Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for HPE-UX Audit File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for HPE-UX Audit File

October 17, 2017

Copyright © 2005 – 2017 Hewlett Packard Enterprise Development LP

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

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	HP has changed to HPE, including Device Vendor.
06/30/2016	Removed support for HPE-UX 11.0 due to end of support by the vendor.
03/31/2016	Updated HPE-UX Audit 11i v3 Device Custom Number 1 mapping.
05/15/2012	Added new installation procedure.
05/15/2011	Added mapping for Source Address for HPE-UX Audit 11i v3.
03/30/2011	Updated mappings.
02/15/2011	Updated command to convert binary file to text format.

SmartConnector for HPE-UX Audit File

This guide provides information for installing the SmartConnector for HPE-UX Audit File and customizing the device for log event collection. HPE-UX Binary Audit versions 11i v1, v2 and v3 are supported.

Product Overview

The HPE-UX Auditing System records instances of access by subjects to objects and to detects any repeated attempts to bypass the protection mechanism, as well as any misuses of privileges.

Configuring HPE-UX Auditing

The auditing system provides administrators with a mechanism to select users and activities to be audited. All auditing tasks can be done manually using the following audit commands:

audsys
Starts and stops auditing; sets and displays audit file information.

audusr
Selects users to be audited.

audevent
Changes or displays event or system call status.

audomon
Sets the audit file monitoring and size parameters.

audisp
Displays the audit record. Run this command against the logs to convert the binary audit logs into human readable form (text) before depositing them in the folder to be monitored by the connector.

The *HPE-UX Reference* provides details on these commands.

The system supplies default auditing parameters at installation. Some of these defaults are activated automatically, some must be enabled.

If auditing is currently turned off, it will be turned on when your changes are activated. Changes to audit are retained as new defaults at system reboot.

Notes:

- By default, when system auditing is on, the audit status for all users is on. New users added to the system are automatically audited. You must explicitly turn audit off for these users, if desired. Changes take effect at the user's next login.
- The event types **admin**, **login**, and **moddac** are selected as default values by the system. Both **Audit Success** and **Audit Failure** are on. This is the minimum event type selection recommended

for running a Trusted System. A record is written when the event type is selected for auditing *and* the user initiating the event has been selected for auditing.

- The following audit monitor and log parameters are provided with default values shown. They can be changed using SAM or audit commands.

Primary log file path name	`/.secure/etc/audfile1`
Primary log file switch size (AFS)	1000 KB
Auxiliary log file path name	`/.secure/etc/audfile2`
Auxiliary log file switch size (AFS)	1000 KB
Monitor wake up interval	1 minute
Allowable free space minimum (FSS)	20% (of file system)
Start sending warning messages when log reaches	90%

- You can assess the size of your file systems using the `bdf` command. Choose a file system with adequate space for your audit log files. For example, using the system-supplied defaults, the `/.secure/etc` file system must have more than 5000 KB available for the primary audit log file and it must have more than 20% of its file space available.

HPE recommends that the primary and auxiliary audit log files reside on separate file systems; therefore, you should provide a new path name for the auxiliary log file. If the file system containing the primary log file is full and no auxiliary log file is specified, any nonroot process that generates audit data will block inside the kernel. Also, if a nonroot process is connected to the system terminal, it will be terminated.

For complete information about the HPE-UX Auditing System, see the *HPE-UX Reference*.

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).

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.

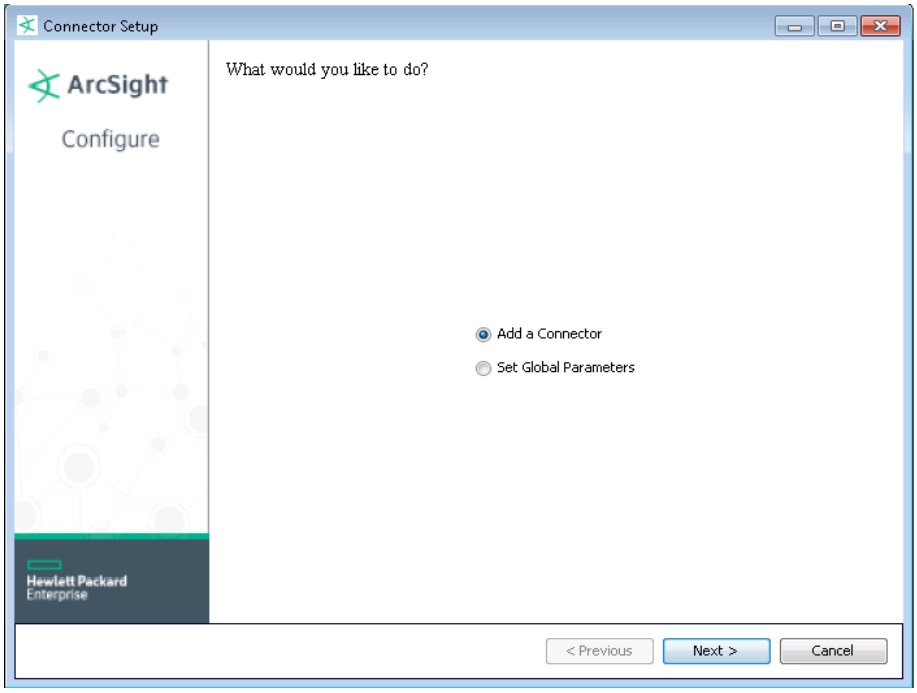
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.
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	When 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. The initial setting is IPv4.

