Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for QoSient ARGUS (Legacy)

Configuration Guide

February 15, 2017

Configuration Guide

SmartConnector for QoSient ARGUS (Legacy)

February 15, 2017

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

Revision History

Date	Description
02/15/2017	Marked connector as legacy.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2012	Added new installation procedure.
03/30/2011	Added note that connector should be installed on same machine as Argus client.
05/26/2010	Added configuration parameter for the ra.conf file.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure for FIPS support.

SmartConnector for QoSient ARGUS (Legacy)

This guide provides information for installing the SmartConnector for QoSient ARGUS (Audit Record Generation and Utilization System) and configuring the device for event collection. This SmartConnector is supported for installation on Linux platforms. QoSient ARGUS versions 2 and 3 are supported.

Product Overview

QoSient ARGUS is a fixed-model, real-time, flow monitor designed to track and report on the status and performance of all network transactions seen in a data network traffic stream. Argus provides a common data format for reporting flow metrics on a per transaction basis. It monitors network traffic while maintaining connection state information. Argus can be used to analyze and report on the contents of packet capture files or it can run as a continuous monitor, examining data from a live interface and generating an audit log of all the network activity seen in the packet stream.

The SmartConnector invokes an **ra** command, which reads Argus data from an Argus server and imports the events generated by Argus into the ArcSight ESM System.

For complete information about compiling, installing, configuring, and running Argus, see http://qosient.com/argus/.

Configuration

If you are configuring the connector for Argus version 3.x:

1 Open the Argus configuration file `ra.conf` and add the following properties to the file:

```
RA_TIME_FORMAT="%y-%m-%d %T"
RA_FIELD_DELIMITER=','
```

2 Save and close the file.

Install the SmartConnector

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

The connector must be installed on the same machine as the Argus client; it will not work properly when installed remotely.

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).

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

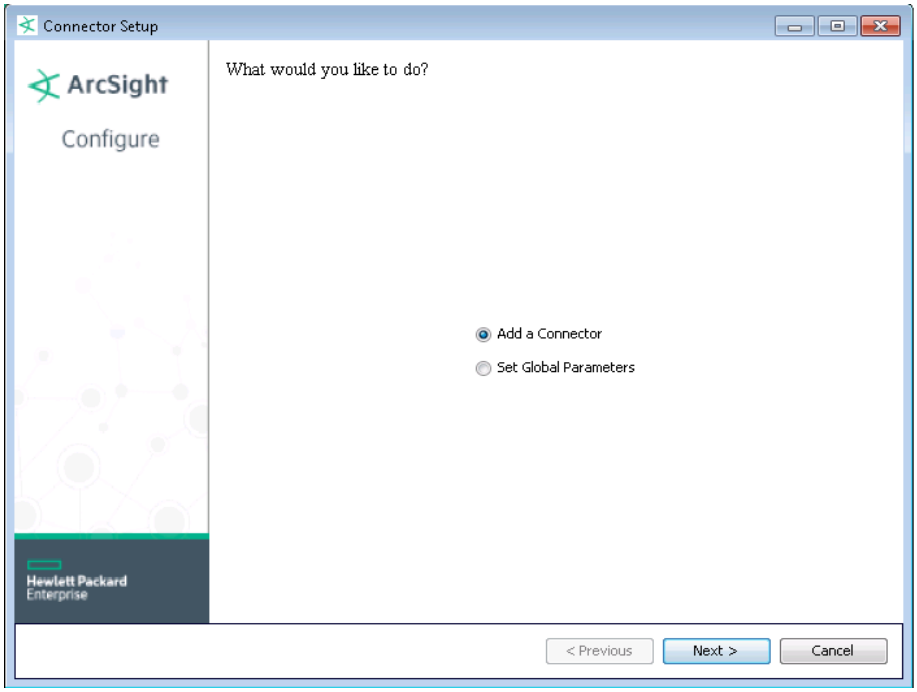
Install Core Software

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)

