



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for TippingPoint SMS Syslog Extended SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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>

Contents

Configuration Guide for TippingPoint SMS Syslog Extended SmartConnector	4
Product Overview	5
Configuration	6
Exporting Security Certificate	6
Installing the SmartConnector	7
Preparing to Install the SmartConnector	7
Installing the SmartConnector	7
Payload Support	10
Locate Payload-Bearing Events	11
Retrieve Payloads	11
Preserve Payloads	11
Discard Payloads	12
Save Payloads to Files	12
Device Event Mapping to ArcSight Fields	13
TippingPoint Syslog Format 2.5/SMS 3.2, 3.3, 3.5, and 3.6 Mappings	13
TippingPoint Syslog Device Audit Mappings	14
TippingPoint Syslog SMS Audit Mappings	15
Troubleshooting	16
Send Documentation Feedback	17

Configuration Guide for TippingPoint SMS Syslog Extended SmartConnector

This guide provides information for installing the SmartConnector for TippingPoint SMS Syslog Extended 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](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for 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.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

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 MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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

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 v2.5 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).

For complete device configuration information, see your TippingPoint documentation.

Exporting Security Certificate

The TippingPoint SMS Syslog Extended connector requires the TippingPoint SMS CA Certificate. To export the certificate:

1. Using Internet Explorer, navigate to the **Welcome to your SMS** home page.
2. Right-click on an open area of the page and select **Properties** from the menu.
3. Click **Certificates** on the Properties dialog.
4. Click the **Details** tab on the Certificate dialog.
5. Click **Copy to File ...**.
6. Click **Next** on the Certificate Export Wizard.
7. Select **Der encoded binary X.509 (.CER)** and click **Next**.
8. Enter the name of the file you want to export or click **Browse** and then navigate to the file. Make sure to note the name and location of the file; you will import the certificate during connector installation.
9. Click **Next**.
10. Click **Finish**.

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 OpenText 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. Exit the installation wizard.
4. If you are using SSL for connector connection, complete the following steps:
 - a. From `$ARCSIGHT_HOME\current\bin`, execute the **keytoolgui** application to import the certificate that you exported. For more information, see [Exporting Security Certificate](#).

```
arcsight agent keytoolgui
```
 - b. Select `jre/lib/security/cacerts`, then select `import cert` to import your certificate. Verify that the correct certificate has been imported.
 - c. When prompted **Trust this certificate?**, click **Yes**.

- d. Save the keystore.
- e. Verify the imported certificates by entering this command from \$ARCSIGHT_HOME\current\bin:

```
arcsight agent keytool -list -store clientcerts
```

The new certificate is listed.
5. Execute `runagentsetup` from \$ARCSIGHT_HOME\current\bin to return to the configuration wizard.
6. Select **TippingPoint SMS Syslog Extended**, from the Type drop-down, then click **Next**.
7. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Network Port	Enter the port on which the connector listens for events.
IP Address	Enter the IP address on the connector listens for events. Use ALL (the default value) to bind to all available addresses.
Protocol	Select the protocol the connector is to use.
Default User Name	Enter the user name with which you access your TippingPoint SMS system.
Default Password	Enter the password for the Default User. The Default User Name and Default Password will be used for the hosts for which credentials are not provided in the host table.

8. Specify the following Host Table Parameters:

Parameter	Description
Hostname/IP	Enter the Hostname or IP address for each TippingPoint SMS system from which you want the connector to retrieve events. You can also delete any SMS systems from which you do not want the connector to retrieve payloads by selecting the host and clicking Delete.
Username	Enter the Username for each TippingPoint SMS system from which you want the connector to retrieve events.
Password	Enter the Password for each TippingPoint SMS system from which you want the connector to retrieve events.

9. Click **Export** to export the host name data you have entered into the table into a CSV file. Click **Import** to select a CSV file to import into the table rather than to add the data manually.
10. Select a [destination and configure parameters](#).
11. Specify a name for the connector.

12. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



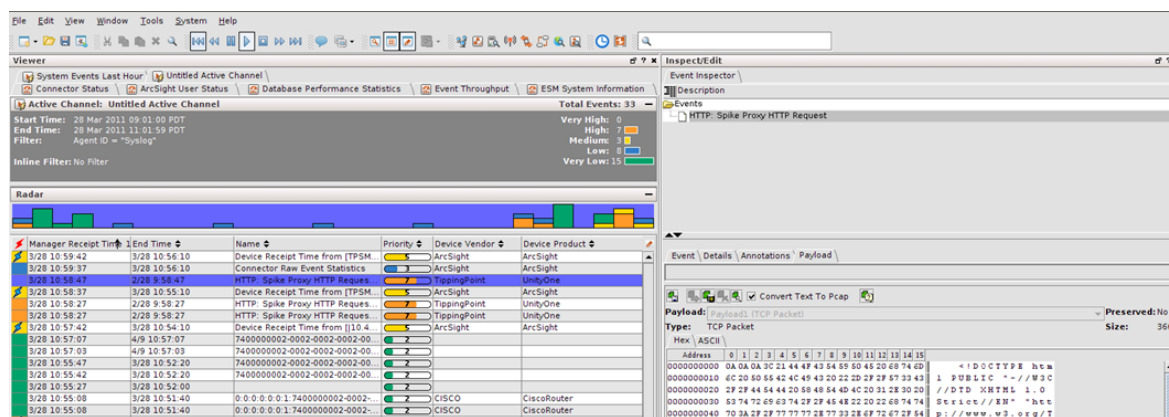
Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

13. Select whether you want to install the connector as a service or in the standalone mode.
14. Complete the installation.
15. [Run the SmartConnector](#).

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

Payload Support

The connector uses the event ID of events with payloads to retrieve the payload. Perform the following procedures to enable payload retrieval. Click on any of the vulnerability events sent by the SmartConnector and you will see in the Event Inspector that Payload data is available. Click on the **Payload** tab for additional information, including **Description** and **Recommendation**.



For services events, **Description** and **Detail** information is displayed.

During SmartConnector installation and configuration, you can set a **Payload Timeout** parameter. The default value for this parameter is 60 seconds. If you enter a value greater than 60 seconds for this parameter, certain properties also must be added to the console.properties file for the ESM Console and the server.properties file for the ESM Manager.

Add the following property to the console.properties file in the config folder on each ArcSight ESM Console machine:

```
console.payloadTimeout=value
```

where *value* is the number of seconds you will specify for the Payload Timeout parameter during connector installation.

Add the following properties to the server.properties file in the config folder of the ArcSight ESM Manager machine:

```
payload.eventrequest.timeout=value  
payload.eventrequest.maxretry=value  
payloadservice.requests.timeout=value
```

where *value* is the number of seconds you will specify for the Payload Timeout parameter during connector installation.

You can retrieve, preserve, view, or discard payloads using the ArcSight Console. Because event payloads are relatively large, ArcSight does not store them by default. Instead, you can request payloads from devices for selected events through the Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the Console.

Payloads are downloaded and stored only on demand; you must configure ESM to log these packets. By default, 256 bytes of payload will be retrieved.

Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

Locate Payload-Bearing Events

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view. In an ArcSight Console Viewer panel grid view, right-click a column header and choose **Add Column > Device > Payload ID**. Look for events showing a Payload ID in that column.

Retrieve Payloads

In a Viewer panel grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab, then click **Retrieve Payload**.

Preserve Payloads

In a grid view, right-click an event with an associated payload, select **Payload**, then **Preserve**. Alternatively, in the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

Discard Payloads

In a grid view, right-click an event with an associated payload and select **Payload**, then **Discard Preserved**. You also can use the Event Inspector: In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Discard Preserved Payload**.

Save Payloads to Files

In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Save Payload**. In the **Save** dialog box, navigate to a directory and enter a name in the **File name** text field. Click **Save**.

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/SMS 3.2, 3.3, 3.5, and 3.6 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 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

Troubleshooting

Why does my TippingPoint SMS lose events?

The connector can sometimes lose events when receiving UDP bursts from the device. To work around this problem, change the TippingPoint and connector settings to specify the TCP transport protocol rather than UDP.

TippingPoint SMS Console:

1. Open the TippingPoint SMS console.
2. Select **Server Properties** and click on the **Syslog** tab.
3. Click **Edit** to edit remote syslog notification settings.
4. For **Protocol**, check **TCP**.
5. Click **OK**.

SmartConnector:

1. From `$ARCSIGHT_HOME\current\bin`, enter:
`runagentsetup`
2. Follow the wizard to change the connector `Protocol` parameter from UDP to 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 TippingPoint SMS Syslog Extended SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!