Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Raw Syslog Daemon

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Raw Syslog Daemon

November 30, 2016

Warranty

Restricted Rights Legend

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/14/2014	Added new configuration parameters to support minimal normalization for source and timestamp.
05/15/2012	Update for new installation procedure.
11/15/2011	First edition of this Configuration Guide.

SmartConnector for Raw Syslog Daemon

This guide provides information for installing the SmartConnector for Raw Syslog Daemon and configuring the device for event collection.

Product Overview

Although normalized data is faster and easier to parse and access, many IT professionals prefer having the raw data available for review, forensics, and litigation. In conjunction with the Raw Syslog connector destination, the SmartConnector for Raw Syslog Daemon lets you extract and collect raw syslog events from syslog servers using the TLS, Raw TCP, or UDP protocols.

Because this connector neither parses nor processes the raw syslog data, there are no mappings to ArcSight fields.

If you are transporting data to ArcSight Logger, you can use specific configuration parameters to provide minimal normalization of the syslog data (for source and timestamp).

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.

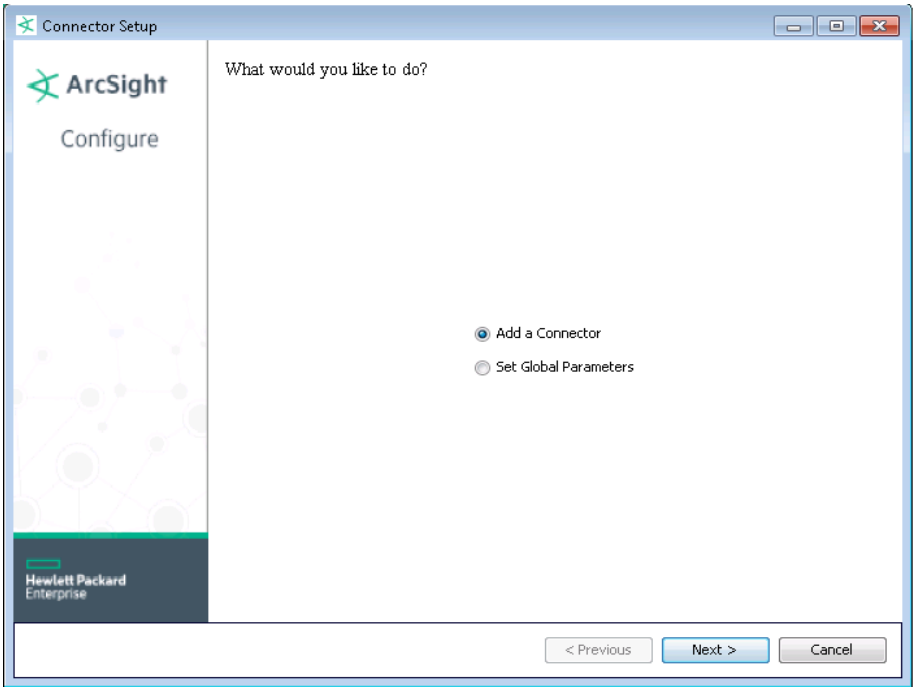
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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:



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:

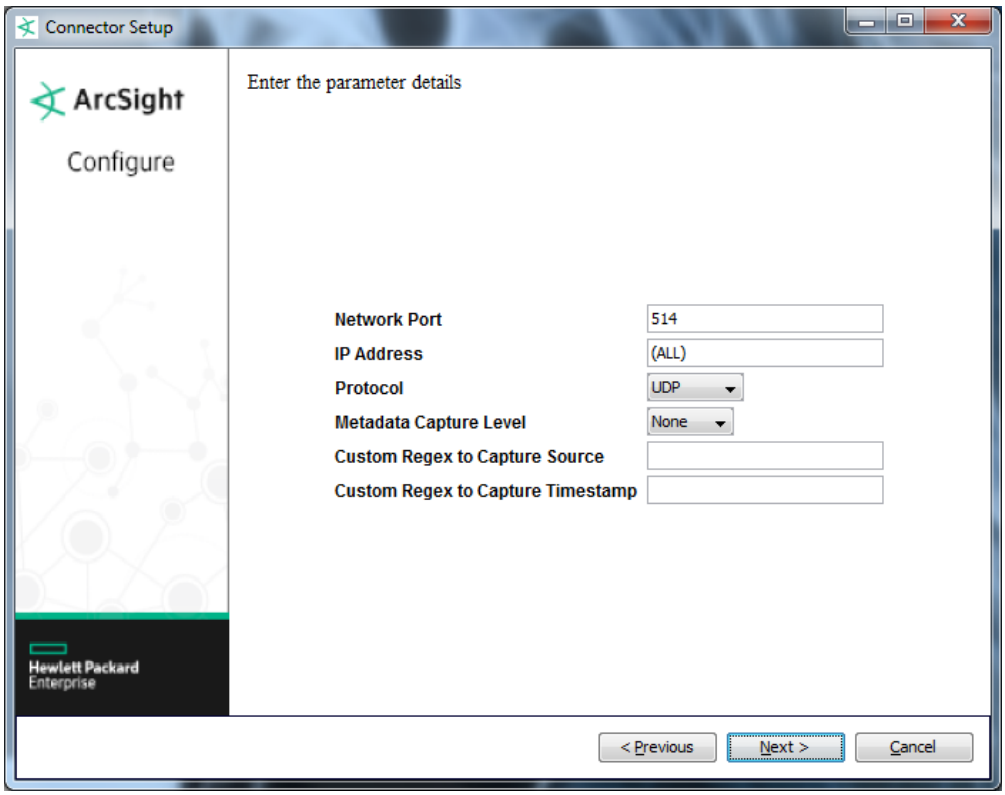
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote 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.

