



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for HPE OpenVMS File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2022-2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

- Configuration Guide for HPE OpenVMS File SmartConnector 4
- Product Overview 5
- Configuration 6
- Install the SmartConnector 7
 - Prepare to Install Connector 7
 - Install Core Software 8
 - Set Global Parameters (optional) 8
 - Select Connector and Add Parameter Information 10
 - Select a Destination 10
 - Complete Installation and Configuration 10
- Run the SmartConnector 12
- Device Event Mapping to ArcSight Fields 13
 - HPE OpenVMS Event Mappings to ArcSight ESM Fields 13
- Additional Data Mappings 15
- Troubleshooting 17
- Send Documentation Feedback 18

Configuration Guide for HPE OpenVMS File SmartConnector

This guide provides information for installing the SmartConnector for HPE OpenVMS File and configuring the device for event collection. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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).

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 OpenText SSO site.

- 1 Download the SmartConnector executable for your operating system from the OpenText 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 finishes, follow on-screen instructions to complete the installation.

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'.

Parameter	Setting
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 OpenText SecureData solutions to provide encryption. See the *OpenText 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 OpenText 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 OpenText 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 OpenText SecureData.
Format Preserving Secret	Enter the secret configured for OpenText 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 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; 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 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
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

ArcSight ESM Field	Device-Specific Field
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
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

Additional Data Field	Mapped to
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`.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for HPE OpenVMS File SmartConnector (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!