



Micro Focus Security ArcSight Connectors

SmartConnector for Apache HTTP Server Syslog

Configuration Guide

July 24, 2019

Configuration Guide

SmartConnector for Apache HTTP Server Syslog

July 24, 2019

Copyright © 2003 – 2017; 2019 Copyright 2019 Micro Focus or one of its affiliates.

Legal Notices

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice. The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus. Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms. U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

| Date | Description |
|------------|---|
| 05/17/2019 | Added Apache HTTP Server Syslog Mappings. |
| 10/17/2017 | Added encryption parameters to Global Parameters. |

| Date | Description |
|------------|--|
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode. |
| 08/14/2015 | Added versions supported. |
| 05/15/2015 | Added new parameters for Syslog File. |
| 03/31/2015 | Updated severity mappings. |
| 02/16/2015 | Added parameter for Syslog Daemon connector configuration. Updated mappings table. |
| 06/30/2012 | Added support for Apache 2.4. Added and updated mappings. |
| 05/15/2012 | Added new installation procedure. |
| 02/11/2010 | Added support for FIPS Suite B and CEF File transport. |

SmartConnector for Apache HTTP Server Syslog

This guide provides information for installing the SmartConnector for Apache HTTP Server Syslog and for configuring the device for syslog event collection. Apache HTTP Server versions 1.3 and 2.4 are supported.

Product Overview

Apache HTTP Server is an open source HTTP web server for UNIX-like systems (BSD, Linux, and UNIX systems), Microsoft Windows, Novell Netware, and other platforms. Apache features highly configurable error messages, DBMS-based authentication databases, and content negotiation. The Apache HTTP Server is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation.

Configuration

Configuring Logging on the Apache HTTP Server

- 1 Edit the file `/etc/httpd/conf/httpd.conf` and add the entries:

```
ErrorLog "| /usr/bin/logger -t 'apache_error_log' "  
CustomLog "| /usr/bin/logger -t 'apache_access_log' "  
combined
```

This will send all access and error logs to syslog on the localhost. If you are forwarding events to a remote log host, the `/etc/syslog.conf` file should be modified.

- 2 Apache (and optionally Syslogd) must then be restarted to load the new configurations. This can be achieved by executing the following commands:

```
service httpd restart  
service syslog restart
```

Using Syslog with Apache 1.3 and Later

Using syslog instead of a filename enables logging via syslogd(8) if the system supports it. The default is to use syslog facility local7, but you can override this by using the `syslog:facility` syntax where facility can be one of the names usually documented in syslog(1). For example:

```
ErrorLog syslog
```

or

```
ErrorLog syslog:user
```

Configure Apache for Solaris Syslog

Additional configuration is required for the Solaris platform. For the purpose of this procedure, the default Apache 1.3 installation directory location on Solaris is used. The installation scripts are designed to determine the actual installation path.

- 1 Unlike the Apache configuration CustomLog directive, only one ErrorLog directive is effective for each httpd server or virtual container configuration. This will be the last encountered ErrorLog directive when the httpd configuration file is read (unless it is contained in a virtual host container). Therefore, in order to direct error messages to a local file as well as the logger command, the `tee` command must be used as follows:

```
ErrorLog "|/usr/bin/tee /var/apache/log/error_log|
/usr/bin/logger -t 'apache_error_log' "
```

- 2 If the Apache program `rotatelog`s is used to manage the `error_log` file, the ability to produce local log files with the addition of ArcSight log collection is more complex. In order to accomplish this, first the messages must be piped to a custom shell script as follows:

```
ErrorLog "|/usr/bin/xargs -s2048 -L1
/usr/apache/bin/error_tee_0.ksh"
```

Note that the Solaris `xargs` command is limited to an argument string of 2048 characters. The 'L1' option ensures the target script is executed for each Apache log message.

The customized script then is used to direct each message (passed as an argument list) to programs through pipe "|" or appended to files using ">>" as in the following example:

```
#!/usr/bin/ksh
echo "${*}"|/usr/apache/bin/rotatelog
/var/apache/log/error_log 86400
echo "${*}"|/usr/bin/logger -p local3.info -t
apache_error_log
exit
```

- 3 Although multiple CustomLog directives may be used in the httpd configuration, it is recommended for consistency that the same method for redirecting access messages be used. In this way, the existing CustomLog directive is replaced rather than adding additional CustomLog directives.

```
CustomLog "{/usr/bin/xargs -s2048 -l1
/usr/apache/bin/access_tee_0.ksh" combined
```



A separate 'access_tee' script is used for each CustomLog or ErrorLog directive encountered. This allows any defined virtual host to direct logs to separate local files.