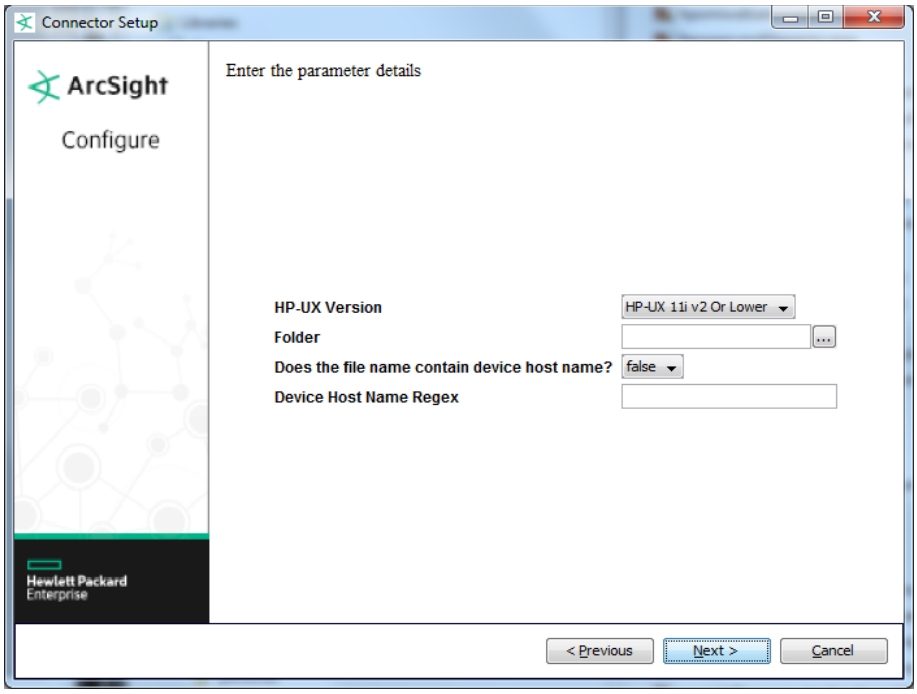
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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 proceed with "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 **HPE-UX Audit File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
HPE-UX Version	Select the HPE-UX version; 'HPE-UX 11i v2 or Lower' or 'HPE-UX 11i v3 or Higher'.
Folder	Absolute path to the folder containing the event log files.
Does the file name contain device host name?	Select true if the file name contains the device host name. The default value is False.
Device Host Name Regex	Enter a regular expression to retrieve the host name from the file name.

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.

HPE-UX Audit 11i v3 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	Error
Device Custom Number 1	GID (GroupID)
Device Custom Number 3	ErrorCode
Device Custom String 1	PPID (Parent PID)
Device Custom String 2	AuditTag

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	TTY
Device Custom String 4	Grp (Real Group)
Device Custom String 5	Groups
Device Custom String 6	Return1 (Return Value 1)
Device Event Class ID	Event
Device Product	'HPE-UX Binary Audit'
Device Receipt Time	Time
Device Vendor	'HPE'
Name	Event
Source Address	source
Source Process Name	PID
Source User ID	UID
Source User Name	User
Source User Privileges	EffectivePrivileges

HPE-UX Audit 11i v2 and Earlier Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High=Failure, Low=Success
Device Action	Status (S=Success, F=Failure)
Device Custom Number 1	RealGroupId (Real GID)
Device Custom Number 2	EffectiveUserId (Effective UID)
Device Custom Number 3	EffectiveGroupId (Effective GID)
Device Custom String 1	ParentProcessId (Parent PID)
Device Custom String 2	AuditId
Device Custom String 3	TTY
Device Custom String 4	RealGroup
Device Custom String 5	EffectiveGroup
Device Custom String 6	ReturnValue1
Device Event Category	EventType
Device Event Class ID	Event
Device Product	'HPE-UX Binary Audit'
Device Receipt Time	Time
Device Severity	Status (S=Success, F=Failure)
Device Vendor	'HPE'
Name	Event
Source Process Name	ProcessId
Source User ID	RealUserId
Source User Name	User