Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Sophos Anti-Virus DB SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for Sophos Anti-Virus DB SmartConnector

Configuration Guide for Sophos Anti-Virus DB SmartConnector

This guide provides information for installing the SmartConnector for Sophos Anti-Virus DB and configuring the database 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 SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

Sophos Anti-Virus detects and cleans up viruses, Trojans, worms, and spyware, as well as adware and other potentially unwanted applications. The Host Intrusion Prevention System (HIPS) technology protects computersfrom suspicious files and rootkits, unidentified viruses, and suspicious behavior.

Configuration

For complete information about Sophos Anti-Virus logging, see *Sophos Endpoint Security and Control Help*.

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 to mssql-jdbc-9.4.0.jre8.jar.
- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

For more information and to download the MS SQL Server JDBC Driver, see aa937724

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 Micro Focus 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 `$ARCSIGHT_HOME/current/user/agent/lib`
5. (Optional) To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$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, as the upgrade process overwrites the $ARCSIGHT_HOME\jre\bin directory.

6. To add JDBC Driver to ArcMC or Connector Applicance, 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 as this file gets overwritten during the upgrade process.

   - Copy the `vjdbc.jar` and `commons-logging-1.1.jar` files to the SmartConnectorinstallation 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 **Sophos Anti-Virus DB** from the **Type** drop-down, then click **Next**.
11. Enter the following parameters to configure the SmartConnector, then click **Next**:

Parameter	Description
JDBC Driver	Select the `com.microsoft.sqlserver.jdbc.SQLServerDriver` driver.
URL	Enter: `jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name>`. Replace with the actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>. To configure JDBC Driver and Windows Authentication, add `;integratedSecurity=true` to the JDBC URL entry for the connection to your database. **Note:** The name or instance of the database configured at installation or audit time must be used. For example, `jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true`
User	Enter the login name of the database user with appropriate privilege.
Password	Enter the password assigned to the Database User.
Frequency	Enter how often the database is to be synchronized to the SmartConnector.

12. Select a destination and configure parameters.
13. Specify a name for the connector.
14. 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.
15. Select whether you want to run the connector as a service or in the standalone mode.
16. Complete the installation.
17. Run the SmartConnector.

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

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.

Sophos Anti-Virus Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High=100, 200, 700; High=250, 600; Medium=400, 500; Low=50, 300
Destination Address	IP Address
Destination DNS Domain	DNSName
Destination Host Name	Name
Destination NT Domain	DomainName
Device Action	ActionTaken
Device Address	_DB_HOST
Device Custom Date 1	ActionSubmittedAt
Device Custom Date 2	DealtWithAt
Device Custom Number 1	Priority
Device Custom String 1	ThreatName
Device Event Class ID	ThreatType
Device Product	'Sophos Anti-Virus'
Device Receipt Time	FirstDetectedAt
Device Severity	Status
Device Vendor	'Sophos'
Device Version	SAVVersion
Event Outcome	Status
External ID	EventID
File Name	FullFilePath
File Path	FullFilePath
Name	ThreatName

Sophos Threat Types, Actions, and Status Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High=Threat type not cleanable, Not cleanable, Cleanup failed; High=Full scan required, Cleanup timed out; Medium=Cleanup in progress, Restart required; Low=Resolved, Cleanable
Destination Address	IP Address
Destination DNS Domain	DNSName
Destination Host Name	Name
Destination NT Domain	DomainName
Device Action	ThreatAction
Device Address	_DB_HOST
Device Custom Date 1	ActionSubmittedAt
Device Custom Date 2	DealtWithAt
Device Custom Number 1	Priority
Device Custom String 1	ThreatName
Device Event Class ID	All of (ThreatType, ActionTaken)
Device Product	'Sophos Anti-Virus'
Device Receipt Time	FirstDetectedAt
Device Severity	ThreatStatus
Device Vendor	'Sophos'
Device Version	SAVVersion
Event Outcome	ThreatStatus
External ID	EventID
File Name	FullFilePath
File Path	FullFilePath
Message	All of (ThreatTypeDescription, ThreatStatus)
Name	All of (ThreatTypeDescription, ThreatAction)

Troubleshooting

"How can I keep the connector from losing events on shutdown?"

If the connector is shut down for some time, on active databases it means a lot of events that could choke the connector. The `preservestate` parameter can be used to avoid this event loss. This parameter is disabled by default.

To enable the `preservestate` parameter, locate the parameter in the `agent.properties` file, found after connector installation at `$ARCSIGHT_HOME\current\user\agent`, and change the `Value` from `false` to `true`. Click **OK** and restart the connector for your changes to take effect.

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection."

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The `preservestate` parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting `preservestate` to disabled (false) in the `agent.properties` file allows the connector to skip the old events and start from real time. The `agent.properties` file is located in the `$ARCSIGHT_HOME\current\user\agent` folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the connector uses. Versions 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar. Versions 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Sophos Anti-Virus DB SmartConnector (SmartConnectors 8.3.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!