permission	nac-client
Old File Type	GROUP_TYPE
Source Host Name	REMOTE_HOST
Source MAC Address	REMOTE_HOST_MAC

## NAC System Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Device Severity 3; High = Device Severity 2; Medium = Device Severity 1; Low = Device Severity 0
Device Custom Number 1	TIME_STAMP
Device Custom String 1	ENFORCER_ID
Device Custom String 2	ENFORCER_TYPE
Device Custom String 3	SITE_NAME
Device Custom String 4	SITE_ID
Device Custom String 5	SITE_TYPE
Device Custom String 6	ENFORCER_TYPE (0 = Gateway Enforcer, 1 = LAN Enforcer, 2 = DHCP Enforcer, 3 = Integrated Enforcer, 4 = NAP Enforcer, 5 = Peer-to-Peer Enforcer)
Device Custom String 6 Label	Group Name
Device Event Class ID	EVENT_ID
Device Product	'Network Access Control'
Device Receipt Time	EVENT_TIME
Device Severity	SEVERITY
Device Vendor	'Symantec'
Message	EVENT_DESC
Name	EVENT_DESC
Old File Permission	nac-system
Old File Type	ENFORCER_TYPE (0 = Gateway Enforcer, 1 = LAN Enforcer, 2 = DHCP Enforcer, 3 = Integrated Enforcer, 4 = NAP Enforcer, 5 = Peer-to-Peer Enforcer)

## NAC Traffic Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	REPETITION
Destination Address	REMOTE_HOST_IP or LOCAL_HOST_IP (depending upon TRAFFIC_DIRECTION)
Destination Port	REMOTE_PORT or LOCAL_PORT (depending upon TRAFFIC_DIRECTION)
Device Custom Date 1	EVENT_TIME
Device Custom Number 1	TIME_STAMP
Device Custom String 1	ENFORCER_ID
Device Custom String 2	ENFORCER_TYPE
Device Custom String 3	SITE_NAME
Device Custom String 4	SITE_ID
Device Custom String 5	CLIENT_ID
Device Custom String 6	GROUP_NAME
Device Direction	TRAFFIC_DIRECTION (0 = Unknown, 1 = Inbound, 2 = Outbound)
Device Event Class ID	EVENT_ID
Device Product	'Network Access Control'
Device Receipt Time	TIME_STAMP
Device Vendor	'Symantec'
End Time	END_TIME
Old File Name	GROUP_NAME
Old File Permission	nac-traffic
Old File Type	GROUP_TYPE
Protocol	NETWORK_PROTOCOL ("1=OTHERS", "2-TCP", "3=UDP", "4=ICMP")
Source Address	LOCAL_HOST_IP or REMOTE_HOST_IP (depending upon TRAFFIC_DIRECTION)
Source Port	LOCAL_PORT or REMOTE_PORT (depending upon TRAFFIC_DIRECTION)
Start Time	BEGIN_TIME

## Notification Alert Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	DELETED (0=Not deleted, 1=Deleted)
Device Custom Date 1	ACKNOWLEDGED_TIME
Device Custom String 1	VIRUS
Device Custom String 2	SOURCE
Device Custom String 3	ACTACTION (1=Quarantined, 3=Deleted, 4=Left alone, 5=Cleaned, 6=Cleaned or macros deleted, 14=Pending repair, 15=Partially repaired, 16=Process termination pending restart, 17=Excluded, 19=Cleaned by deletion, 20=Access denied, 21=Process terminated, 22=No repair available, 23=All actions failed, 98=Suspicious)
Device Custom String 4	ACKNOWLEDGED (0=Not acknowledged, 1=Acknowledged)
Device Custom String 5	ACKNOWLEDGED_USERID
Device Custom String 6	EMAILSUBJECT
Device Event Category	CATEGORY (-1_Unknown, >=5_Very Severe, >=4_Severe, >= 3_Moderate, >=2_Low, >=1_Very Low, >=-1_All, _)
Device Event Class ID	TYPE
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP
Device Vendor	'Symantec'
End Time	ALERTDATETIME
Message	MSG
Name	SUBJECT
Old File Permission	notificationalerts
Old File Type	CLIENTGROUP

