Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for sFlow

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for sFlow

November 30, 2016

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

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.
05/16/2016	Updated mappings.
05/15/2015	Removed "InMon" from connector name.
09/30/2013	Added support for TippingPoint sflow.
06/30/2012	Added information about the sflowtool and support for Linux.
05/15/2012	First release of this connector.

SmartConnector for sFlow

This guide provides information for installing the SmartConnector for sFlow and configuring the device for event collection. sFlow version 5 and TippingPoint sflow (TP TOS 3.6) are supported.

Product Overview

sFlow is the leading, multi-vendor, standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources. sFlow supports traffic monitoring on Gigabit and higher-speed networks and provides scalability to allow one sFlow collector to monitor multiple sFlow agents.

sFlow has two components: an sFlow agent embedded in a switch, and a remote sFlow collector. The sFlow agent collects traffic statistics and packet information from the sFlow-enabled interfaces on the switch and encapsulates them into sFlow packets. When an sFlow packet buffer overflows, or an sFlow packet ages out (the aging time is one second), the sFlow agent sends the packet to the specified sFlow collector. The sFlow collector analyzes the sFlow packets and displays the results. sFlow has two sampling mechanisms:

- Flow sampling: Packet-based sampling, used to obtain packet content information.

- Counter sampling: Time-based sampling, used to obtain port traffic statistics.

The sflowtool is a component of the sFlow toolkit. For Windows, you can obtain the compiled sflowtool from the InMon website. For Linux, the sflowtool is part of the connector and is located in the `/bin/agent/InMon/sflowtool/linux` directory.

The sflowtool must be installed on a different box than the SmartConnector.

Use the following commands to specify where the packets are sent:

`c:\sflowtool -p <sflow agent listening port> -c <IP Address> -d <port number>` - for Windows

`./ sflowtool -p <sflow agent listening port> -c <IP Address> -d <port number>` - for Linux

Where `<IP Address>` is the IP address of the connector and `<port number>` is the port number of the connector.

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

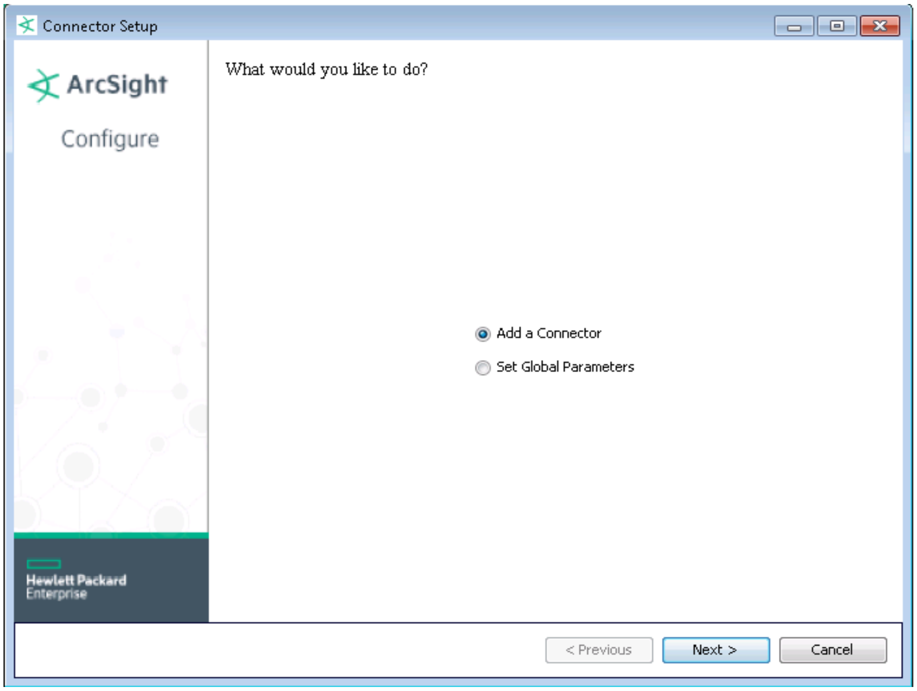
Install Core Software

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:



What would you like to do?

