



Micro Focus Security ArcSight Connectors

SmartConnector for Symantec Endpoint Protection DB

Configuration Guide

July 18, 2018

Configuration Guide

SmartConnector for Symantec Endpoint Protection DB

July 18, 2018

Copyright © 2003 – 2018 Micro Focus and its affiliates and licensors.

Warranty

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

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Trademark Notices

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

Revision History

Date	Description
07/18/2018	Updated event mappings for agent-behavior, virus-category and alerts.
02/21/2018	Version 11 of Symantec Endpoint Protection DB is no longer supported due to end of support by the vendor.
10/17/2017	Added Old File Name, Old File Type, and Old File Permission mappings for group names and types. Added encryption parameters to Global Parameters.
09/15/2017	Added troubleshooting information about English-language only support for virus names. Added mappings in the Alerts Events Mappings tables (v12 and v14) for collecting OS information.
07/15/2017	Added v14.0 support for Anti-Virus and Anti-Spyware Protection Events.
05/15/2017	Added v14.0 support for Network Threat Protection, Scan, Notification Alert, and Server Policy Events.
04/17/2017	Added v14.0 support for System Events.
03/15/2017	Updated to support v14 events in the following mapping tables: Server Admin Log, Behavior, and Virus. Updated the Agent mappings table to extra support v12 events. Added "Device Version" support to the Traffic, Behavior, Server-Admin, and Virus mappings. Added support for File Path and File Hash to the Alerts mappings.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Updated Security and Traffic mappings. Removed support for ODBC drivers and embedded database due to Java 8 implementation.

SmartConnector for Symantec Endpoint Protection DB

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

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.

Configuration

Symantec Endpoint Protection collects and reads the 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. Privilege to connect to and select from the database is required.

Minimal Privileges Required for Connector to Access Files from DB

To configure the SQL account to connect with the minimum permissions/tables required:

- 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**.

Configure 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.

Download and Install a JDBC Driver

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

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



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

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

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

Install the driver.

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

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


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

- 1 From the Connector Appliance/ArcSight Management Center, select **Setup -> Repositories**.
- 2 Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
- 3 Click **Upload to Repository**.
- 4 From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
- 5 Retain the default selection and click **Next**.
- 6 Click **Upload** and locate and select the `.jar` file you downloaded in step 3 of SmartConnector Installation.
- 7 Click **Submit** to add the specified file to the repository and click **Next** to continue.
- 8 After adding all files you require, click **Next**.
- 9 In the **Name** field, enter a descriptive name for the zip file (`JDBCdriver`, for example). Click **Next**.
- 10 Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
- 11 To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
- 12 Select the container or containers into which the driver is to be uploaded; click **Next**.

- 13 Click **Done** to complete the process.
- 14 Add the connector through the Connector Appliance/ArcSight Management Center interface; see the *Connector Appliance/ArcSight Management Center Online Help* for detailed information. Descriptions of parameters to be entered during connector configuration are provided in the "Install the SmartConnector" section of this guide.


Configure the JDBC Driver and Windows Authentication

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

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

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

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

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

- 2 Go to `$ARCSIGHT_HOME\current\bin` and double-click `runagentsetup` to continue the SmartConnector installation.
- 3 When entering the connector parameters, in the **JDBC Database URL** field, append `;integratedSecurity=true` to the end of the URL string.

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

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

- 4 Complete the remaining connector wizard configuration steps.

