
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for TippingPoint SMS 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.

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs |

Contents

- Configuration Guide for TippingPoint SMS Syslog SmartConnector 5
- Product Overview 6
- Configuration 7
 - Configuring TippingPoint Syslog 7
 - Configuring for the Syslog SmartConnectors 7
- Installing the SmartConnector 11
 - Preparing to Install the SmartConnector 11
 - Installing and Configuring the SmartConnector 11
- Device Event Mapping to ArcSight Fields 15
 - TippingPoint Syslog Format 2.5 Mappings 15
 - TippingPoint Syslog Format 2.0 Mappings 16
 - TippingPoint Syslog Device Audit Mappings 17
 - TippingPoint Syslog SMS Audit Mappings 18
- Send Documentation Feedback 19

Configuration Guide for TippingPoint SMS Syslog SmartConnector

This guide provides information for installing the SmartConnector for TippingPoint SMS Syslog and configuring the device for syslog event collection. Support for SMS and IPS device audit events is also included. For supported devices and versions, see [Technical Requirements](#).



The CEF certified event format used in SMS 4.0 complies with the requirements of the Micro Focus ArcSight Common Event Format. Micro Focus's "SmartConnector for ArcSight Common Event Format Syslog" processes all events correctly for SMS 4.0 and makes all events available for use within Micro Focus's ArcSight product.

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

The TippingPoint Security Management System (SMS) is a hardened appliance that provides global vision and control for multiple TippingPoint Intrusion Prevention Systems (IPS). The SMS is responsible for discovering, monitoring, configuring, diagnosing and reporting for multiple TippingPoint IPS systems.

Configuration

Configuring TippingPoint Syslog

The TippingPoint product has two types of devices, sensors and SMS devices, which act as the management console and central logging point. The SMS provides a separate syslog output format option that works with third-party network security devices and host applications. ArcSight currently supports only events sent to our connector from the SMS console, not the events sent directly to the connector from the sensor devices, as the two devices log in slightly different formats.

When configuring the SMS console for syslog event collection, make sure to:

- Select to receive syslog from **manager** instead of **device**.
- Set the Syslog format to **SMS v2.0 syslog Format** or **SMS v2.5 syslog Format**. Syslog format 2.5 is supported only with TippingPoint versions 3.2, 3.3, 3.5, and 3.6.
- Set up the syslog messages to be tab delimited (not pipe, semi colon, or comma).
- Set the **Include timestamp** in header radio button to none.
- Uncheck the **Include SMS hostname** in header box.

For complete device configuration information, see your TippingPoint documentation.



See the TippingPoint integration guide to setup and retrieve payload successfully. The Common Event Format Configuration Guide for Micro Focus TippingPoint Next Generation Firewall (Micro Focus TippingPoint CEF) is available on Protect 724 at: <https://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs>. Scroll to and click the Micro Focus logo under the heading "DLP & Data Security".

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 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 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.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next**, then specify the following parameters:

| Parameters | Description |
|--------------|--|
| Network port | The SmartConnector for Syslog Daemon listens for syslog events from this port. |
| IP Address | The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses. |
| Protocol | Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning. |
| Forwarder | This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file. For the real-time mode, retain the default value None . |

- b. Click **Next**.

- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, then specify the following parameters:

| Parameters | Description |
|-------------------------|---|
| Pipe Absolute Path Name | Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> . |
| File Absolute Path Name | <p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none"> • Solaris: <code>\var\adm\messages</code> • Linux: <code>\var\log\messages</code> <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none"> • Date format log rotation: The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code> • Index log rotation: The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, 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: <code>filename '%d,1,99,true'.log</code>; Specifying <code>true</code> indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of <code>true</code> is optional. |

| Parameters | Description |
|---|---|
| Reading Events Real Time or Batch | Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning. |
| Action Upon Reaching EOF | This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None . |
| File Extension If Rename Action | This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension. |

- b. Click **Next**.
5. Select a destination and configure parameters.
6. Specify a name for the connector.
7. 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.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. 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.