## Scans Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	COMPUTER_NAME
Destination User Name	CURRENT_LOGIN_USER

## Configuration Guide for Symantec Endpoint Protection DB SmartConnector

### Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Action	DELETED (0=Not deleted, 1=Deleted)
Device Custom Date 1	TIME_STAMP_CHANGED ('Change Time')
Device Custom Number 1	TOTALFILES ('Files scanned')
Device Custom Number 2	THREATS ('Threats')
Device Custom Number 3	INFECTED ('Files infected')
Device Custom String 1	BIOS_SERIALNUMBER ('BIOS Serial Number')
Device Custom String 2	OS_FUNCTION ('Operating System Function')
Device Custom String 3	STATUS ('Scan status')
Device Custom String 4	ATP_DEVICE_ID ('Advance Threat Protection Device ID')
Device Custom String 5	TELEMETRY_MID ('MonitoringID')
Device Custom String 6	TELEMETRY_HWID ('HardwareID')
Device Event Category	One of('Active Scan', 'Full Scan', 'Admin-defined Scan', SCAN_TYPE)
Device Event Class ID	'Scanning System'
Device Host Name	PARENT_SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP
Device Vendor	'Symantec'
End Time	STOPDATETIME
Event Outcome	STATUS
External ID	USN
Message	MESSAGE2
Name	MESSAGE1
Old File Name	GROUP_NAME
Old File Permission	scans
Old File Type	GROUP_TYPE
Source User Name	One of (CLIENTUSER1, CLIENTUSER2)
Start Time	STARTDATETIME

## Server Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 1000 – 10000; High = 900 – 999; Medium = 800 – 899; Low = 700 – 799; Very Low = 400 – 699
Device Custom Number 1	TIME_STAMP
Device Custom Number 3	ERROR_CODE
Device Custom String 1	STACK_TRACE
Device Custom String 6	Group Name
Device Event Class ID	EVENT_ID
Device Product	'Endpoint Protection'
Device Receipt Time	TIME_STAMP
Device Severity	SEVERITY
Device Vendor	'Symantec'
Device Version	null
Message	EVENT_DESC
Old File Permission	server
Old File Type	TYPE

## Server-Admin Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 1000..10000; High = 900..999; Medium = 800..899; Low = 400..799
Destination User Name	ADMIN_NAME
Device Custom String 3	STACK_TRACE
Device Custom String 4	DOMAIN_ID
Device Custom String 5	SITE_ID
Device Custom String 6	SERVER_ID
Device Event Class ID	EVENT_ID
Device Product	'Endpoint Protection'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	TIME_STAMP
Device Severity	SEVERITY
Device Vendor	'Symantec'
Device Version	null
External ID	USN
Message	EVENT_DESC
Old File Permission	server-admin
Old File Type	TYPE
Reason	ERROR_CODE

## Server Client Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	SITE_NAME
Device Custom String 6	GROUP_NAME
Device Domain	SERVER_DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	EVENT_TIME
Device Vendor	'Symantec'
Name	EVENT_ID
Old File Name	GROUP_NAME
Old File Permission	server-client
Old File Type	TYPE
Source Host Name	HOST_NAME
Source NT Domain	DOMAIN_NAME
Source User Name	USER_NAME



## Server Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	TIME_STAMP_CHANGED (Changed Time)
Device Custom String 2	SITE_NAME (Site Name)
Device Custom String 6	TYPE
Device Custom String 6 Label	Group Name
Device Domain	DOMAIN_NAME
Device Event Class ID	Both ('audit:', EVENT_ID)
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	EVENT_TIME
Device Vendor	'Symantec'
Message	EVENT_DESC
Name	EVENT_ID (0=Policy added, 1=Policy deleted, 2=Policy edited, 3=Add shared policy upon system install, 4=Add shared policy upon system upgrade, 5=Add shared policy upon domain creation)
Old File Permission	server-policy
Old File Type	TYPE
Source Host Name	SERVER_NAME
Source NT Domain	DOMAIN_NAME

## Virus Category Mappings

ArcSight ESM Field	Device-Specific Field
File Type	blank or concatenate("Group Name: ",group_type)
Agent (Connector) Severity	Very High=Very Severe, High=Severe, Medium=Moderate, Low=Unknown,Very Low,Low
Device Action	deleted (0=Not deleted, 1=Deleted)
Device Custom String 1	Security Risk (stealth,"0=No rating","1=Low","2=Low","3=Medium","-1=Not applicable","High")

