Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide

First Published: 2019-06-26

Last Modified: 2023-09-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

Important Information About Integrating Secure Firewall Threat Defense and Cisco SecureX Threat Response

About Cisco SecureX Threat Response and This Integration

Cisco SecureX threat response (formerly Cisco Threat Response or CTR) is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats using data aggregated from multiple products and sources.

This integration sends supported events from devices to Cisco SecureX threat response for analysis alongside data from your other products and other sources.

For more information about Cisco SecureX threat response, see Cisco SecureX Threat Response product page. For videos about the use and benefits of the application on YouTube, see http://cs.co/CTRvideos.

If you do not already have a Cisco SecureX threat response account, you can create one using Cisco Defense Orchestrator (CDO). To create a Cisco SecureX threat response account from CDO, follow the instructions here.

For more information about this integration, see the FAQs at http://cs.co/ctr_firepower_faq and the online help in Cisco SecureX threat response, including the release notes.

Cisco SecureX Threat Response Regional Clouds

Region	Link to Cloud	Supported Integration Methods
North America	https://visibility.amp.cisco.com	• Direct integration: Release 6.4 and later • Integration via syslog: Release 6.3 and later
Europe	https://visibility.eu.amp.cisco.com	• Direct integration: Release 6.5 and later • Integration via syslog: Release 6.3 and later
Asia (APJC)	https://visibility.apjc.amp.cisco.com	• Direct integration: Release 6.5 and later • Integration via syslog: Release 6.3 and later

Guidelines and Limitations for Choosing a Regional Cloud

Before choosing a regional cloud, consider these important points:

- Selecting regional cloud depends on your version and integration method (syslog or direct).

  See Cisco SecureX Threat Response Regional Clouds, on page 2 for specifics.
- When possible, use the regional cloud nearest to your deployment.
- You cannot merge or aggregate data in different regional clouds.
- If you need to aggregate data from multiple regions, devices in all regions must send data to the same regional cloud.
- You can create an account on each regional cloud and the data on each cloud remains separate.
- The region you select in your product is also used for the Cisco Support Diagnostics and Cisco Support Network features, if applicable and enabled. For more information about these features, see the online help for your product.

Supported Event Types

The threat defense and Cisco SecureX threat response integration supports the following event types:

Table 1: Version Support for Sending Events to the Cisco Cloud

Feature	Devices Managed by Secure Firewall Management Center Version (Direct integrations)	Devices Managed by Secure Firewall Device Manager Version (Direct integrations)	Syslog
Intrusion (IPS) events	6.3 and later (via syslog) 6.4 and later (via direct connection)	6.3 and later (via syslog) 6.4 and later (via direct connection)	Supported
Security Intelligence connection events	6.5 and later	6.5 and later	Not supported
File and malware events	6.5 and later	6.5 and later	Not supported

Comparison of Methods for Sending Events to the Cloud

Devices make events available to Cisco SecureX threat response through the Security Services Exchange portal, either using syslog or directly.

Sending Events Directly	Sending Events Using Syslog Through a Proxy Server
Supports only threat defense (NGFW) devices running supported versions of software.	Supports all devices running supported versions of software.
Supports version 6.4 and later.	Supports version 6.3 and later.
Supports all event types listed in Supported Event Types, on page 2.	Supports only intrusion events.
Supports SecureX tiles that show system status information such as whether your appliances and devices are running the optimal software versions.	System status features are not supported with syslog-based integrations.
Threat defense devices must be connected to the internet.	Devices do not need to be connected to the internet.
Your deployment cannot be using a Smart Software Manager on-premises server (formerly known as a Smart Software Satellite Server).	Your deployment can be using a Smart Software Manager on-premises server.

Sending Events Directly	Sending Events Using Syslog Through a Proxy Server
No need to set up and maintain an on-premises proxy server.	Requires an on-premises virtual Cisco Security Services Proxy (CSSP) server. More information about this proxy server is available from the online help in Security Services Exchange (SSE). To access SSE, see Access Security Services Exchange, on page 26.

