Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for Apache Tomcat File

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

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

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

Configuration Guide for 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.

Configuring Apache Tomcat to Send Events

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

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

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Select **Apache Tomcat File** in the **Type** drop-down, then click **Next**.
5. Specify the following 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.
File Name Pattern	The log file name ('filename.2013-*.log') has the following parts: • Part 1: ('filename') is the file • Part 2: ('2013_*') is the date • Part 3: ('.log' or '.txt') is the file type For example, 'apache_tomcat_file.2013-11-15.log'; or 'catalina.2013-11-15.txt'; or 'localhost_access_log.2013-10-10.txt' For more information about log file rotation, see Log Rotation- File Name Pattern.

Parameter	Description
Log Type	Select the appropriate option from the drop-down list: 'apache_tomcat_file' or 'apache_tomcat_access_file': Select apache_tomcat_access_file if the file name includes localhost_access and has the following event format: “%h %l %u %t "%r" %s %b”. An example of the apache_tomcat_access_file would be the file name created by the default setting. For example: localhost_access_log.2013-10-10.txt (Note the file type is .txt, not .log.) For example: 10.10.3.108 - tomcat [11/Apr/2012:16:43:24 -0700] "GET /manager/status HTTP/1.1" 200 5636 Select apache_tomcat_file if the file name includes catalina, host-manager, localhost, and manager. Also, an event has two lines. For example: • The first line maps to regex: \\w{3} \\d+, \\d+ \\d+:\\d+:\\d+ \\w+ \\S+.* • The second line maps to regex: (ALL|FINEST|FINER|FINE|CONFIG|INFO|WARNING|SEVERE):.* For example: Apr 11, 2012 4:43:15 PM org.apache.coyote.AbstractProtocol init **INFO:** Initializing ProtocolHandler ["ajp-bio-8009"] **Note:** Click **Add** again to add additional log types. You can also change folder paths.
Version	Select the appropriate option from the drop-down list: 'Older than 8' or '8 and 9'. If the Log version is older than 8, select 'Older than 8'. If Log version is 8 and 9, select '8 and 9'.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see SmartConnector Installation and User Guide.

Log Rotation - File Name Pattern

You can use the File Name Pattern parameter to get data rotation. In a typical scenario, 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 following example:

```
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
```

Device Event Mapping to ArcSight Fields

The following tables list 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
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

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
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

Apache Tomcat File Version 8 and 9 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
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	Thread Name
Device Custom String 5	Protocol Handler
Device Custom String 6	Servlet Engine
Device Product	'Tomcat'
Device Receipt Time	Timestamp(DateTime,"MMM dd, yyyy HH:mm:ss a")
Device Severity	Severity
Device Vendor	'Apache'
Message	MessageContent

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 SmartConnector for Apache Tomcat File (SmartConnectors 8.3.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!