The customized script used to direct each message is very similar to the script used for ErrorLog directives.

```
#!/usr/bin/ksh
echo "${*}" | /usr/apache/bin/rotatelog
/var/apache/log/access_log 86400
echo "${*}" | /usr/bin/logger -p local3.info -t
apache_access_log
exit
```

- 4 When this common log format or combined log format access messages are piped in this way, a change must also be made to the [LogFormat](#) directive. This is because the escaped double quotes (\") are evaluated. Therefore, to preserve the correct format, a double escape must be used (\\") as in the following:

```
LogFormat "%h %l %u %t \\\\"%r\\\\" %>s %b \\\\"%{User-Agent}i\\\\" " combined
LogFormat "%h %l %u %t \\\\"%r\\\\" %>s %b" %>s %b" common
```

- 5 When virtual host containers are used in the httpd configuration, both the error and access log messages specific to the specified virtual host or hosts may be directed to different local log files. This can be used to separate log information for different applications hosted by a single Web server. If this is done, each ErrorLog and CustomLog directive within each virtual host container must be replaced when configuring the Apache Web server for CSAT R1.
- 6 Finally, the TransferLog directive (if used) formats log messages based upon the default format. The default LogFormat usually is the same as the "common" format. However, this also must be reset to include the double escaped quotes by adding a Log Format directive without specifying the format name prior to the use of the TransferLog directive.

```
LogFormat "%h %l %u %t \\\\"%r\\\\" %>s %b"
```

To successfully implement the required configuration changes to Apache Web servers for CSAT R1, the changes have been automated and incorporated as part of the ArcSight Syslog Pipe connector installation. However, the scope of these changes will not extend beyond those changes necessary for log collection.

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

- Syslog Daemon
- Syslog Pipe
- Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.



Messages longer than 1024 bytes may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file (`rsyslog.conf`) can be added to write the events to either a **file** or a system **pipe** and the ArcSight SmartConnector can be configured to read the events from it. **In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon.**

The **Syslog Pipe** SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The **Syslog File** SmartConnector is similar to the Pipe SmartConnector; however, this SmartConnector monitors events written to a syslog file (such as `messages.log`) rather than to a system pipe.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the `/etc/rsyslog.conf` file, which contains specific details about which events to write to files, write to pipes, or send to another host. First, create a pipe or a file; then modify the `/etc/rsyslog.conf` file to send events to it.

For syslog pipe:

- 1 Create a pipe by executing the following command:

```
mkfifo /var/tmp/syspipe
```

- 2 Add the following line to your `/etc/rsyslog.conf` file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug | /var/tmp/syspipe
```

depending on your operating system.

- 3 After you have modified the file, restart the syslog daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.

On RedHat Linux, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

