Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for RSA Identity Management Service SNMP (Legacy)

Configuration Guide

May 15, 2017

Configuration Guide

SmartConnector for RSA Identity Management Service SNMP (Legacy)

May 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

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
05/15/2017	Marked connector as Legacy; use the SmartConnector for SNMP Unified.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	3DES option for Privacy parameter has been removed.
06/30/2015	Added note to use SmartConnector for SNMP Unified for future version support.
11/14/2014	Updated release date.
06/30/2014	General availability of this connector.
02/14/2014	Beta release of SmartConnector documentation.

SmartConnector for RSA Identity Management Service SNMP (Legacy)

This guide provides information for installing the SmartConnector for RSA Identity Management Service SNMP and configuring the device for event collection. RSA Identity Management Service version 8.0 is supported. For later versions, use the SmartConnector for SNMP Unified. Support for SNMP v3 event collection is also provided.

Product Overview

RSA Identity and Access Management provides identity, security, and access management for physical, virtual, and cloud-based environments.

The SmartConnector uses Simple Network Management Protocol (SNMP) to communicate with controllers, including SNMP v3 support. In contrast to SNMPv1 and SNMPv2, SNMPv3 supports authentication and encryption. SNMPv3 uses the concept of a user for which security parameters (levels of security, authentication, privacy protocols, and keys) are configured.

SNMP Versions

For instructions about forwarding SNMP traps to the ArcSight SmartConnector, see the documentation for your vendor's product.

SNMP Versions

SNMP is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates.

The different versions of SNMP are the SNMPv1, SNMPv2c, and SNMPv3. The following is a brief description of each version.

SNMPv1: This is the first version of the protocol, which is defined in RFCs 1155 and 1157. It is easy to set up, requiring only a plaintext community.

SNMPv2c: This is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, MIB structure elements but using the existing SNMPv1 administration structure ("community based" and hence SNMPv2c). It is defined in RFC 1901, RFC 1905, RFC 1906, RFC2578. In practical terms, v2c is identical to version 1, except it adds support for 64 bit counters.

SNMPv3: SNMPv3 defines the secure version of the SNMP. SNMPv3 also facilitates remote configuration of the SNMP entities. It is defined by RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415. It adds security to the 64 bit counters with both encryption and authentication, which can be used together or separately. Setup is more complex than just defining a community string.

SNMPv3 security comes primarily in two forms:

- Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the EngineID of the entity. The key is shared with the intended recipient and used to receive the message.

- Privacy is used to encrypt the payload of the SNMP message to ensure that it cannot be read by unauthorized users. Any intercepted traps will be filled with garbled characters and will be unreadable.

Using Zebedee Secure IP Tunnel with SNMP

ArcSight SNMP-based SmartConnectors support Zebedee, an open source UDP tunnel program that provides optional compression and encryption. To configure Zebedee, follow these steps:

1. Use Zebedee to create public and private keys on each of the devices. Create client and server `.zbd` configuration files as described in the Zebedee documentation to refer to the keys.

2. Install the SmartConnector. Start Zebedee in listen server mode on the SmartConnector host, with the command:

   ```
   zebedee -U -f server.zbd -s
   ```

   This prepares Zebedee to listen for connectionless UDP traffic.

3. The client machine is the host that is to send events to the SmartConnector. Run Zebedee on the client with the command:

   ```
   zebedee -U -f client.zbd 162:agent_hostname:162
   ```

   This prepares Zebedee to send UDP traffic to the SmartConnector host, `agent_hostname`.

Unless the device address is included in the SNMP trap, events do not record the host that actually sent the SNMP trap. Using Zebedee makes all SNMP traffic to the SmartConnector appear to come from `localhost`.

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).

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.

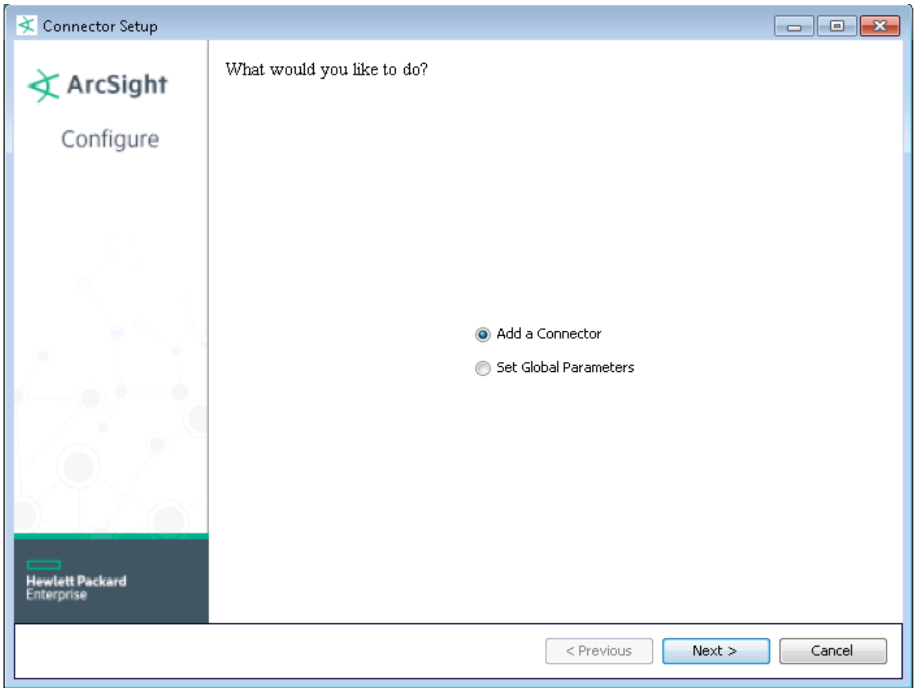
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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. 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'.