TippingPoint Syslog Format 2.5 Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|---|
| Agent (Connector) Severity | Very High = Critical; High = Major; Medium = Low or Minor; Low = Normal |
| Application Protocol | protocol |
| Base Event Count | evtcount |
| Destination Address | dstip |
| Destination Port | dstport |
| Device Action | actiontype (7=Permit, 8=Block, 9=P2P, 12=Quarantine) |
| Device Custom IPv6 Address 2 | srcip |
| Device Custom IPv6 Address 3 | dstip |
| Device Custom Number 1 | vlanid |
| Device Custom Number 2 | alarmid |
| Device Custom String 2 | policyUUID |
| Device Custom String 3 | signatureUUID |
| Device Custom String 4 | Both (srczonename, dstzonename) |
| Device Custom String 5 | _SYSLOG_SENDER (Device Name) |
| Device Custom String 6 | querieddomain |
| Device Event Class ID | appid |
| Device Host Name | devicename (SMS Host Name) |
| Device Inbound Interface | phyport |
| Device Product | 'SMS' |
| Device Receipt Time | apptimestamplong |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|---|
| Device Severity | appseverity (0=Normal, 1=Low, 2=Minor, 3=Major, 4=Critical, 5=Critical) |
| Device Vendor | 'TippingPoint' |
| External ID | seqnumber |
| Name | message |
| Source Address | srcip |
| Source Port | srcport |
| Transport Protocol | protocol |

TippingPoint Syslog Format 2.0 Mappings

| ArcSight ESM Field | Device-Specific Field |
|--------------------------|--|
| Application Protocol | protocol |
| Base Event Count | Evtcount |
| Destination Address | dstIP |
| Destination Port | dstport |
| Device Action | Action Type (7=Permit, 8=Block, 9=P2P) |
| Device Custom Number 1 | alarmID |
| Device Custom String 2 | policyUUID |
| Device Custom String 3 | signatureUUID |
| Device Custom String 4 | devicesegment |
| Device Custom String 5 | devicename |
| Device Event Class ID | appID |
| Device Inbound Interface | deviceslot |
| Device Product | 'SMS' |
| Device Receipt Time | apptimestamplong |
| Device Severity | App Severity (0=Normal, 1=Low, 2=Minor, 3=Major, 4=Critical, 5=Critical) |
| Device Vendor | 'TippingPoint' |
| Name | Message |

| ArcSight ESM Field | Device-Specific Field |
|--------------------|-----------------------|
| Source Address | srcIP |
| Source Port | srcport |
| Transport Protocol | protocol |

TippingPoint Syslog Device Audit Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--|
| Agent (Connector) Severity | Medium = FAIL; Low = PASS |
| Destination Address | destination IP |
| Destination Port | destination port number |
| Destination User Name | deviceUser |
| Device Action | Device Action |
| Device Custom Date 1 | Rotation start date |
| Device Custom Date 2 | Rotation end date |
| Device Custom IPv6 Address 2 | Source IPv6 Address |
| Device Custom String 5 | Device Name |
| Device Event Category | category |
| Device Event Class ID | Short description of the message field |
| Device Inbound Interface | interface |
| Device Product | 'SMS' |
| Device Severity | result |
| Device Vendor | 'TippingPoint' |
| Event Outcome | Status |
| Message | message |
| Name | Short description of the message field |
| Source Address | sourceIP |

TippingPoint Syslog SMS Audit Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--|
| Agent (Connector) Severity | Medium = fail; Low = success |
| Destination Address | destination IP |
| Device Action | action |
| Device Custom IPv6 Address 2 | Source IPv6 Address |
| Device Custom Number 1 | Session ID |
| Device Custom String 1 | ActionSet rule |
| Device Custom String 3 | Signature version |
| Device Custom String 5 | Device Name |
| Device Event Class ID | Short description of the description field |
| Device Inbound Interface | interface |
| Device Product | 'SMS' |
| Device Receipt Time | eventtimestamp |
| Device Severity | status |
| Device Vendor | 'TippingPoint' |
| Event Outcome | status |
| Message | description |
| Name | Short description of the description field |
| Source Address | clientAddress |
| Source Host Name | clientAddress |
| Source Port | clientPort |
| Source User Name | username |
| Transport Protocol | protocol |

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 TippingPoint SMS 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!