Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for HPE OpenVMS File

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for HPE OpenVMS 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

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://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	HP has changed to HPE, including Device Vendor.
02/15/2016	Added support for OpenVMS versions 8.3 and 8.4.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Added global update to installation procedure.
03/01/2008	Updated installation procedure.
08/15/2007	General SmartConnector availability.
06/26/2007	Updated field mapping for File Name field.
03/28/2007	First beta edition of this Configuration Guide.

SmartConnector for HPE OpenVMS File

This guide provides information for installing the SmartConnector for HPE OpenVMS File and configuring the device for event collection. OpenVMS versions 7.3, 8.3, and 8.4 are supported.

Product Overview

OpenVMS is a multitasking and multiprocessing operating system based on VMS. The "Open" suggests the added support for the UNIX-like interfaces of the POSIX standard. Programs written to the POSIX standard, which includes a set of standard C language programming functions, can be ported to any POSIX-supporting computer platform.

Configuration

The operating system provides several log files that record information about the use of system resources, error conditions, and other system events. The audit server process preallocates disk space and writes security-relevant system events to the Security Audit Log file.

Security auditing is the act of recording security-relevant events as they occur on the system. By default, the system enables security auditing when you install or upgrade your system for `ACL`, `AUDIT`, `AUTHORIZATION`, `BREAKIN`, and `LOGFAILURE` events. The audit server process, created at system startup, records these event types in the default audit log file `SECURITY.AUDIT$JOURNAL` (created in the `SYS$COMMON:[SYSMGR]` directory).

You can enable security auditing for other event classes by using the DCL command `SET AUDIT`. See the *HPE OpenVMS Guide to System Security* for descriptions of event classes you can enable.

To extract information from the Security Audit journal, enter the following command:

```
analyze/audit/full Sys$manager:Security.Audit$journal
```

Many parameters can be added to this command to extract just those items you want to extract. The content and format of the audit files is documented in Appendix F of *HPE OpenVMS System Management Utilities Reference Manual*.

When OpenVMS is installed on multiple servers (such as front-end and back-end servers), you will need to process audit security journal files from each server. These files should be collected on one server, in the folder you specify during SmartConnector installation.

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

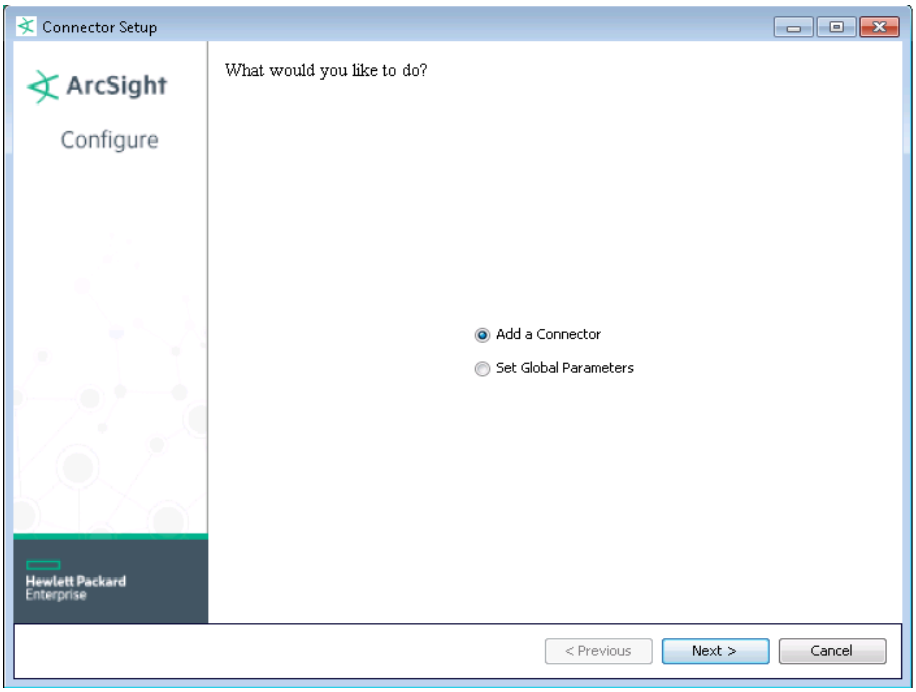
Install Core Software

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:



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'.

