Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Juniper Steel-Belted Radius File

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Juniper Steel-Belted Radius File

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

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2012	Added new installation procedure.
03/30/2011	Updated versions supported.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure.
03/27/2009	Added information regarding default rotation scheme.
02/11/2009	Updated field mappings.
11/12/2008	Added support for device version 6.0; added mappings for Accept and Reject events.

Contents

SmartConnector for Juniper Steel-Belted Radius File

This guide provides information for installing the SmartConnector for Juniper Steel-Belted Radius File and configuring the device for event collection. Steel-Belted Radius Global Enterprise Edition versions 5.03, 5.30, 5.40, and 6.0 are supported.

Product Overview

Steel-Belted Radius is an implementation of the RADIUS (Remote Authentication Dial In User Service) protocol that runs in Windows, Solaris, or Linux environments. It interfaces with a wide variety of network access equipment and authenticates remote and WLAN users against numerous back-end databases, letting the administration of your remote and WLAN users be consolidated, however they connect to the network. Steel-Belted Radius records usage statistics in an accounting database for tracking and documenting user sessions for accounting and billing.

Configuring the Device for Event Collection

The SmartConnector for Juniper Steel-Belted Radius supports the Accounting, Authentication, Authentication Accept, and Authentication Reject logs.

Only the default log format is supported; changing the format of these logs will cause parsing problems.

The following files establish settings for logging and reporting. For complete information, see the *Juniper Steel-Belted Radius Reference Guide* for details about these initialization files and "Logging and Reporting" in the *Juniper Steel-Belted Radius Administration Guide* for how to set up and use logging and reporting in Steel-Belted Radius.

File Name	Function
account.ini	Controls how RADIUS accounting attributes are logged.
authlog.ini	Controls how RADIUS authentication requests are logged.
authReport.ini	Controls what authentication logs are generated.
authReportAccept.ini	Controls options for the acceptance authentication log file.
authReportReject.ini	Controls options for the rejection authentication log file.

Authentication Log Files

The `authlog.ini` initialization file contains information that controls how RADIUS authentication request attributes are logged in the comma-delimited *yyyymmdd*`.authlog` file.

The [Configuration] section of `authlog.ini` specifies the location of the *yyymmdd*`.authlog` file. Use the `LogDir` parameter to specify the destination directory on the local host where *yyyymmdd*`.authlog` files are stored. The default value is the directory where Steel-Belted Radius is installed.

The [Settings] section of `authlog.ini` controls which entries are written to the authentication request log file, and ensures the compatibility of these entries with a variety of database systems.

Steel-Belted Radius writes all authentication request data to the current authentication request log file (*yyyymmddM*`.authlog`) until that log file is closed. When Steel-Belted Radius closes an authentication request log file, it immediately opens a new one and begins writing authentication request data to it. You can configure how often this rollover of the authentication request log file occurs.

The naming conventions of the authentication request log files support the fact that Steel-Belted Radius can create more than one file per day. The formats are as follows, where *y* = year digit, *m* = month digit, *d* = day digit, and *h* = hour digit. The extra sequence number *_nnnnn* starts at _00000 each day.

File Generation Method	File Naming Convention
Default (24 hours)	yyyymmdd.authlog
Non 24-hour rollover	yyyymmdd_hhmm.authlog
Rollover due to size	yyyymmdd_nnnnn.authlog
Rollover due to size or startup when non-24-hour time is in effect	yyyymmdd_hhmm_nnnnn.authlog

Accounting Log Files

The `account.ini` file contains information that controls how RADIUS accounting attributes are logged to a the comma-delimited text file by Steel-Belted Radius.

The [Configuration] section of `account.ini` specifies the location of the *yyymmdd*`.act` file. Use the **LogDir** parameter to specify the destination directory on the local host where *yyyymmdd*`.act` files are stored. The default value is the directory where Steel-Belted Radius is installed.

The [Settings] section of `account.ini` controls which entries are written to the accounting log file, and ensures the compatibility of these entries with a variety of database systems.

Steel-Belted Radius writes all accounting data to the current accounting log file (yyyymmddM=.act) until that log file is closed. When Steel-Belted Radius closes an accounting log file, it immediately opens a new one and begins writing accounting data to it. You can configure how often this rollover of the accounting log file occurs.

The naming conventions of the accounting log files support the fact that Steel-Belted Radius can create more than one file per day. The formats are as follows, where *y* = year digit, *m* = month digit, *d* = day digit, and *h* = hour digit. The extra sequence number *_nnnnn* starts at _00000 each day.

File Generation Method	File Naming Convention
Default (24 hours)	yyyymmdd.act
Non 24-hour rollover	yyyymmdd_hhmm.act
Rollover due to size	yyyymmdd_nnnnn.act
Rollover due to size or startup when non-24-hour time is in effect	yyyymmdd_hhmm_nnnnn.act

Authentication Acceptance Log Files

You can configure what is logged to the acceptance report by entering attributes in the `[Attributes]` section of `authReportAccept.ini` in the sequence in which they should appear.