Best Practices

Follow guidelines and setup instructions in the following topics precisely, including Requirements topics and Before You Begin sections in referenced procedure topics:

- For all integrations:

  See Guidelines and Limitations for Choosing a Regional Cloud, on page 2.

- For direct integration:

  See How to Send Events Directly to the Cisco Cloud, on page 12.

- For integration using syslog:

  See How to Send Events to the Cisco Cloud Using Syslog, on page 24.

CHAPTER 2

Cisco Cloud Accounts

Required Account for Cisco SecureX Threat Response Access

To use Cisco SecureX threat response and associated tools including SSE, you must have one of the following accounts on the regional cloud:

- Cisco Security Account
- Secure Endpoint account
- Secure Malware Analytics account
- SecureX account

Important If you or your organization already has any of the above accounts on the regional cloud, use the existing account. Do not create a new account. Data associated with an account is available only to that account.

If you do not have an account, see Get an Account to Access Cisco SecureX Threat Response, on page 5.

Get an Account to Access Cisco SecureX Threat Response

Important If you or your organization already has an account on the regional cloud you want to use, do not create a new account. Use the existing account to access Cisco SecureX Threat Response.

Procedure

Step 1 Determine which Cisco SecureX threat response regional cloud you want to use:

See Guidelines and Limitations for Choosing a Regional Cloud, on page 2.

Step 2 If you do not already have an account on the regional cloud, ask your management if your organization already has any of the supported accounts for that cloud.

For supported account types, see Required Account for Cisco SecureX Threat Response Access, on page 5.

Step 3 If anyone else in your organization already has an account for that regional cloud:

Have the administrator of that account add an account for you. For instructions, see Manage Access to Your Cloud Accounts, on page 6.

Step 4 If you do not already have a Cisco SecureX Threat Response account, you can create one using Cisco Defense Orchestrator (CDO). To create a Cisco SecureX Threat Response account from CDO, follow the instructions here.

Manage Access to Your Cloud Accounts

Managing user accounts varies based on the type of cloud account you have.

Note If you access the cloud using a Secure Malware Analytics or Secure Endpoint account, see the documentation for those products.

Manage User Access to Your SecureX Account

If your organization uses a SecureX account to access the cloud, use this procedure to manage users.

Before you begin

Your SecureX account must have administrator-level privileges.

Procedure

Step 1 Sign in to your SecureX regional cloud.

Step 2 Click **Administration**.

Step 3 If you have questions, see the online help in SecureX.

Manage Access To Your Organization's Cisco Security Account

If you are a Cisco Security Account owner or administrator, you can grant additional users access to your organization's Cisco Security Account and manage existing users, including resending the account activation email.

Procedure

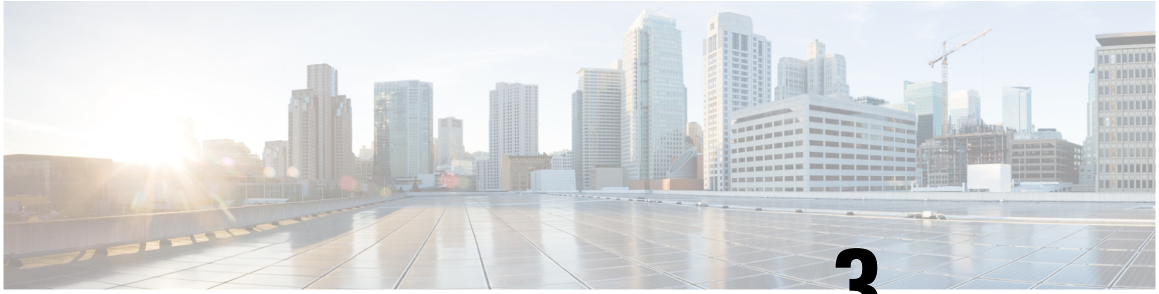
Step 1 Go to the appropriate URL for your regional cloud:

- North America: https://castle.amp.cisco.com
- Europe: https://castle.eu.amp.cisco.com
- Asia (APJC): https://castle.apjc.cisco.com

Step 2 Click **Users**.

