



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for PureSight Content Filter
DB

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for PureSight Content Filter DB

November 30, 2016

Copyright © 2006 – 2016 Hewlett Packard Enterprise Development LP

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
06/30/2016	Updated MySQL JDBC driver information.
05/16/2016	Updated link for MySQL JDBC driver.
05/15/2012	Added new installation procedure.
02/15/2012	Added driver download information for Connector Appliance.
08/15/2011	Added information about downloading the MySQL driver.
02/11/2010	Added support for FIPS Suite B and CEF File transport.

SmartConnector for PureSight Content Filter DB

This guide provides information for installing the SmartConnector for PureSight Content Filter DB and configuring the device for database event log collection. PureSight Content Filter Version 4.6 is supported.

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 may find it necessary to configure MySQL to allow connections from the host where the ArcSight PureSight SmartAgent is running. 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

Install the SmartConnector

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

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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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

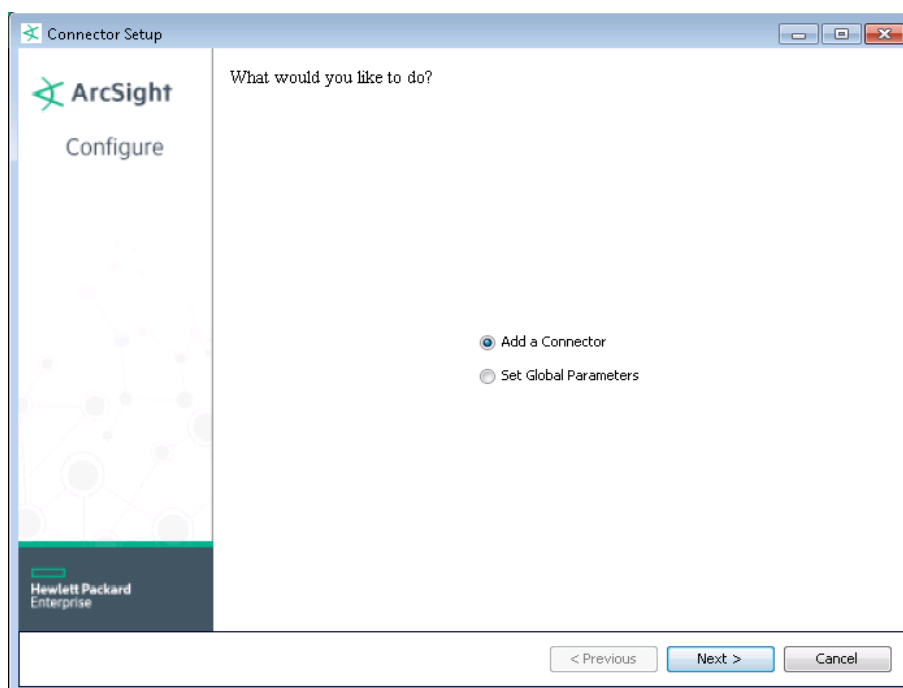
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the HPE 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 MySQL JDBC Driver

- 1 Click **Cancel** to leave the configuration wizard at this point.
- 2 The following steps are required when you use the MySQL JDBC driver, required for Connector Appliance/ArcSight Management Center and Linux systems.
 - A 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>

Install the driver.
 - B For software connectors, 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`. For Connector Appliance/ArcSight Management Center users, see "Add a JDBC Driver to the Connector Appliance/ArcSight Management Center" later in this guide.
 - C From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

Set Global Parameters (optional)

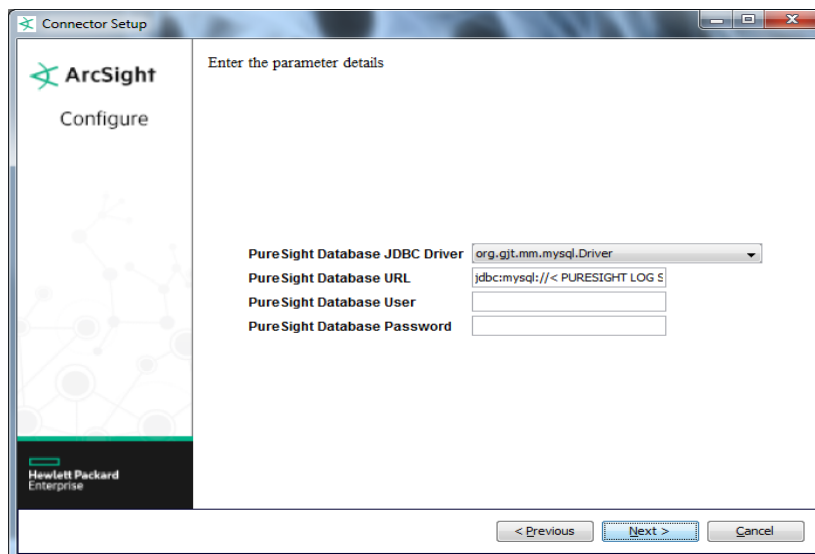
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' 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 'Disable'.
Set Remote Management	Set to 'Enable' 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 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	If 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. When both values are present, the initial setting is IPv4.

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 the "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 **PureSight Content-Filter DB** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, 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.

Select a Destination

- 1 The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)
- 2 Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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 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 some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.



Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

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

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.

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>