Global Parameter	Setting
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.

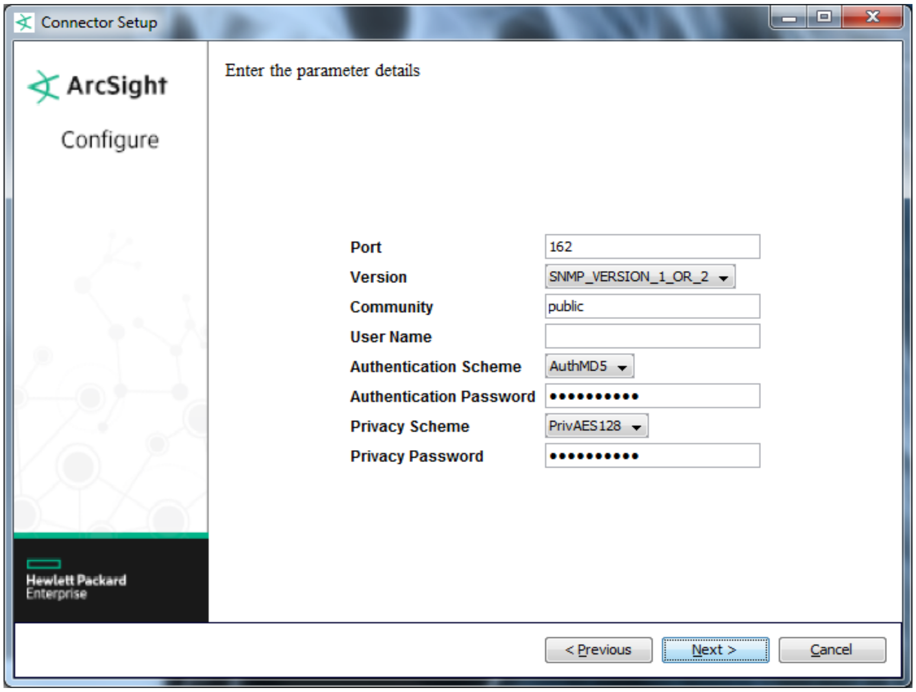
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **RSA Identity Management Service SNMP** and click **Next**.

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



Enter the parameter details

Port	162
Version	SNMP_VERSION_1_OR_2
Community	public
User Name	
Authentication Scheme	AuthMD5
Authentication Password	••••••••••
Privacy Scheme	PrivAES128
Privacy Password	••••••••••

Parameter	Description
Port	Enter the port number to which SNMP traps are sent. The default is 162.

Parameter	Description
Version	The SNMP version being used. Select SNMP_VERSION_3 or SNMP_VERSION_1_OR_2. SNMP_VERSION_1_OR_2 is the default. When you select SNMP_VERSION_1_OR_2, you need not enter values for the Authentication Scheme, Authentication Password, Privacy Scheme, or Privacy Password parameters as these are valid only for SNMP v3.
Community	Enter the community name to which SNMP trap messages are sent. The default is public.
User Name	Enter the name that identifies the SNMP v3 user.
Authentication Scheme	The type of authentication being used. Select AuthMD5 or AuthSHA. AuthMD5 is the default.
Authentication Password	Enter the authentication password.
Privacy Scheme	The type of privacy being used. Select PrivAES128, PrivAES192, or PrivAES256.
Privacy Password	Enter the privacy password.

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 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.

RSA Authentication Manager Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium = ERROR, System; Low = INFO
Destination Address	client
Destination User ID	ID
Destination User Name	login name
Device Custom String 3	User Full Name
Device Custom String 4	Security Domain ID
Device Custom String 6	Session ID
Device Event Class ID	action id
Device Payload ID	ID
Device Product	'Identity Management Service'
Device Receipt Time	time
Device Severity	Severity
Device Vendor	'RSA'
Event Outcome	result
Message	One of (reason, Message)
Name	One of (action, Name)
Reason	reason