Step 3 Add or edit user access.

If you select **Account Administrator**, the person will have permissions to grant and manage user access.



CHAPTER 3

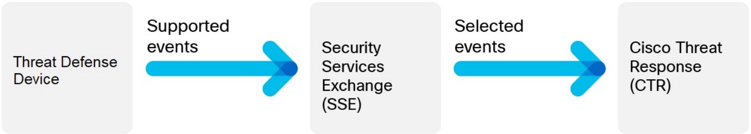
Send Events to the Cloud Directly

About Direct Integration

Beginning in release 6.4, you can configure your system to send supported events directly to the Cisco cloud from threat defense devices.

Specifically, your devices send events to Security Services Exchange (SSE), from where they can be automatically or manually promoted to incidents that appear in Cisco SecureX threat response.

You can also view information about system status, such as whether your appliances and devices are running current software versions.



Requirements for Direct Integration

Requirement Type	Requirement
Device	Threat defense devices. • Managed by the management center. • Managed by the device manager.

Requirement Type	Requirement
Version	US cloud: 6.4 or later EU cloud: 6.5 or later APJC cloud: 6.5 or later Version requirement applies both to devices and to the management center (if applicable).
Licensing	No special license is required for this integration. However: • Your system must be licensed to generate the events that you want to view in Cisco SecureX threat response. For details, see https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-licensing-information-listing.html. • This integration is not supported under an evaluation license. • Your environment cannot be using a Cisco Smart Software Manager On-Prem server (formerly known as Smart Software Satellite Server) or be deployed in an air-gapped environment.
Account	See Account Requirements for Direct Integration, on page 11.
Connectivity	Management center and managed devices must be able to connect outbound on port 443 to the Cisco cloud at the following addresses: • North America cloud: • api-sse.cisco.com • https://eventing-ingest.sse.itd.cisco.com • https://mx*.sse.itd.cisco.com • EU cloud (6.5 and later): • api-sse.cisco.com • api.eu.sse.itd.cisco.com • https://eventing-ingest.eu.sse.itd.cisco.com • https://mx*.eu.sse.itd.cisco.com • Asia (APJC) cloud (6.5 and later): • api.apj.sse.itd.cisco.com • https://mx*.apj.sse.itd.cisco.com • https://eventing-ingest.apj.sse.itd.cisco.com
General	Your system is generating events as expected.

Account Requirements for Direct Integration

- You must have an account for the regional cloud to which you want to send your event data.

  For supported account types, see Required Account for Cisco SecureX Threat Response Access, on page 5.

  If you or your organization already has an account on the regional cloud that you want to use, do not create another. You cannot aggregate or merge data in different accounts.

  To obtain an account, see Get an Account to Access Cisco SecureX Threat Response, on page 5.

  Your cloud account must have administrator-level privileges.

- You must have administrator privileges for the Cisco Smart Account from which your products are licensed.

  To determine your Smart Account user role, do the following:

  1. Go to https://software.cisco.com.
  2. Click **Manage Smart Account** and select a Smart Account in the top-right area of the page.
  3. Click **Users** tab and search for your User ID.

- Both your licensing Smart Account and the account you use to access the cloud must be associated with the same Cisco CCO account.

- Your account must have one of the following user roles:
  - Admin
  - Access Admin
  - Network Admin
  - Security Approver

High Availability Deployment and Cisco SecureX threat response Integration

Configuring High Availability requires two identical devices that are connected to each other through a dedicated failover link. The devices form an active/standby pair where the active device passes traffic. The standby device does not pass traffic, but synchronizes configuration and other state information from the active device. When the active device fails, the standby device takes over and helps to keep your network operational.

The following describes the guidelines for integrating threat defense High Availability deployment with Cisco SecureX threat response.

- To integrate threat defense High Availability or cluster deployment with SSE, you must integrate all peers with SSE.
- SSE integration requires all threat defense devices in the High Availability deployment to have connectivity to the internet.