The [Settings] section of authReportAccept.ini specifies the characteristics of the authentication acceptance report. If the MaxMinutesPerFile parameter is set to 0, the file name of the authentication acceptance report is accepts_yyyymmdd.csv (where yyyymmdd identifies the date the report was generated). If the MaxMinutesPerFile parameter is set to a value greater than 0, the file name of the report is accepts_yymmdd_hhmm.csv (where yyyymmdd identifies the date and hhmm identifies the time the report was generated).

Authentication Rejection Log Files

You can configure what is logged to the authentication rejection report by entering attributs in the [Attributes] section in the sequence in which they should appear.

The [Settings] section of authReportReject.ini specifies the characteristics of the authentication rejection report. If the MaxMinutesPerFile parameter is set to 0, the file name of the authentication rejection report is rejects_yyyymmdd.csv (where yyyymmdd identifies the date the report was generated). If the MaxMinutesPerFile parameter is set to a value greater than 0, the file name of the report is rejects_yyyymmdd_hhmm.csv (where yyyymmdd identifies the date and hhmm identifies the time the report was generated.

Enabling and Disabling Log Files

Use the **Enable** parameter in the [Settings] section of the appropriate initialization file to enable the log. If set to **1**, the log feature is enabled. If set to **0**, no log files are created on this server. The default value is 1 for Accounting logs and 0 for Authentication logs.

For Authentication logs, you also can enable or disable logging from the user interface:

1. Open the **Reports** panel and click the **Auth Logs** tab.
2. From the **Logs** drop-down list, select each authentication log file you want to enable, one at a time, and click the **Enable logging** checkbox.

Install the SmartConnector

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

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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

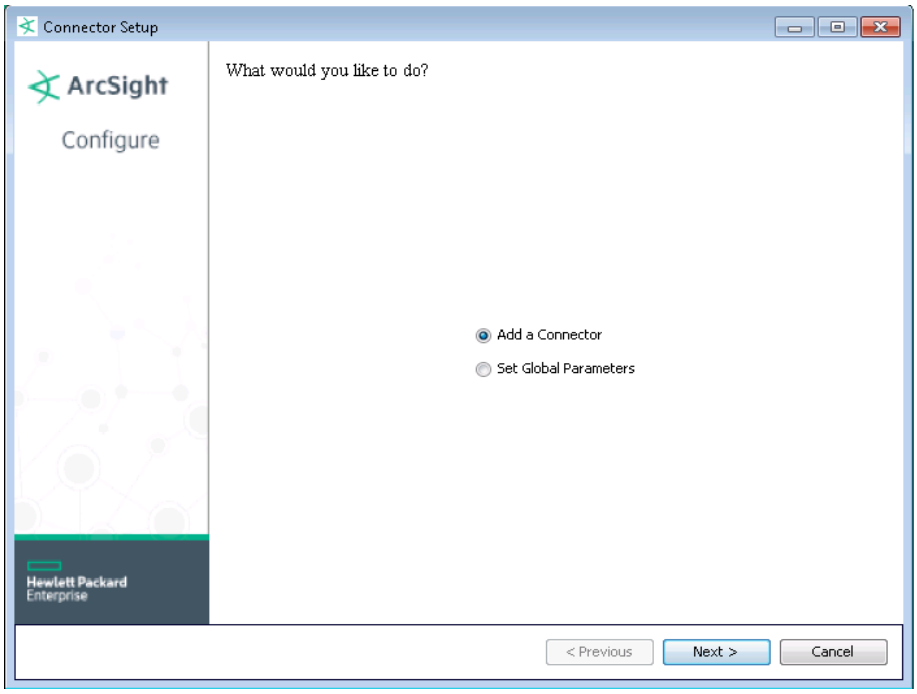
Install Core Software

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)

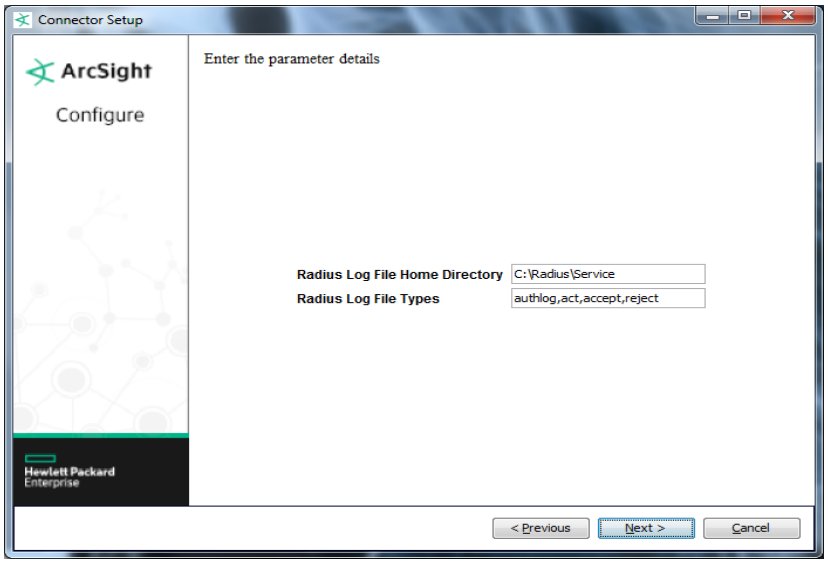
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

