Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for TippingPoint SMS Syslog Extended

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for TippingPoint SMS Syslog Extended

November 30, 2016

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/14/2014	Added support for SMS and IPS audit events for devices. Updated Device Product mapping.
11/15/2013	Added support for SMS 3.6.
09/30/2013	For syslog format 2.5, added mapping for Device Host Name and updated mapping for Device Custom String 5.
05/15/2013	Added support for SMS 3.5.
05/15/2012	Added new installation procedure.
02/15/2012	Updated IPv6 mappings.
11/15/2011	Added support for TippingPoint SMS 3.3.
05/16/2011	First version of Configuration Guide.

SmartConnector for TippingPoint SMS Syslog Extended

This guide provides information for installing the SmartConnector for TippingPoint SMS Syslog Extended and configuring the device for syslog event collection. SMS 3.2, 3.3, 3.5, and 3.6 are supported with SMS syslog format 2.5. CEF syslog event collection from SMS 3.3 devices is also supported. Support for SMS and IPS device audit events is also included.

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, that 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, be sure to:

- Choose 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.

Security Certificate

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

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**.

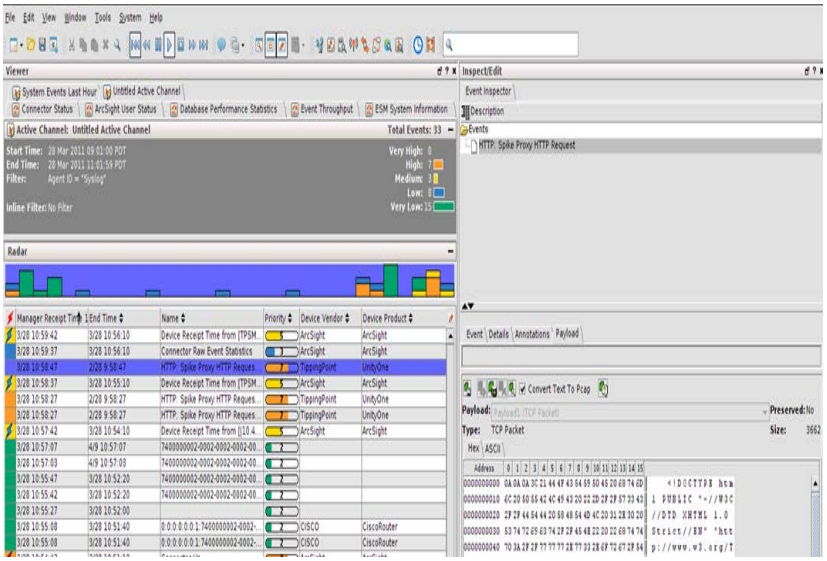
8 Enter the name of the file you want to export or click **Browse** and then navigate to the file. Make sure to note the name and location of the file; you will import the certificate during connector installation.

9 Click **Next**.

10 Click **Finish**.

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**.

Install the SmartConnector

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

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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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

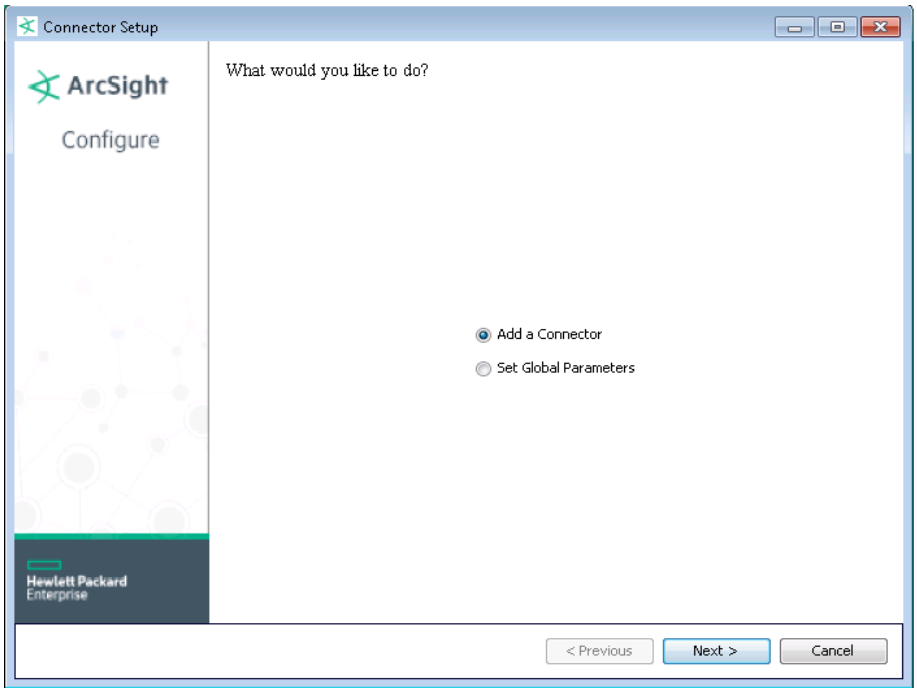
Install Core Software

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 HPE SSO and Protect 724 sites.