● Add a Connector

○ Set Global Parameters

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.

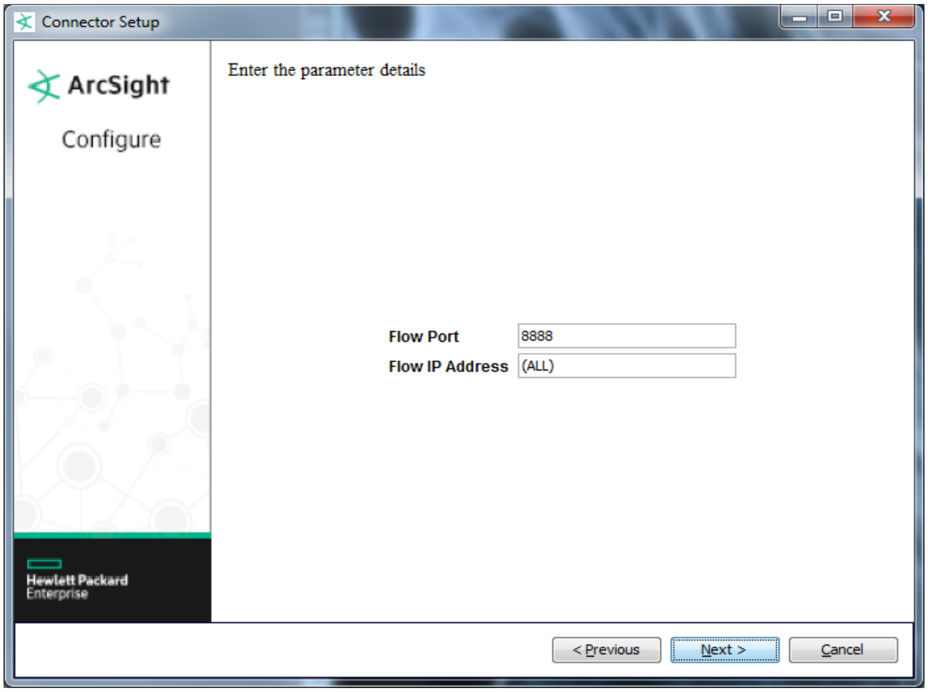
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **sFlow** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Enter the parameter details

Flow Port 8888

Flow IP Address (ALL)

Parameter	Description
Flow Port	Enter the number of the port to which the SmartConnector will listen.
Flow IP Address	The connector listens to all IP addresses on the specified port; individual IP addresses cannot be specified at this time.

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.

sFlow Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Bytes In	dOctets
Destination Address	dstaddr
Destination Port	dstport
Device Address	DeviceAddress
Device Custom Number 1	count
Device Custom Number 2	dPkts
Device Custom Number 3	tcp_flags
Device Custom String 1	nexthop
Device Custom String 2	src_as
Device Custom String 3	dst_as
Device Custom String 4	src_mask
Device Custom String 5	dest_mask
Device Custom String 6	tcp_flags descr
Device Event Class ID	'flow'
Device Product	'sFlow'
Device Receipt Time	unix_secs
Device Vendor	'sFlow'
Device Version	version
Name	'sFlow Event'
Source Address	srcaddr
Source Port	srcport
Transport Protocol	prot (1=ICMP, 2=IGMP, 4=IP, 6=TCP, 8=EGP, 9=IGP, 17=UDP, 41=IPv6, 43=IPv6-Route, 44=IPv6-Frag, 46=RSVP, 47=GRE, 50=ESP, 51=AH, 58=IPv6-ICMP, 59=IPv6-NoNxt, 60=IPv6-Opts, 88=EIGRP, 89=OSPFIGP, 94=IPIP, 98=ENCAP, 115=L2TP, 118=STP, 124=ISIS)