



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Apache Tomcat File

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Apache Tomcat File

November 30, 2016

Copyright © 2013 – 2016 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://www.protect724.hpe.com/docs/DOC-13026>.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/14/2014	Added the "Log Rotation - File Name Pattern" section.
11/15/2013	First edition of this Configuration Guide.

SmartConnector for Apache Tomcat File

This guide provides information for installing the SmartConnector for Apache Tomcat File and configuring the device for event collection. This SmartConnector is supported on the Linux platform. Apache Tomcat version 7.0 is supported.

Product Overview

Tomcat is an application server from the Apache Software Foundation that executes Java servlets and renders Web pages that include Java Server Page coding. The Apache Tomcat Server is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation.

Configuration

For information on configuring Apache Tomcat to send events to the ArcSight SmartConnector, see: http://tomcat.apache.org/tomcat-7.0-doc/logging.html#Documentation_references



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

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

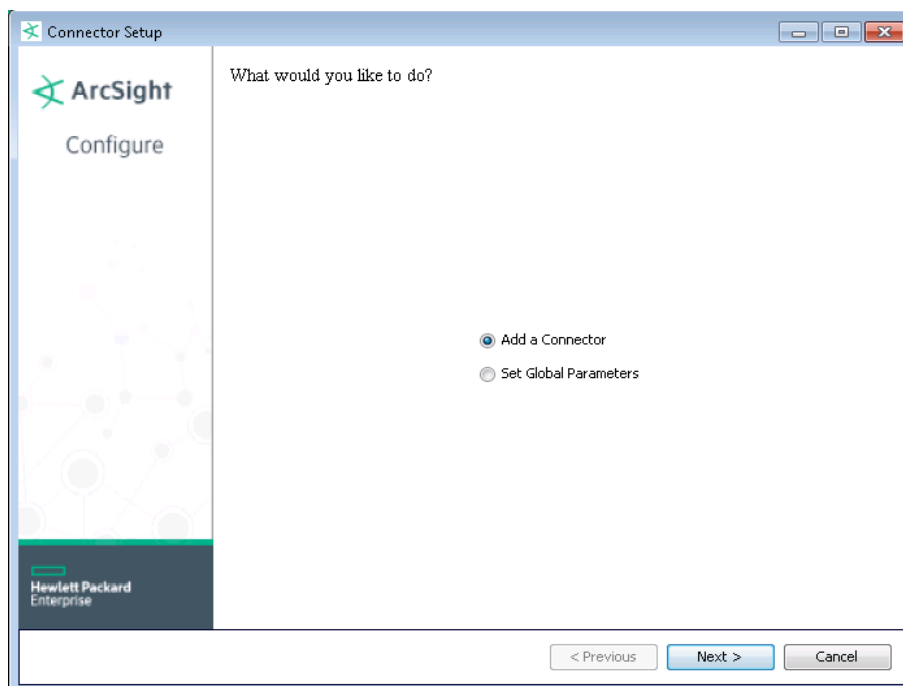
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

- 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:

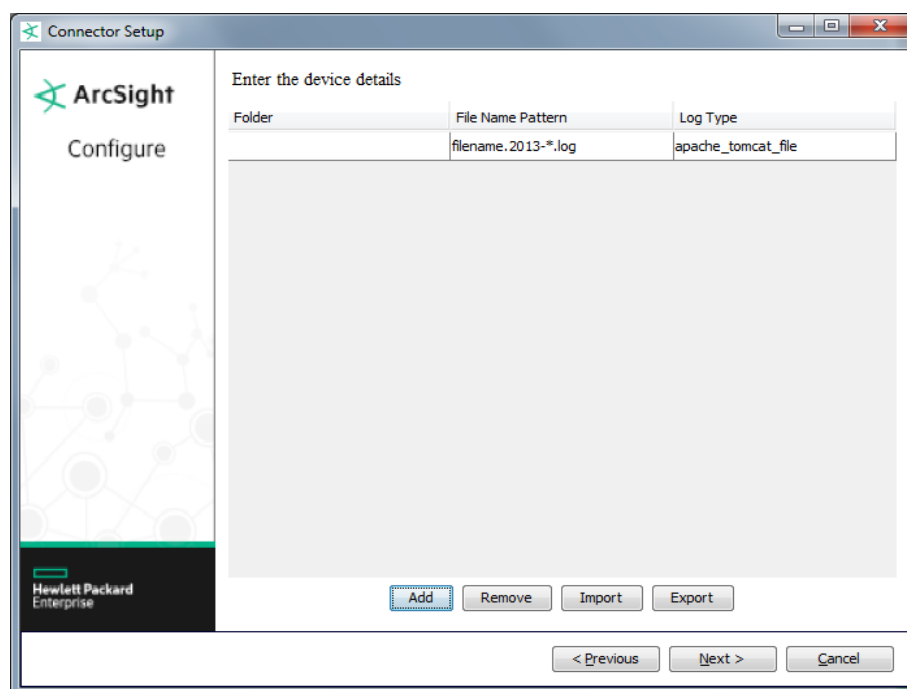
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.

