Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for PureSight Content Filter 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

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

Configuration Guide for PureSight Content Filter DB SmartConnector

Configuration Guide for PureSight Content Filter DB SmartConnector

This guide provides information for installing the SmartConnector for PureSight Content Filter DB and configuring the device for database event log collection.

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

PureSight combines Internet filtering capabilities with powerful management tools to offer an Internet content-filtering solution. PureSight is based upon proprietary Artificial Content Recognition (ACR) technology. PureSight allows Internet usage policies to be defined, implemented, and modified.

Configuration

Because MySQL supports host-based access control, you might need to configure MySQL to allow connections from the host where the ArcSight PureSight SmartAgent is running.

Configuring Access to MySQL

To allow MySQL access, execute the following command in a MySQL prompt:

```
GRANT SELECT ON PureSightdb.* to MySQLuser@'agenthost' identified by
'MySQLpassword';
```

where the parameters are defined as follows:

Parameter	Description
PureSightdb	The name of the database used by PureSight
MySQLuser	The user that you created for the ArcSight SmartConnector to access the MySQL database
AgentHost	The host name (or IP address) of the host running the ArcSight SmartConnector (for testing puposes, you could use %, which means 'any host')
MySQLPassword	The password of the user you created for the ArcSight SmartConnector

Downloading the MySQL JDBC Driver

Download the MySQL JDBC driver based on the connector version that you are using:

- For connector versions 7.2.4 and later, download the latest MySQL JDBC Driver from: http://dev.mysql.com/downloads/connector/j
- For connector versions 7.2.3 and earlier, download the MySQL 5.0.8 JDBC Driver from: https://dev.mysql.com/downloads/connector/j/5.0.html
- For connector versions 7.14.0 and later, download the latest DB2 JDBC Driver from: https://www.ibm.com/support/pages/db2-jdbc-driver-versions-and-downloads

Installing the SmartConnector

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

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 appropriate jar file to `$ARCSIGHT_HOME\current\user\agent\lib`, where `$ARCSIGHT_HOME` refers to the connector install folder, such as `c:\ArcSight\SmartConnectors`.
5. To install on Connector Appliance/ArcSight Management Center, see Adding a JDBC Driver to the Connector Appliance/ArcSight Management Center.
6. From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.
7. Select **PureSight Content-Filter DB** from the **Type** drop-down, then click **Next**.
8. Enter the following SmartConnector paramenters, then click **Next**.

Parameter	Description
PureSight Database JDBC Driver	Database JDBC Driver.
PureSight Database URL	Database JDBC URL. Accept the default value jdbc:odbc:<DSN Name>, where <DSN Name> is the name of the ODBC connection to PureSight.
PureSight Database User	Database Username.
PureSight Database Password	Database password.

9. Select a destination and configure parameters.
10. Specify a name for the connector.
11. 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.
12. Select whether you want to run the connector as a service or in the standalone mode.
13. Complete the installation.
14. Run the SmartConnector.

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

Adding a JDBC Driver through the Connector Appliance/ArcMC

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.

PureSight Content Filter Field Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	0 = High; 1 = Medium; 2 = Low
Device Address	PURESIGHT_CF_IP
Device Custom Number 1	TABLE_NUMBER
Device Custom Number 2	LOG_ID
Device Event Class ID	BLOCK_CODE (0 = Block, 1 = Warn, 2 = Allow)
Device Host Name	PURESIGHT_CF_NAME
Device Product	'Platform'
Device Receipt Time	DATE_TIME_STAMP
Device Severity	BLOCK_CODE (0 = Block, 1 = Warn, 2 = Allow)
Device Vendor	'PureSight'
File Size	SIZE_IN_BYTES
Request URL	INTERNET_DOMAIN plus REMAINING_URL
Source Address	USER_IP
Source User Name	USER_NAME

Advanced Configuration

The SmartConnector for PureSight Content Filter DB not only follows the table but also the ID, which is reset to 0 every time a new table is created.

When `preservestate` is enabled, the connector remembers the current table being processed and the location or ID in the table. Therefore, if for some reason the connector is stopped and you restart it, the connector starts reading the events from the same table and location.

Three advanced configuration options relate to this function:

`preservestate`
Enable so that the connector will remember and preserve the state of processing.

`startattable`
Use to specify the table where processing is to resume.

`startatid`
Use to specify the ID within the table where processing is to resume.

For example:

```
preservestate=true
 startattable=-1
 startatid=-1
```

Any value greater than or equal to 0 is a valid value.

Any value less than 0, including -1, has a default meaning. For table, it means go to the last table or max table. For id, it means, go to the end of the table or max id in the table.

To configure these options, from the `$ARCSIGHT_HOME\current\user\agent` directory, edit the `agent.properties` file; change values as appropriate and save.

Troubleshooting

"When I use the latest MySQL JDBC driver, the connector does not receive events."

Connector versions 7.2.4 and later use the latest MySQL JDBC driver. For connector versions 7.2.3 and earlier, you will need the MySQL 5.0.8 JDBC Driver, which you can download from:

https://dev.mysql.com/downloads/connector/j/5.0.html

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 PureSight Content Filter 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!