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

Install the SmartConnector

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

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

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

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

- 1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

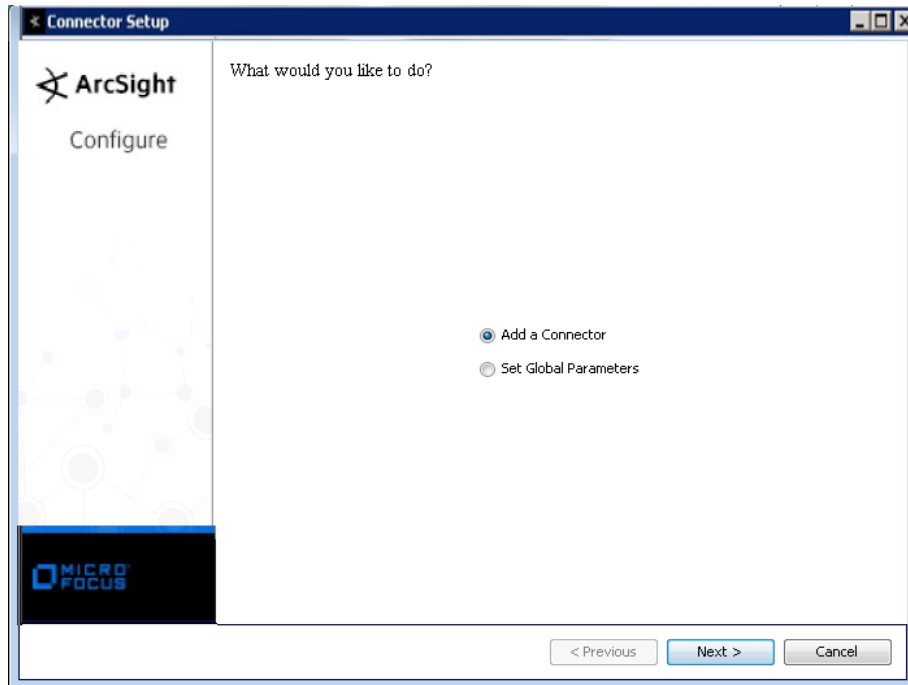
Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder

Pre-Installation Summary

Installing...

- 3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Download SQL Server JDBC Driver

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

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

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.

Parameter	Setting
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

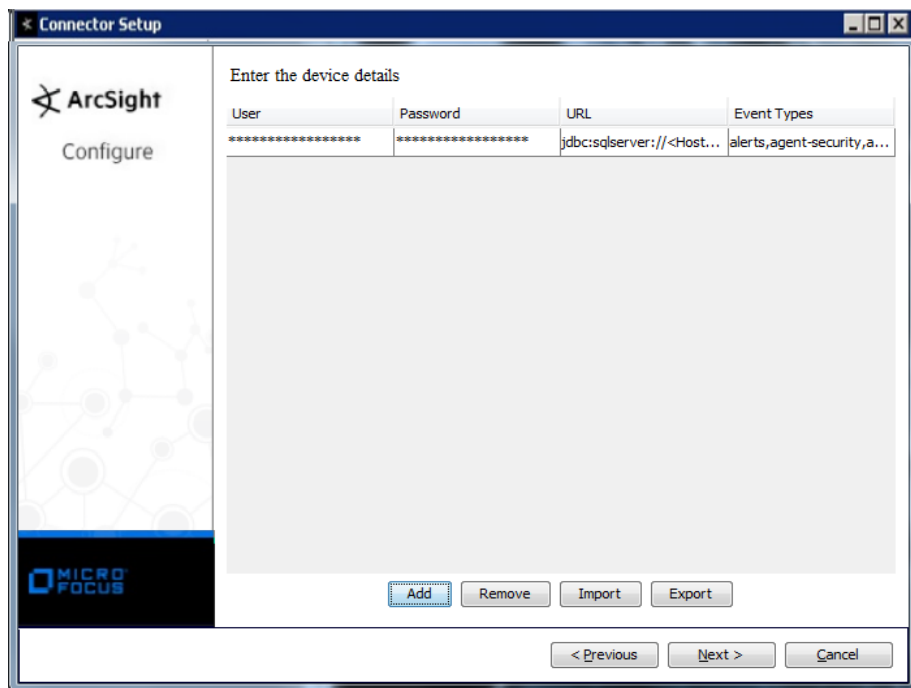
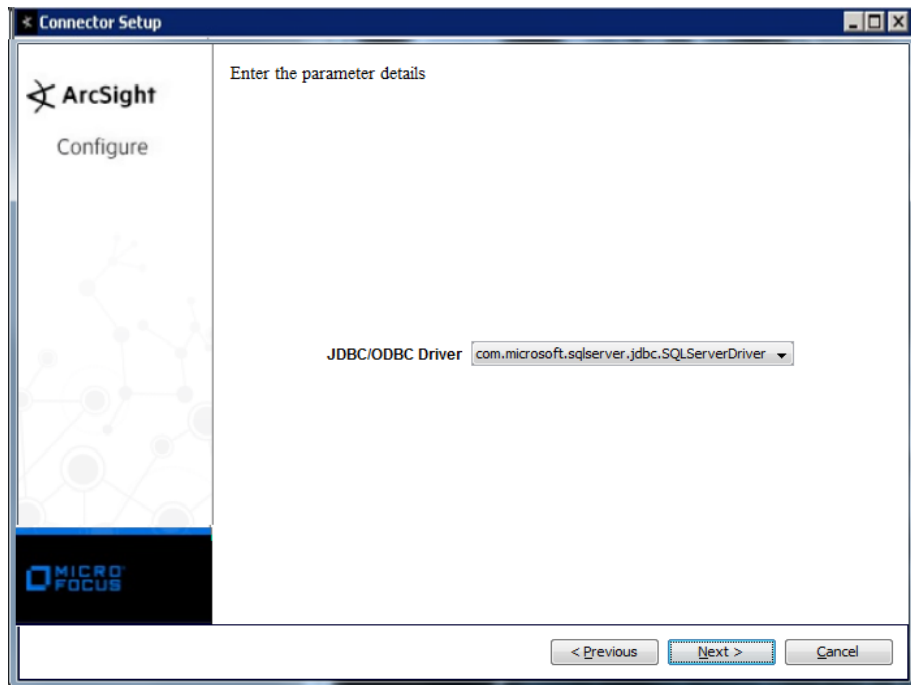
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Symantec Endpoint Protection DB** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
JDBC Driver	Select 'com.microsoft.sqlserver.jdbc.SQLServerDriver'
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.