Global Parameter	Setting
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 Tomcat File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	The absolute path to the location of the log files, such as 'c:\Program Files\Apache Software Foundation\Apache2.2\logs\' on a Windows platform) or '/var/log/apache/' on a UNIX platform.

Parameter	Description
File Name Pattern	<p>The log file name ('filename.2013-*.log') has three parts:</p> <ul style="list-style-type: none"> - Part 1: ('filename') is the file - Part 2: ('2013_*) is the date - Part 3: ('.log' or '.txt') is the file type <p>- For example: 'apache_tomcat_file.2013-11-15.log'; or 'catalina.2013-11-15.txt'; or 'localhost_access_log.2013-10-10.txt'</p> <p>See the section "Log Rotation - File Name Pattern" for details on log file rotation.</p>
Log Type	<p>Select the appropriate option from the drop-down list: 'apache_tomcat_file' or 'apache_tomcat_access_file':</p> <ul style="list-style-type: none"> - Select <code>apache_tomcat_access_file</code> if the file name includes <code>localhost_access</code> and has the following event format: "%h %l %u %t \"%r\" %s %b". An example of the <code>apache_tomcat_access_file</code> would be the file name created by the default setting. For example: <code>localhost_access_log.2013-10-10.txt</code> (Note the file type is <code>.txt</code>, not <code>.log</code>.) <p>For example:</p> <pre>10.10.3.108 - tomcat [11/Apr/2012:16:43:24 -0700] "GET /manager/status HTTP/1.1" 200 5636</pre> <ul style="list-style-type: none"> - Select <code>apache_tomcat_file</code> if the file name includes <code>catalina</code>, <code>host-manager</code>, <code>localhost</code>, and <code>manager</code>. Also, an event has two lines. For example: <ul style="list-style-type: none"> + The first line maps to regex: <code>\\w{3} \\d+, \\d+ \\d+:\\d+:\\d+ \\w+ \\S+.*</code> + The second line maps to regex: <code>(ALL FINEST FINER FINE CONFIG INFO WARNING SEVERE):.*</code> <p>For example:</p> <pre>Apr 11, 2012 4:43:15 PM org.apache.coyote.AbstractProtocol init INFO: Initializing ProtocolHandler ["ajp-bio-8009"]</pre> <p>NOTE: Click Add again to add additional log types. Folder paths can be changed too.</p>

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.

Apache Tomcat File Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Connector (Agent) Severity	High = SEVERE, Medium = WARNING, Low = INFO, CONFIG, FINE, FNER, FINEST, ALL
Destination Host Name	hostname
Device Action	action

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Process Time
Device Custom Number 2	Server Startup Time
Device Custom String 1	Packet Name
Device Custom String 2	Class Name
Device Custom String 3	Servlet Container
Device Custom String 4	Catalina Type
Device Custom String 5	Protocol Handler
Device Custom String 6	Servlet Engine
Device Event Class ID	message
Device Product	'Tomcat'
Device Receipt Time	Timestamp(DateTime,"MMM dd, yyyy HH:mm:ss a")
Device Severity	severity
Device Vendor	'Apache'
File Path	filePath
FileName	fileName
Message	MessageContent
Name	message

Apache Access File Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	http
Connector (Agent) Severity	High = 400..599, Medium = 300..399, Low = 0..299
Destination Process Name	'apache'
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	_safeToLong(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	'Tomcat'
Device Receipt Time	Date
Device Severity	ReturnCode
Device Vendor	'Apache'
Name	message
Request Client Application	UserAgent
Request Method	Method
Request URL	URL
Source Address	One of Address(SourceHost)
Source User ID	UserID
Transport Protocol	TCP

Log Rotation - File Name Pattern

You can use the File Name Pattern parameter to get data rotation. A typical scenario could be, the device writes to xyz.timestamp.log on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after processing is complete. The connector then creates a new reader thread to the new xyz.timestamp.log and begins processing that file. To enable this log rotation, set the [File Name Pattern](#) parameter to a date format, as shown in the example below:

```
FileName.'yyyy-MM-dd'.FileSuffix
```

Where for a data file name of `foo.2013-09-23.log`

```
fileName = foo  
'yyyy-mm-dd' = current date  
FileSuffix = .log
```