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

   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:



If you are using SSL for connector connection, follow these steps; otherwise, continue with step 4.

To import the certificate to the connector's certificate store:

A From `$ARCSIGHT_HOME\current\bin`, execute the **keytoolgui** application to import the certificate (see "Security Certificate" earlier in this guide).:

```
arcsight agent keytoolgui
```

The graphical interface asks you to open a keystore.

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.

F Return to the configuration wizard by entering the following command from `$ARCSIGHT_HOME\current\bin` and clicking **Yes** to use the Wizard.

```
arcsight connectorsetup
```

Set Global Parameters (optional)

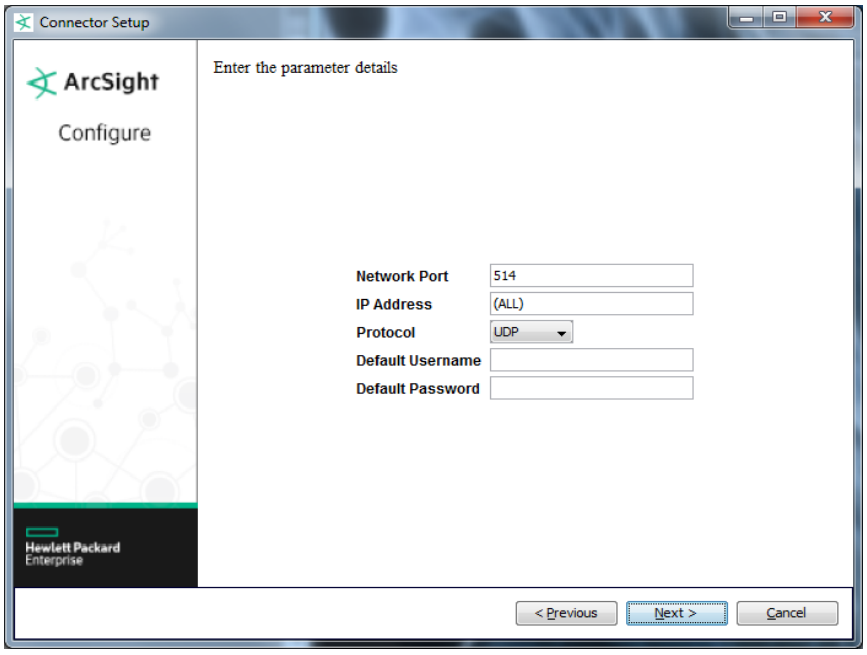
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

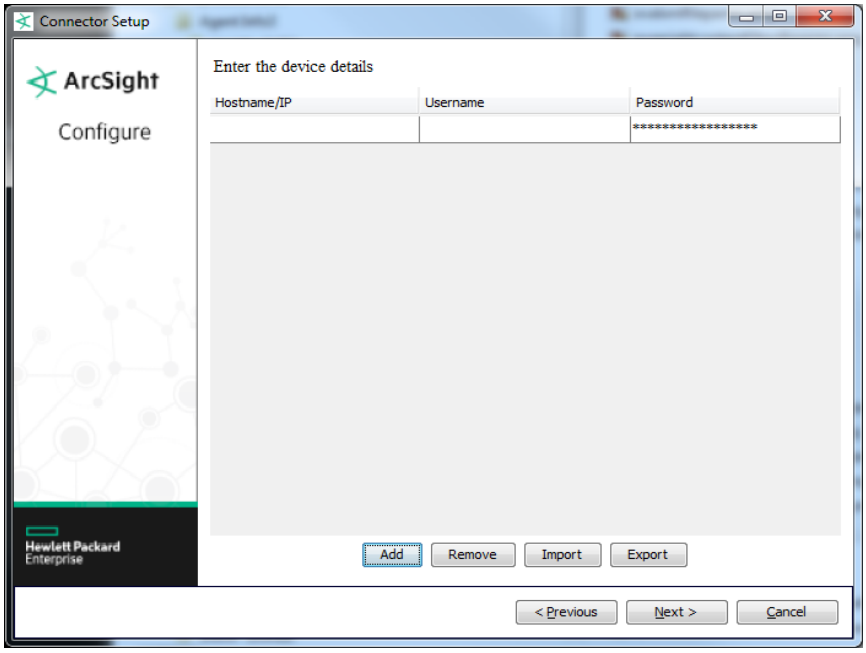
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote 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 'Disable'.
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	If 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. When both values are present, the initial setting is IPv4.

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 the "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 **TippingPoint SMS Syslog Extended** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.





Parameter	Description
Network Port	Enter the port to which the connector will listen for events.
IP Address	Enter the IP address to which the connector will listen 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. Click 'Next'. The Default User Name and Default Password will be used for the hosts for which credentials are not provided in the host table.
TippingPoint SMS Hosts Table Parameters:	
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.

You can click the 'Export' button to export the host name data you have entered into the able into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

Select a Destination

1. The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2. Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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. 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 some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

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.

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
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

ArcSight ESM Field	Device-Specific Field
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:

   ```
   arcsight connectorsetup
   ```

2. Follow the wizard to change the connector `Protocol` parameter from `UDP` to `TCP`.