# Configuration Guide for Symantec Endpoint Protection DB SmartConnector

## Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Skill Level (removal,"0=No rating","1=Low","2=Low","3=Medium","-1=Not applicable","High")
Device Custom String 3	Computer Performance (performance,"0=No rating","1=Low","2=Low","3=Medium","-1=Not applicable","High")
Device Custom String 4	Privacy Level (privacy,"0=No rating","1=Low","2=Low","3=Medium","-1=Not applicable","High")
Device Custom String 5	Dependency component (dependency,"0=No rating","1=Low","2=Low","3=Medium","-1=Not applicable"),"High")
Device Custom String 6	Both (catDes (0 = Viral, 1 = Non-viral malicious, 2 = Malicious, 3 = Antivirus heuristic, 4 = Security risk, 5 = Hack tool, 6 = Spyware, 7 = Trackware, 8 = Dialer, 9 = Remote access, 10 = Adware, 11 = Jokeware, 12 = Client compliancy, 13 = Generic load point, 14 = Proactive Threat Scan - Heuristic, 15 = Cookie)), Viral)
Device Custom String 6 Label	Group Name
Device Event Class ID	vrType
Device Host Name	_DB_HOST
Device Product	'Endpoint Protection'
Device Receipt Time	timestamp
Device Severity	vrCat (-1=Unknown, 1=Very low, 2=Low, 3=Moderate, 4=Severe, 5=Very Severe)
Device Vendor	'Symantec'
Device Version	Unknown
End Time	discovered
File Name	blank or concatenate("Group Name: ",group_name)
Message	translation
Name	One of(virusname, Unknown Signature)
Old File Permission	virus-category
Old File Type	Both (catDes (0 = Viral, 1 = Non-viral malicious, 2 = Malicious, 3 = Antivirus heuristic, 4 = Security risk, 5 = Hack tool, 6 = Spyware, 7 = Trackware, 8 = Dialer, 9 = Remote access, 10 = Adware, 11 = Jokeware, 12 = Client compliancy, 13 = Generic load point, 14 = Proactive Threat Scan - Heuristic, 15 = Cookie)), Viral)

# Actions

-1	Action Failed
1	Quarantined
2	Renamed
3	Deleted
4	Left alone
5	Cleaned
6	Cleaned or Macros Deleted
7	Saved
9	Move Back
10	Rename Back
11	Undo
12	Bad
13	Backup
14	Pending Repair
15	Partially repaired
16	Reboot Pending
17	Exclude
18	Reboot Processing
19	Cleaned by deletion
20	Access Denied
21	Process Terminated
22	No Repair Available
23	No Action Taken
98	Suspicious
99	Details Pending
100	IDS block
101	FW violation
110	CALDetection

111	ForcedDetection
1000	ForcedHashDetection
200	Attachment stripped
500	Not applicable

## Alerts

1	Virus found
2	Security risk found
3	FW Violation Event
4	IDS Event
5	CAL Evemnt
6	Forced Detection Event
7	Detection Whitelisted
8	Potential fisk found
9	Risk submitted

## Categories

0	Viral
1	Non-Viral malicious
2	Malicious
3	Antivirus - Heuristic
4	Security risk
5	Hack tool
6	Spyware
7	Trackware
8	Dialer
9	Remote access
10	Adware
11	Jokeware
12	Client compliancy
13	Generic load point
14	Proactive Threat Scan - Heuristic
15	Cookie

# 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`. please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to receive events.

**Why aren't all of the generated SEP anti-virus events sent to ArcSight?**

This problem can occur if a locale other than English is used in virus names returned from Symantec Endpoint Protection. Even though ESM and Symantec support multiple languages, virus names as returned data for a query are restricted to an English-only translation to avoid multiple events sharing the same `virusname_idx` value. The connector will only retrieve one value and leave out the others. Contact Support if languages other than English are needed.



# 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 Symantec Endpoint Protection DB SmartConnector (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](mailto:MFI-Documentation-Feedback@opentext.com).

We appreciate your feedback!