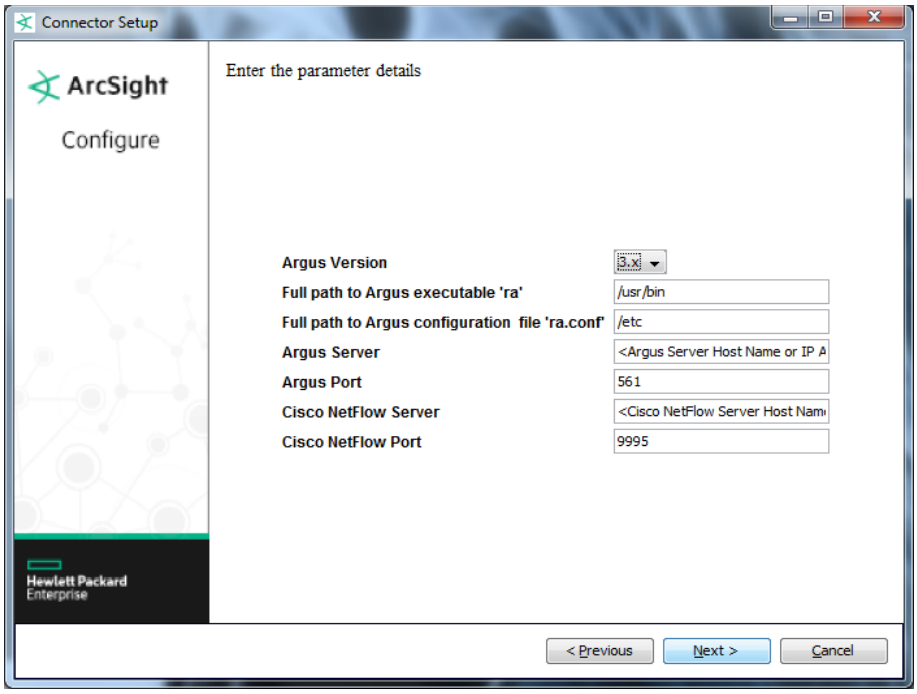
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

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



Parameter	Description
Argus Version	Select the product version from the drop-down list. Version 2.x is selected by default.
Full path to Argus executable 'ra'	Enter the full path to the location of the 'ra' executable. The default value is '/usr/bin'.
Full path to Argus configuration file 'ra.conf'	Enter the full path to the location of the 'ra.conf' file. The default value is '/etc'. This parameter is required only when you have selected Argus version 3.x.
Argus Server	Enter the host name or IP address of the Argus Server. Note that 'localhost' cannot be used as the server if traffic is received from a remote Argus Server.
Argus Port	Enter the port number to be used for SmartConnector communications with Argus. The default value is '561'.
Cisco NetFlow Server	Enter the host name or IP address of the Cisco NetFlow Server.
Cisco NetFlow Port	Enter the port number to be used for Cisco NetFlow communications. The default value is '9995'.

During connector installation in interactive mode, if you cannot enter null values or blank values for the parameters, you can leave the values in their default state so that the connector will ignore them. The connector will ignore the values for the Argus Server, Argus Port, Cisco NetFlow Server, and Cisco NetFlow Port parameters if they contain the prefix '<' and suffix '>'. Also, for the command line options used for the Argus versions 2 and 3 ra command, see "Device Event Mapping to Arcsight Data Fields."

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be 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 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.

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

For version 2, the following command line options for the **ra** executable are used:

```
ra -S <Argus Server>:<Argus Port> -C <Cisco NetFlow Server>:<Cisco
NetFlow Port> -n -s lasttime dur ind proto mac saddr sport dir dstid
daddr dport bytes pkts status
```

For version 3, the following command line options for the **ra** executable are used:

```
ra -F <Argus Configuration File Path>/ra.conf -S <Argus Server>:<Argus
Port> -C <Cisco NetFlow Server>:<Cisco NetFlow Port> -n -s stime ltime
dur flgs proto smac dmac saddr sport dir daddr dport sbytes dbytes spkts
dpkts state
```

Qosient Argus v3 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Bytes In	Source Bytes
Bytes Out	Destination Bytes
Destination Address	Destination Address
Destination Mac Address	Destination Mac Address
Destination Port	Destination Port
Device Action	State
Device Custom Number 1	Source Packets
Device Custom Number 2	Destination Packets
Device Custom String 1	Flag
Device Custom String 2	Direction
Device Custom String 3	Duration
Device Custom String 4	Destination Mac Address
Device Custom String 5	Source Address
Device Custom String 6	Destination Address
Device Product	'Argus'
Device Receipt Time	End Time
Device Vendor	'QoSient'
Device Version	'3.x'
End Time	End Time
Source Address	Source Address
Source Mac Address	Source Mac Address
Source Port	Source Port
Start Time	Start Time

ArcSight ESM Field	Device-Specific Field
Transport Protocol	Protocol

Qosient Argus v2 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	Application Protocol
Bytes In	Bytes In
Bytes Out	Bytes Out
Destination Address	Destination Address
Destination Mac Address	Dest Mac
Destination Port	Destination Port
Device Action	Status
Device Custom Number 1	Packets In
Device Custom Number 2	Packets Out
Device Custom Number 3	Duration
Device Custom String 1	Flag
Device Custom String 2	Direction
Device Custom String 4	Destination Mac Address
Device Event Class Id	Flag
Device Product	'Argus'
Device Receipt Time	Detect Time
Device Vendor	'QoSient'
Device Version	'2.x'
End Time	Detect Time
Source Address	Source Address
Source Mac Address	Source Mac
Source Port	Source Port
Transport Protocol	Protocol