- When integrating an active/standby management center deployment with Cisco SecureX threat response, you must integrate the active peer with Cisco SecureX threat response.
- If you promote the standby management center peer to active role, the Cisco SecureX threat response configuration gets transferred between the active and standby peers. The Cisco SecureX threat response ribbon continues to appear in both active and standby peers.
- If you break management center High Availability deployment, both the peers remain integrated with Cisco SecureX threat response.

See the Threat Defense and Management Center online help for more information about configuring and managing a High Availability deployment.

How to Send Events Directly to the Cisco Cloud

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	Make decisions about the events to send, the method of sending those events, the regional cloud to use, etc.	See the topics under Important Information About Integrating Secure Firewall Threat Defense and Cisco SecureX Threat Response, on page 1
Step	Meet requirements	Requirements for Direct Integration, on page 9 and its subtopics.
Step	In your browser, access Security Services Exchange, the cloud portal for Cisco SecureX threat response that you will use for managing devices and filtering events.	See Access Security Services Exchange, on page 14 .
Step	(Device Manager Only) If you are using Cisco Defense Orchestrator (CDO) to manage configurations on your threat defense device, you must merge your CDO account with the account you use for the services described in this document.	See Link Your Cisco Defense Orchestrator and SecureX or Cisco XDR Tenant Accounts, on page 14.
Step	In Security Services Exchange, link your licensing accounts so that you can view and work with event data from devices registered to different accounts in your organization.	See Link Smart Licensing Accounts, on page 16.

	Do This	More Information
Step	In Security Services Exchange, enable the eventing service.	Click **Cloud Services** and enable these options: • **Cisco SecureX threat response** • **Eventing**
Step	In your product, enable integration with the Cisco cloud.	**Tip:** Don't skip the prerequisites in these topics! • For devices managed by the device manager, see: Configure the Device Manager to Send Events to the Cisco Cloud, on page 17 • For devices managed by the management center, see: Configure the Management Center Devices to Send Events to the Cisco Cloud, on page 18
Step	Allow time for your system to generate events.	--
Step	Verify that your integration is set up correctly. If necessary, troubleshoot issues.	See: • Verify that Events Reach Security Services Exchange (Via Direct Connection), on page 20 • Troubleshoot a Direct Integration, on page 20
Step	In Security Services Exchange, configure the system to automatically promote significant events.	**Important** If you do not automate event promotion, you may need to manually review and promote events in order 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 14.
Step	(Optional) In Security Services Exchange, configure automatic deletion of certain non-significant events.	See information in the online help in Security Services Exchange about filtering events. To access SSE, see Access Security Services Exchange, on page 14.
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** > **Available Integration Modules** 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 will open in a new browser window.

Link Your Cisco Defense Orchestrator and SecureX or Cisco XDR Tenant Accounts

If your Firepower Threat Defense or Firepower Management Center device is used with Cisco Defense Orchestrator or Cisco Security Analytics and Logging (SaaS) and SecureX or Cisco XDR, you must link your Cisco Defense Orchestrator tenant account with the SecureX or Cisco XDR tenant account associated with the device.

Note the following:

- Only one Cisco Defense Orchestrator tenant account can be linked with one SecureX tenant account.
- If you have tenant accounts on more than one regional cloud, you must link tenant accounts separately for each regional cloud.
- If you link a SecureX or Cisco XDR tenant to Cisco Defense Orchestrator on one cloud, you do not need to do it again for Cisco XDR on the same cloud, and vice versa.

Note This operation is not reversible.

Before you begin

- You must be able to sign in to Cisco Defense Orchestrator and to the applicable regional SecureX or Cisco XDR cloud with your Security Cloud Sign On account.
- Your Cisco Defense Orchestrator user account must have admin or super admin privileges.
- Your SecureX or Cisco XDR user account must have admin privileges.

Procedure

Step 1 Sign in to the appropriate regional Cisco Defense Orchestrator site that contains the tenant you wish to link with SecureX or Cisco XDR.