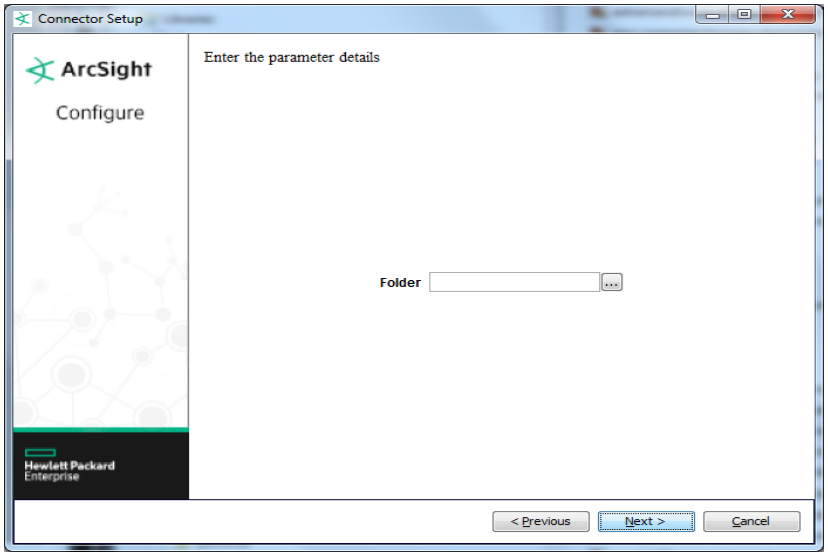
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **HPE OpenVMS File** and click **Next**.

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



Parameter	Description
Folder	Enter the name of the folder in which your log files are stored.

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.

HPE OpenVMS Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
ArcSight Severity (Low)	I or S
ArcSight Severity (Medium)	F or E
Destination Process Name	Process name
Destination User Name	One of (Remote username, User record added)
Destination User Privileges	Privileges used
Device Action	Access requested
Device Custom String 1	Matching ACE

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	PID
Device Custom String 3	Fields modified
Device Custom String 4	One of (Logical name, Volume name)
Device Custom String 5	Mount flags
Device Custom String 6	Terminal name
Device Event Class ID	Status plus Auditable event
Device Host Name	Hostname
Device Product	'OpenVMS'
Device Receipt Time	Event time
Device Severity	Status
Device Vendor	'HPE'
File Name	File name, Directory entry, Object name, Log file closed, or Log file opened
File Path	Directory name
File Permission	Object protection
File Type	Object class name
Message	Both (Status, Event information)
Name	Auditable event
Source Host Name	Terminal name
Source Port	Terminal name
Source Process Name	Image name
Source User Name	Username

Additional Data Mappings

Additional Data Field	Mapped to
systemid	Systemid
attributes	Attributes
directoryId	Directory ID
eventInformation	Event information
holderName	Holder name
identifierName	Identifier name
identifierValue	Identifier value
newIdentifierName	New identifier name
objectOwner	Object owner
posixGid	Posix GID
posixUid	Posix UID
processOwner	Process owner
remoteNodeId	Remote node id
remoteNodename	Remote nodename
sequenceKey	Sequence key
userData	User Data
flagsOriginal	Original

Additional Data Field	Mapped to
account	Account
defaultDevice	Default Device
defaultDirectory	Default Directory
flagsNew	Flags
lastInteractiveLogin	Last Interactive Login
lastNetworkLogin	Last Network Login
localAccounts	Local accounts
loginFailures	Login failures
owner	Owner
password	Password
passwordDate	Password Date
passwordLifetime	Password Lifetime
uic	UIC
userRecord	User record

Troubleshooting

How do I know when a data transfer has been successfully completed?

For all network transfers, a trigger file can be created after the data file is sent to indicate that the transfer was successfully completed. You can create this file after you have installed the SmartConnector.

To create a trigger file, change the value of the `usetriggerfile` property in `user/agent/agent.properties` from `false` to `true` and restart the connector.

```
agents[0].usetriggerfile=true
```

When the transfer is complete, create an empty file with the same name as the original file, but with an extension `.done`. For example, if your report is named `xyz.log`, create a trigger file with the name `xyz.done`.