Parameter	Description
JDBC Database URL	The following default value is shown for JDBC drivers: 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>;1433;DatabaseName=<MS SQL Server Database Name>'. Substitute actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.
Event Types	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. NOTE: If an event type for which no data exists is entered, the error message "Database version could not be detected" is displayed.

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the SmartConnector User's Guide for more information.

Select a Destination

- 1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- 2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
- 3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

- 1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
- 3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
- 4 Click **Next** on the summary window.

- 5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.



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

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

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

ArcSight ESM Field	Device-Specific Field
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
External ID	LOG_IDX
Message	EVENT_DESC
Name	One of (EVENT_DESC, EVENT_SOURCE)
Old File Name	GROUP_NAME
Old File Permission	agent
Old File Type	GROUP_TYPE

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 Name	CALLER_PROCESS_NAME
Destination User Name	USER_NAME
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
File Size	FILE_SIZE
Name	DESCRIPTION
Old File Name	GROUP_NAME
Old File Permission	agent-behavior

ArcSight ESM Field	Device-Specific Field
Old File Type	GROUP_TYPE
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
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)

ArcSight ESM Field	Device-Specific Field
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))
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)
Device Domain	DOMAIN_NAME
Device Event Class ID	EVENT_ID
Device Host Name	SERVER_NAME
Device Product	'Endpoint Protection'

ArcSight ESM Field	Device-Specific Field
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=UDP, 4=ICMP, OTHERS)
Start Time	BEGIN_TIME

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
Device Host Name	PARENT_SERVER_NAME
Device Product	'Endpoint Protection'
Device Receipt Time	ALERTINSERTTIME
Device Vendor	'Symantec'
Device Version	14
External ID	SCAN_ID
File Hash	HPP_APP_HASH
File Id	DOMAIN_ID
File Name	FILEPATH

ArcSight ESM Field	Device-Specific Field
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 Path	Both (OPERATION_SYSTEM, SERVICE_PACK)
Old File Permission	alerts
Old File Type	GROUP_TYPE
Request Context	GROUP_ID
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

ArcSight ESM Field	Device-Specific Field
File Hash	HPP_APP_HASH
File Id	DOMAIN_ID
File Name	FILEPATH
File Path	FILEPATH
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
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
--------------------	-----------------------

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

ArcSight ESM Field	Device-Specific Field
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
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')

ArcSight ESM Field	Device-Specific Field
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'
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)

ArcSight ESM Field	Device-Specific Field
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
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")
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
Message	translation
Name	One of(virusname, Unknown Signature)
Old File Permission	virus-category

ArcSight ESM Field	Device-Specific Field
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`.

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.