Hewlett Packard Enterprise

HPE Security ArcSight Connectors

SmartConnector for Apache HTTP Server
Access Multiple File

Configuration Guide

May 15, 2017

Configuration Guide

SmartConnector for Apache HTTP Server Access Multiple File

May 15, 2017

Revision History

Date	Description
05/15/2017	First edition of guide for multiple file connector.

SmartConnector for Apache HTTP Server Access Multiple File

This guide provides information for installing the SmartConnector for Apache HTTP Server Access Multiple File and configuring the device for event collection. This SmartConnector is supported on AIX, Linux, and Solaris platforms. Apache HTTP Server versions 1.3 and 2.4 are supported.

Product Overview

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. Apache is a secure, efficient, and extensible server that provides HTTP services in sync with the current HTTP standards.

The Apache HTTP server access log records all requests processed by the server. The location and content of the access logs are controlled by the CustomLog directive. The LogFormat directive can be used to simplify the selection of the contents of the logs. (See the Apache HTTP Server documentation for more information.)

Configuration

This section provides instructions for configuring a device to send events to the ArcSight SmartConnector.

1   Make sure that you are using Apache's default log formats.

The SmartConnector for Apache HTTP Server Log uses only four Apache default log formats. The default formats must appear in Apache's configuration file, `/etc/apache/httpd.conf`, as the following:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"
%T %v" full
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"
%P %T" debug
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

2   In Apache's configuration file, `/etc/apache/httpd.conf`, change the following line to:

```
customlog /var/log/apache/access.log<log file>
```

where <log file> is one of the following: **full**, **debug**, **combined**, or **common**.

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:
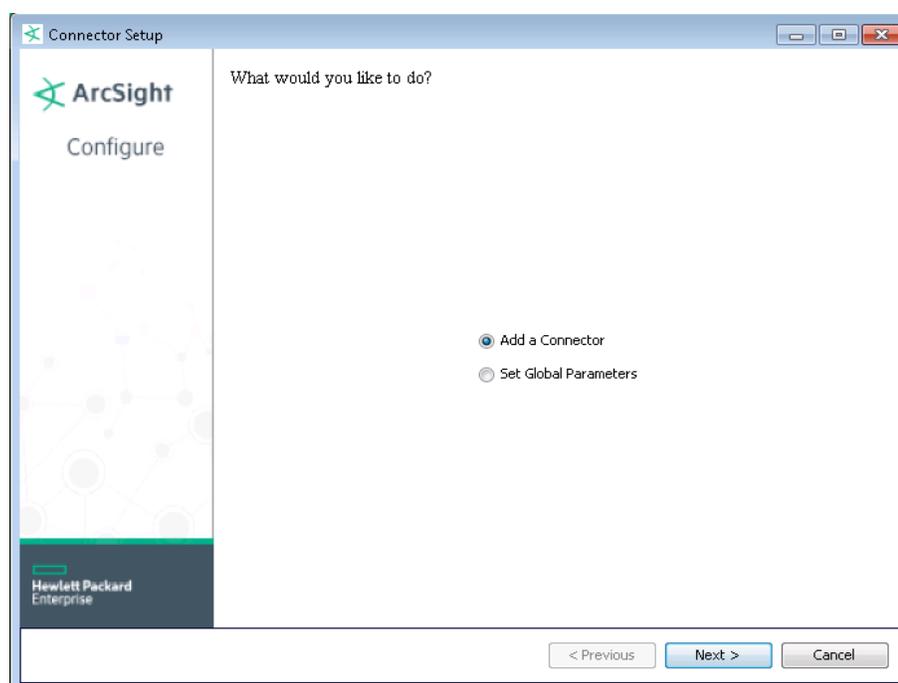
Set Global Parameters (optional)

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'.
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 **Apache HTTP Server Access Multiple File** and click **Next**.

3   Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.
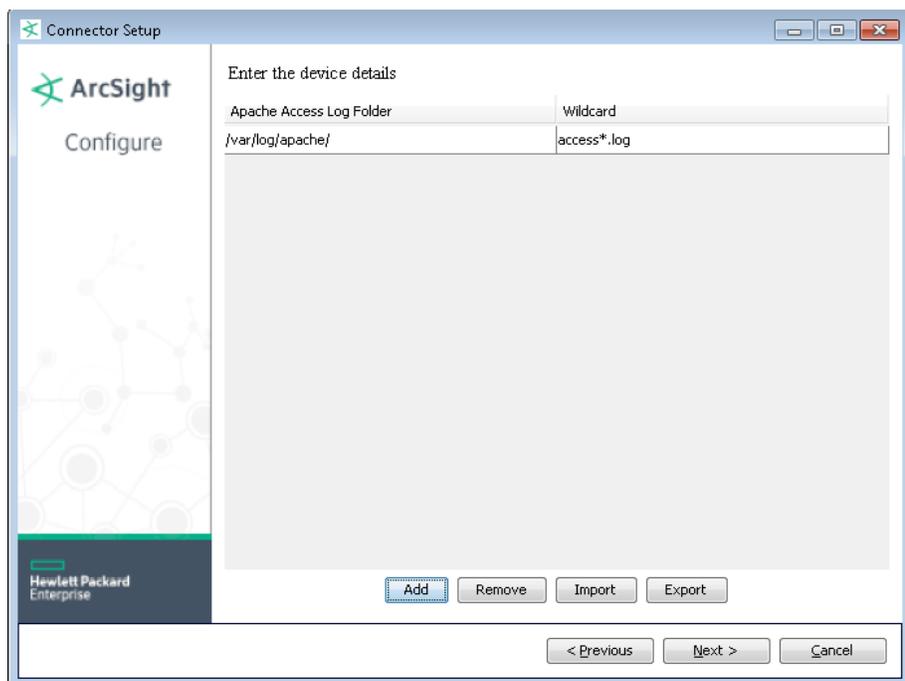
Parameter	Description
Apache Access Log Folder	The absolute path to the location of the log files (such as 'c:\Program Files\Apache Software Foundation\Apache2.2\logs\access.log' on a Windows platform), or accept the default /var/log/apache/access.log.
Wildcard	Enter a wildcard for data file names. Using the default value (access*.log), the connector will look for log files starting with "access".

Prior to installing the connector, make sure the Apache HTTP Server is configured to use Apache default log formats. The default formats must appear in Apache's configuration file, /etc/apache/httpd.conf.

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.

Apache HTTP Server Access Multiple File Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400..599; Medium = 300..399; Low = 0..299
Application Protocol	'http'

ArcSight ESM Field	Device-Specific Field
Destination Process Name	'apache'
Device Custom Number 1	Token12
Device Custom String 3	Length
Device Custom String 4	Referer
Device Custom String 5	Token13
Device Event Class ID	ReturnCode
Device Process Name	'apache'
Device Product	'apache'
Device Receipt Time	Date
Device Severity	ReturnCode
Device Vendor	'Apache'
Name	Entire
Request Client Application	UserAgent
Request Method	Method
Request URL	URL
Source Address	SourceHost
Source User ID	UserID
Transport Protocol	'TCP'