```
kill -HUP `cat /var/run/syslog.pid`
```

This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

- Syslog Daemon
- Syslog Pipe
- Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

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 Micro Focus SSO and Protect 724 sites.

- 1** Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
- 2** Start the SmartConnector installation and configuration wizard by running the executable.

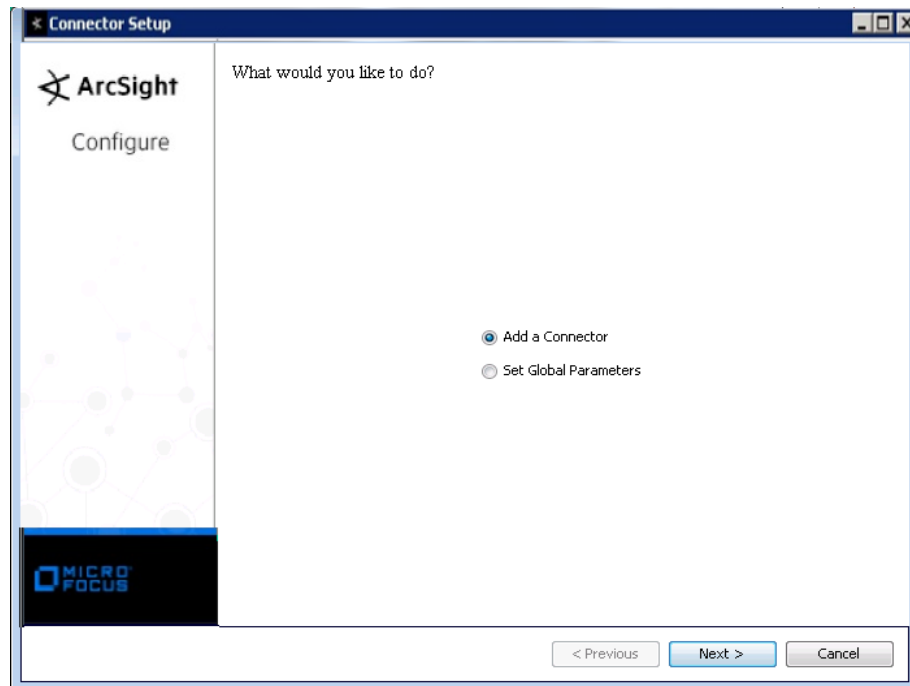


When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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:

| 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'. |
| 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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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. |

| Parameter | Setting |
|------------------------------|--|
| Format Preserving Policy URL | Enter the URL where the Micro Focus 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 Micro Focus 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 Micro Focus SecureData. |
| Format Preserving Secret | Enter the secret configured for Micro Focus 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 **Syslog Daemon, Syslog File, or Syslog Pipe** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

| | | |
|---------------------------------|--------------------------------|--|
| Syslog Daemon Parameters | <i>Network port</i> | The SmartConnector for Syslog Daemon listens for syslog events from this port. |
| | <i>IP Address</i> | The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses). |
| | <i>Protocol</i> | The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages. |
| | <i>Forwarder</i> | Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields. |
| Syslog Pipe Parameter | <i>Pipe Absolute Path Name</i> | Absolute path to the pipe, or accept the default: <code>/var/tmp/syspipe</code> |
| Syslog File Parameters | <i>File Absolute Path Name</i> | Enter the full path name for the file from which this connector will read events or accept the default: <code>\var\adm\messages</code> (Solaris) or <code>\var\log\messages</code> (Linux). A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation. |

For date format log rotation, the device writes to 'filename.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 'filename.timestamp.log' and begins processing that file. To enable this log rotation, use a date format in the file name as shown in the following example:

```
filename 'yyyy-MM-dd'.log;
```

For index log rotation, the device writes to indexed files - 'filename.log.001', 'filename.log.002', 'filename.log.003', and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:

```
filename '%d,1,99,true'.log;
```

Specifying 'true' indicates that it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.

| | |
|--|---|
| <i>Reading Events Real Time or Batch</i> | Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only. |
| <i>Action Upon Reaching EOF</i> | For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter. |
| <i>File Extension If Rename Action</i> | For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'. |

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 Syslog Mappings to ArcSight ESM Fields

| ArcSight ESM Field | Device-Specific Field |
|--------------------|-----------------------|
| Additional data | errorCode |
| Additional data | errorStatus |
| Additional data | HTTPVersion |
| Additional data | Identity |

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|---|
| Additional data | lineNumber |
| Additional data | moduleName |
| Additional data | pid |
| Additional data | request |
| Additional data | RequestingApplication |
| Additional data | require |
| Additional data | sourceFileName |
| Additional data | UserAgent |
| Agent (Connector) Severity | Very High = crit, emerg, alert; High = err, error, 400..599; Medium = warn, 300..399; Low = info, notice, debug, 0..299 |
| Application Protocol | 'http' |
| Destination Address | destination address |
| Destination Host Name | destination host name |
| Destination Port | destination port |
| Destination Process Name | 'apache' |
| Device Action | action taken by the device |
| Device Custom Date 1 | Server built time |
| Device Custom IPv6 Address 2 | Source IPv6 Address |
| Device Custom IPv6 Address 3 | Destination IPv6 Address |
| Device Custom Number 3 | Threat ID |
| Device Custom String 1 | Module |
| Device Custom String 2 | Host OS |
| Device Custom String 3 | Length |
| Device Custom String 4 | Referer |
| Device Custom String 5 | Mutex |
| Device Custom String 6 | Facility |
| Device Host Name | HostName |
| Device Process Name | One of (Module, 'apache') |
| Device Product | 'apache' |
| Device Receipt Time | device receipt time |
| Device Severity | Priority |
| Device Vendor | 'Apache' |
| Device Version | version |
| File Name | file name |
| File Path | file path |
| Name | Message |
| Reason | reason |
| Request Method | request method |
| Request URL | URL |
| Source Address | source ip |
| Source Host Name | source host name |
| Source Process ID | source process ID |
| Source User ID | source user ID |

| ArcSight ESM Field | Device-Specific Field |
|---------------------------|------------------------------|
| Target User ID | target user ID |
| Transport Protocol | 'TCP' |
