
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Apache HTTP Server Syslog SmartConnector

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

© Copyright 2022 Micro Focus or one of its affiliates

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.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

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.

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/

Contents

- SmartConnector for Apache HTTP Server Syslog 5
- Product Overview 6
- Configuration 7
 - Configuring Logging on the Apache HTTP Server 7
 - Using Syslog with Apache 1.3 and Later 7
 - Configuring Apache for Solaris Syslog 7
 - Configuring for the Syslog SmartConnectors 9
- Installing the SmartConnector 13
 - Preparing to Install the SamrtConnector 13
 - Installing and Configuring the SmartConnector 13
- Device Event Mapping to ArcSight Fields 17
 - Apache HTTP Server Syslog Mappings to ArcSight ESM Fields 17
- Send Documentation Feedback 19

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.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact [Micro Focus Customer Care](#).

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 `/etc/httpd/conf/httpd.conf` file to add the entries:

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

This sends all access and error logs to syslog on the localhost.
2. If you are forwarding events to a remote log host, then modify the `/etc/syslog.conf`.
3. Restart Apache (and optionally Syslogd) load the new configurations.

```
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
```

Configuring Apache for Solaris Syslog

The Solaris platform requires additional configuration. The installation scripts are designed to determine the actual installation path. However, in the following procedure the default Apache 1.3 installation directory location on Solaris is used as an example.

- 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). To direct error messages to a local file as well as the logger command, use the tee command as follows:

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

- If the Apache program rotatelog 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. You must pipe the first the messages 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 is used to direct each message (passed as an argument list) to programs through pipe "|" or appended to files using ">>" as shown 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
```

- Although multiple CustomLog directives might be used in the httpd configuration, it is recommended for consistency that the same method is used to redirect access messages. The existing CustomLog directive is replaced rather than adding additional CustomLog directives. The 'L1' option ensures the target script is executed for each Apache log message.

```
CustomLog "{/usr/bin/xargs -s2048 -l1 /usr/apache/bin/access_tee_  
0.ksh".
```

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
```

- 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
```

- 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.
- The TransferLog directive (if used) formats log messages based on 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.

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Deamon, Syslog Deamon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Deamon 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 Deamon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Deamon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Deamon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

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

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 additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Deamon SmartConnector configurations are done.

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.

Using the SmartConnector for Syslog Pipe or File

This section provides information 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.

For Syslog Pipe:

1. Execute the following command to create a pipe:

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

2. Add one of the following lines depending on your OS to the `/etc/rsyslog.conf` file:

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

or

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

3. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the `/etc/rsyslog.conf` file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

3. Restart the syslog daemon in one of the following methods:
 - a. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

Installing the SmartConnector

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

Preparing to Install the SamrtConnector

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 and Configuring 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.

Syslog Daemon SmartConnector

The Syslog Deamon 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 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

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

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 additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

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.

Using the SmartConnector for Syslog Pipe or File

This section provides information 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.

For Syslog Pipe:

- a. Execute the following command to create a pipe:

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

- b. Add one of the following lines depending on your OS to the `/etc/rsyslog.conf` file:

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

or

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

- c. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

For Syslog File:

- a. Create a file or use the default file into which log messages must be written.

- b. Modify the `/etc/rsyslog.conf` file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

- c. Restart the syslog daemon in one of the following methods:

- i. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

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

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

For instructions about upgrading the connector or modifying parameters, see [SmartConnector Installation and User Guide](#).

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
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

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

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 Apache HTTP Server Syslog SmartConnector (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!