For example, the US cloud is https://defenseorchestrator.com and the EU cloud is https://defenseorchestrator.eu.

Step 2 Choose the tenant to link with SecureX or Cisco XDR.

Step 3 Generate a new API token for your account:

a) From the user menu in the top right corner of the window, select **Settings**.
b) In the **My Tokens** section, click **Generate API Token** or **Refresh**.
c) Copy the token.

For more information about API tokens, see the online help in Cisco Defense Orchestrator at https://docs.defenseorchestrator.com/#!c-api-tokens.html.

Step 4 In Security Services Exchange, click the tools menu icon ☒ in the top right of any page and select **Link Cisco Defense Orchestrator Account**.

Step 5 Paste the token that you copied from Cisco Defense Orchestrator.

Step 6 Verify that you are linking the tenant that you intended to link.

Step 7 Click **Link Cisco Defense Orchestrator Account**.

Step 8 Sign out of your Cisco Defense Orchestrator account, and then sign back in.

What to do next

- Your account credentials do not change as a result of this procedure. After linking tenants, continue to use your Security Cloud Sign On account credentials to access each product (Cisco Defense Orchestrator, SaaS, SecureX, Cisco XDR, and so on) as before.
- If you completed this procedure before registering your devices to Security Services Exchange, continue with the steps in How to Send Events Directly to the Cisco Cloud, on page 12.
- If you performed this procedure after registering your devices for Cisco Defense Orchestrator and SecureX or Cisco XDR integration, you may have duplicate device instances on the Devices page in Security Services Exchange.

- In this case, the instance of your device that was previously associated with your Cisco Defense Orchestrator registration is now also associated with the linked SecureX or Cisco XDR tenant.
- Events generated by devices before linking tenants will have a different device ID than events generated by the same device after linking tenants.
- If you do not need to map events to the devices that generated them, you can delete the "Unregistered" device entries for devices that are now associated with the linked tenant.

Link Smart Licensing Accounts

To integrate products registered under different Smart/Virtual licensing accounts into a single view in the cloud, you must link those Smart/Virtual licensing accounts to the account that you use to access SecureX and Cisco SecureX threat response.

Before you begin

- To link Smart/Virtual licensing accounts, you must have administrator-level privileges for all of the Smart/Virtual licensing accounts, including the account you use to access SecureX or Cisco SecureX threat response.
- To link a Smart/Virtual licensing account, your SecureX or Cisco SecureX threat response username/email address must match the Smart/Virtual licensing account username/email address.

  If not, you can invite a user and create a SecureX sign-on account with an email address that matches the Smart/Virtual licensing account email address:

  1. Log in to SecureX as an administrator.
  2. Invite a user to join your SecureX organization by sending an invite to the email address that has Smart/Virtual licensing access. For details, see Inviting Users in the SecureX online help.
  3. Use the emailed invite to create a new SecureX sign-on account. During your first log in attempt, after you enter your username/email address, click **Other login options** and select **Cisco**. For details, see the SecureX sign-on guide.

- If you have accounts already linked for use with Cisco SecureX threat response, you do not need to link them again for SecureX, and vice-versa.
- To view linked accounts, a user-level account is sufficient.

Procedure

Step 1 In the top right corner of any page in Security Services Exchange, click the Tools button (🛠) and choose **Link Smart/Virtual Accounts**.

Step 2 Click **Link more accounts**.

Step 3 Select the accounts to integrate with this cloud account.

Step 4 Click **Link Smart/Virtual Accounts**.

Step 5 Click **OK**.

Unlink Smart Licensing Accounts

If you need to unlink Smart Licensing accounts that are currently linked, see instructions in the online help in Security Services Exchange (SSE).

Configure the Device Manager to Send Events to the Cisco Cloud

Note Available options depend on your device manager version. Skip any steps that are not applicable to your version. For example, the ability to select region and event types are version-dependent.

