Send Events to the Cloud Using Syslog

About Integration via Syslog

From release 6.3 onwards, you can use syslog to send supported events to the Cisco cloud from devices. You must set up an on-premises Cisco Security Services Proxy (CSSP) server and configure your devices to send syslog messages to this proxy.

Every 10 minutes, the proxy forwards collected events to Security Services Exchange (SSE), from where they can be automatically or manually promoted to incidents that appear in Cisco SecureX threat response.

Requirements for Integration Using Syslog

Requirement Type	Requirement
Device	Any device running a supported version of software.
Version	6.3 or later
Account on the Cisco SecureX threat response cloud that you will use	See Required Account for Cisco SecureX Threat Response Access.

Requirement Type	Requirement
Licensing	No special license is required for this integration. However: • Your system must be licensed to generate the events that you want to send to Cisco SecureX threat response. For details, see the Licensing Information. • This integration is not supported under an evaluation license. • Your environment cannot be deployed in an air-gapped environment.
General	Your system is generating events as expected.

How to Send Events to the Cisco Cloud Using Syslog

Note If your devices are already sending events to the cloud, you do not need to configure sending them again. SecureX and Cisco SecureX threat response use the same set of event data.

	Do This	More Information
Step	Decide which events you want to send to the cloud, the method of sending events and the regional cloud to use.	See the topics under Important Information About Integrating Secure Firewall Threat Defense and Cisco SecureX Threat Response.
Step	Meet the requirements.	See Requirements for Integration Using Syslog, on page 1.
Step	Access Security Services Exchange (SSE), the portal for Cisco SecureX threat response that you use for managing devices and filtering events.	See Access Security Services Exchange, on page 4.
Step	Install and configure a Cisco Security Services Proxy (CSSP) server.	Download the free installer and instructions from Security Services Exchange: In SSE, from the Tools button (🛠) near the top-right of the browser window, select **Downloads**.
Step	In Security Services Exchange, enable features.	Click **Cloud Services** and enable the following options: • **Cisco SecureX threat response** • **Eventing**

	Do This	More Information
Step	Configure your devices to send syslog messages for supported events to the proxy server.	• For devices managed by the device manager: Look in the device manager online help for information about "Configuring Syslog for Intrusion Events". • For devices managed by the management center: Look in the management center online help for information about syslog in the "Event Analysis Using External Tools" chapter.
Step	In your product, ensure that the messages identify the device that generated each event.	• In the device manager: Specify a hostname in **Device** > **Hostname**. • In the management center: In the Platform Settings **Syslog Settings** tab, **Enable Syslog Device ID** and specify an identifier.
Step	Allow time for your system to generate supported events.	--
Step	Verify that your events appear as expected in Security Services Exchange and troubleshoot if necessary.	See: • Verify that Events Reach Security Services Exchange (Via Syslog), on page 4. • Troubleshoot a Syslog Integration, on page 5.
Step	In Security Services Exchange, configure the system to automatically promote significant events.	**Important** If you do not automate event promotion, you must manually review and promote events to view them in Cisco SecureX threat response. See information in the online help in Security Services Exchange about promoting events. To access SSE, see Access Security Services Exchange, on page 4.
Step	(Optional) In Security Services Exchange, configure automatic deletion of certain nonsignificant events.	For more information on filtering events, see Security Services Exchange online help. To access SSE, see Access Security Services Exchange, on page 4.
Step	In SecureX, add a module. With this module configured, CTR will return sightings from intrusion events in SSE even if they have not been promoted.	In SecureX, navigate to **Integration Modules** > **Integration** and add a module. For more information about this module, see the online help in SecureX.

	Do This	More Information
Step	In Cisco SecureX threat response, verify that promoted events appear as expected in the Incident Manager.	In Cisco SecureX threat response, click **Incidents**.

Access Security Services Exchange

Before you begin

In your browser, disable pop-up blocking.

Procedure

Step 1 In a browser window, go to your SecureX cloud:

- North America cloud: https://securex.us.security.cisco.com
- Europe cloud: https://securex.eu.security.cisco.com
- Asia cloud: https://securex.apjc.security.cisco.com

Step 2 Sign in using the credentials for your SecureX, Secure Endpoint, Secure Malware Analytics, or Cisco Security account.

Your account credentials are specific to the regional cloud.

Step 3 Navigate to Security Services Exchange:

Select **Dashboard** > **Applications & Integrations** > **Security Services Exchange** and click **Launch**.

Security Services Exchange opens in a new browser window.

Verify that Events Reach Security Services Exchange (Via Syslog)

Before you begin

Verify that the events appear in the device as you expected.

Procedure

Step 1 Wait for about 15 minutes after your device has detected a supported event to allow messages to be forwarded from the proxy to Security Services Exchange.

Step 2 Access SSE. For more information, see Access Security Services Exchange, on page 4.

Step 3 In SSE, click **Events**.

Step 4 Look for events from your device.

If you do not see the expected events, see tips in Troubleshoot a Syslog Integration, on page 5 and look again at How to Send Events to the Cisco Cloud Using Syslog, on page 2.

Troubleshoot a Syslog Integration

Events are not reaching Cisco Security Services Proxy

Make sure your devices can reach Cisco Security Services Proxy on the network.

Problems accessing the cloud

- If you activate your cloud account immediately before attempting to configure this integration and you encounter problems implementing this integration, try waiting an hour or two and then log in to your cloud account.
- Make sure you are accessing the correct URL for the regional cloud associated with your account.

Expected events are missing from the Events list

Check the following:

- Click the **Refresh** button on the Events page to refresh the list.
- Verify that the expected events appear on the device.
- Check your configurations for automatic deletion (filtering out events) in the **Eventing** settings on the **Cloud Services** page in Security Services Exchange.
- Make sure you are viewing the regional cloud to which you are sending your events.

Questions about Syslog Fields

For syslog fields and descriptions, see the Threat Defense Syslog Messages.