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.
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 **Juniper Steel-Belted Radius File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Radius Log File Home Directory	Enter the path to and name of the directory containing the log files (for example, C:\Radius\Service).
Radius Log File Types	Select authentication log (authlog), accounting log (act), accept, reject, or any combination of log types. By default, all logs are selected.

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*.

Log Rotation Scheme

The SmartConnector supports daily (24-hour) rotation scheme by default. However, non-daily rotation is supported by changing the internal parameter `rotationschemeparams`. The following is an overview.

File Generation Method	File Naming Convention	rotationschemeparams
Default (24 hours)	yyyymmdd.authlog	yyyyMMdd (by default)
Non 24-hour rollover	yyyymmdd_hhmm.authlog	yyyyMMdd_HHmm

After SmartConnector installation, you can update the `rotationschemeparams` parameter by editing the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Be sure to save the file and restart the connector for your changes to take effect.

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.

Juniper Steel-Belted Radius ACCEPT Log Mappings

ArcSight ESM Field	Device-Specific Field
ArcSight Severity	Low when Device Severity = ACCEPT
Destination User Name	User-Name
Device Action	'ACCEPT'
Device Custom Number 3	NAS-Port-Type
Device Custom String 1	RAS-Client
Device Custom String 3	Full-Name
Device Event Class ID	'Authentication - ACCEPT'
Device Product	'Steel-Belted Radius'
Device Receipt Time	Date,Time

ArcSight ESM Field	Device-Specific Field
Device Severity	'ACCEPT'
Device Vendor	'Juniper'
Name	'Authentication - ACCEPT'
Source Address	NAS-IP-Address
Source Host Name	Calling-Station-Id

Juniper Steel-Belted Radius REJECT Log Mappings

ArcSight ESM Field	Device-Specific Field
ArcSight Severity	Medium when Device Severity = REJECT
Destination User Name	User-Name
Device Action	'REJECT'
Device Custom String 1	RAS-Client
Device Event Class ID	'Authentication - REJECT'
Device Product	'Steel-Belted Radius'
Device Receipt Time	Date,Time
Device Severity	'REJECT'
Device Vendor	'Juniper'
Message	All of (Reject-Method, Reject-Reason, Reject-Log)
Name	'Authentication - REJECT'
Source Address	NAS-IP-Address

Juniper Steel-Belted Radius ACCOUNTING Log Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	FullNameWithDomain=Full-Name
Additional data	UserNameWithDomain=User-Name
ArcSight Severity	Low when Device Severity = Low
Bytes In	Acct-Input-Octets
Bytes Out	Acct-Output-Octets
Destination User Name	User-Name
Device Action	Record-Type
Device Custom Number 2	Acct-Session-Time
Device Custom String 1	Acct-Session-Id
Device Custom String 2	Service-Type
Device Custom String 3	Full-Name
Device Custom String 4	Acct-Input-Packets
Device Custom String 5	Acct-Output-Packets
Device Custom String 6	Called-Station-ID
Device Event Class ID	'Accounting -' plus Record-Type
Device Product	'Steel-Belted Radius'
Device Receipt Time	Date,Time
Device Severity	'Low'
Device Vendor	Juniper'

ArcSight ESM Field	Device-Specific Field
External ID	Acct-Session-Id
Name	'Accounting -' plus Record-Type
Source Address	NAS-IP-Address
Source Host Name	NAS-Identifier
Source Translated Address	Framed-IP-Address

Juniper Steel-Belted Radius Authentication Log Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	UserNameWithDomain=User-Name
ArcSight Severity	Medium when Device Severity = REJECT; Low when Device Severity = ACCEPT
Destination User Name	User-Name
Device Action	Acc/Rej
Device Custom String 1	RAS-Client
Device Custom String 2	Service-Type
Device Custom String 3	Full-Name
Device Custom String 6	Called-Station-ID
Device Event Class ID	'Authentication -' plus Acc/Rej
Device Product	'Steel-Belted Radius'
Device Receipt Time	Date,Time
Device Severity	Acc/Rej
Device Vendor	'Juniper'
External ID	Acct-Session-Id
Name	'Authentication -' plus Acc/Rej
Source Address	NAS-IP-Address
Source Host Name	NAS-Identifier
Source Translated Address	Framed-IP-Address