Global Parameter	Setting
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 **Raw Syslog Daemon** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



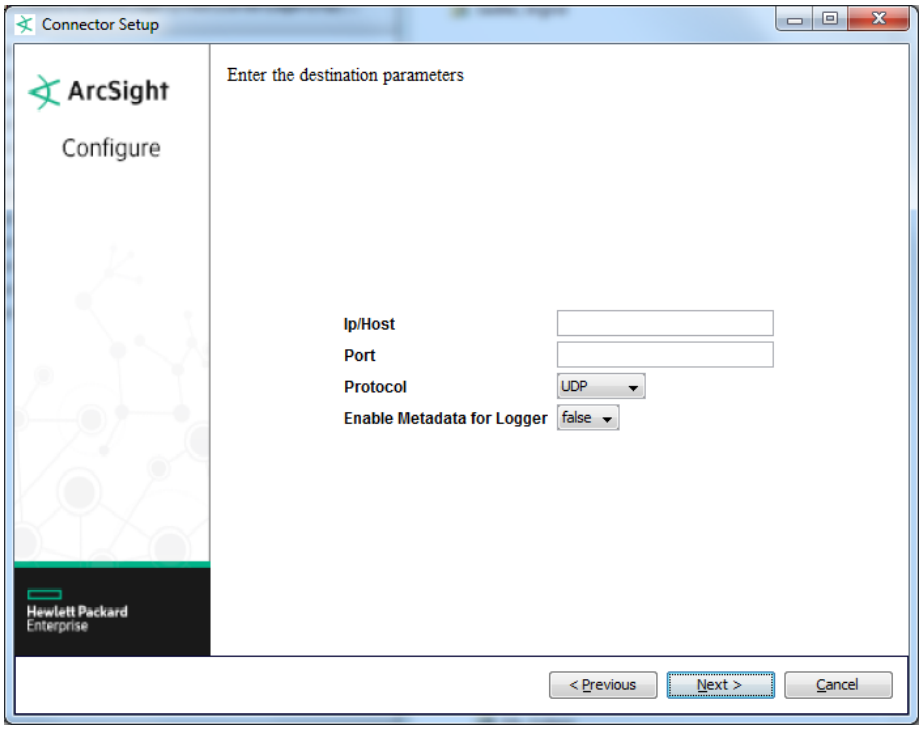
Parameter	Description
Network Port	Specify the port to which the connector is to listen for syslog events. The default is port 514.
IP Address	Enter the IP address of the device to which the connector is to listen exclusively, or accept the default value of (ALL) to bind to all available IP addresses.
Protocol	Select UDP, Raw TCP, or TLS as the protocol to be used by the connector to receive incoming messages. The default value is UDP.

Parameter	Description
Metadata Capture Level	Use if metadata (for source and timestamp) will be included in the outgoing messages to ArcSight Logger. Leave the default of None if you do not require this metadata be sent to ArcSight Logger. Otherwise, select one of these options: **Simple**: Uses the current machine timestamp and the actual IP address that was the source of the event. No parsing occurs. **Header:** Uses the timestamp and source information from the event message header. If that data cannot be derived, then the connector uses the Simple option. **Custom:** Uses the regular expressions provided in the Custom Regex to Capture Source and the Custom Regex to Capture Timestamp fields. If you specify a Metadata Capture Level of Custom, you must use at least one of these fields.
Custom Regex to Capture Source	Custom regular expression to capture source; the capturing group indicates the location of the source IP or host name. This regular expression needs to match the entire raw syslog event, and have at least one capturing group, which tells the connector how to find the source address. For example, this regular expression would find everything between the words “before” and “after:” .*?before(.*)after.* For the following event, that regular expression would capture the IP address 192.168.1.2: Hello there before192.168.1.2after and goodbye
Custom Regex to Capture Timestamp	Custom regular expression to capture timestamp; the capturing group indicates the location of the timestamp. Uses the parsing for the __parseMutableTimeStampSilently token operation. See the *ArcSight FlexConnector Developer’s Guide* for details on token operations.

Select a Destination

1 The next window asks for the destination type; make sure **Raw Syslog** 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 destination parameter values. Click **Next**.



Parameter	Description
Ip/Host	Enter the IP address or host name to which the connector is to send events.
Port	Specify the port to which the connector is to send events.
Protocol	Select either UDP, Raw TCP, or TLS as the protocol to be used by the connector to send events. The default value is UDP.
Enable Metadata for Logger	Select either true or false. If you select true, metadata about the source and timestamp is included in the outgoing message for ArcSight Logger, though you should only select this if you previously choose a level other than None for the Metadata Capture Level parameter.

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.

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*.

Run the SmartConnector

SmartConnectors can be installed and run in standalone 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 standalone 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 *SmartConnector User's Guide*.

To run all SmartConnectors installed in standalone 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.