Before you begin

- Perform the steps up to this point in How to Send Events Directly to the Cisco Cloud, on page 12.
- In the device manager, make sure that your device has a unique name. If not, assign one now, in **Device > System Settings** > **Hostname**.
- In the device manager, apply intrusion and other applicable policies to at least one access control rule and verify that the device is successfully generating events.
- Make sure you have your cloud credentials and can sign in to the Cisco SecureX threat response regional cloud on which your account was created.

  For URLs, see Cisco SecureX Threat Response Regional Clouds, on page 2.
- In your browser:
  - Disable pop-up blocking.
  - Allow third-party cookies.

Procedure

Step 1 In the device manager: Click **Device**, then click the **System Settings** > **Cloud Services** link.

If you are already on the System Settings page, simply click **Cloud Services** in the table of contents.

Step 2 Click **Enable** for the **Send Events to the Cisco Cloud** option.

Step 3 Select the types of events to send to the cloud and click **OK**. Later, you can change the event selection by clicking **Edit** next to the list of selected events.

If you choose to send connection events, only Security Intelligence connection events are used in this integration.

Step 4 Verify that your device has registered successfully in Security Services Exchange:

a) If you do not already have Security Services Exchange open in a browser window, see Access Security Services Exchange, on page 14.

b) In Security Services Exchange, click **Devices**.

c) Verify that your threat defense device appears in the list.

Note: The description shown for the threat defense device in the Devices list is the serial number, which matches the serial number shown if you run the **show running-config** command in the command-line interface of the device.

What to do next

- If your deployment is a High Availability configuration, see High Availability Deployment and Cisco SecureX threat response Integration, on page 11 for more instructions.
- Continue with the remaining steps in How to Send Events Directly to the Cisco Cloud, on page 12.

Important If you enable integration with CDO after you configure sending events to the cloud, your devices may become unregistered from SSE. If you see this problem in the Devices tab of SSE, see Link Your Cisco Defense Orchestrator and SecureX or Cisco XDR Tenant Accounts, on page 14.

Configure the Management Center Devices to Send Events to the Cisco Cloud

Configure the management center to have managed threat defense devices send events directly to the cloud.

Note Available options depend on your management center version. Skip any steps that do not apply to your version.

Before you begin

- In the management center:
  - Go to the **System** > **Configuration** page and give your management center a unique name so it will be clearly identified in the Devices list in the cloud.
  - Add your threat defense devices to the management center, assign licenses to them, and ensure that the system is working correctly. (That is, you have created the necessary policies, and events are being generated and display as expected in the management center web interface under the Analysis tab.)
- Perform the steps up to this point in How to Send Events Directly to the Cisco Cloud, on page 12.
- Make sure you have your cloud credentials and can sign in to the Cisco SecureX threat response regional cloud on which your account was created.

  For URLs, see Cisco SecureX Threat Response Regional Clouds, on page 2.
- If you are currently sending events to the cloud using syslog, disable these sends to avoid duplication.

Procedure

Step 1 In the management center: Select **System** > **Integration**.

Step 2 Click **Cloud Services**.

Step 3 Enable the slider for **Cisco Cloud Event Configuration** or **Cisco Cloud** (depending on your management center version).

Step 4 If you have not already done so, and your management center offers a **Cisco Cloud Region** option: Select the Cisco Cloud Region on which you have created your account.

Step 5 Enable the types of events to send to the cloud.

Starting in release 7.0, events you send to the cloud can be used for multiple integrations:

Integration	Supported Event Options	Notes
Cisco Security Analytics and Logging (SaaS) (Starting with version 7.0)	All	High priority connection events include: • Security Intelligence connection events • Connection events related to file and malware events • Connection events related to intrusion events
Cisco SecureX and Cisco SecureX threat response	Depending on your version: • Some connection events* • Intrusion • File and malware events	* If you send connection events, Cisco SecureX and Cisco SecureX threat response support only Security Intelligence events.

Step 6 Click **Save**.

If the **Save** button is unavailable, this means the management center is already registered to the selected regional cloud.

Step 7 Verify that the feature is properly enabled:

a) Wait a few minutes to allow the systems to synchronize.

b) On the same page that you enabled the feature, click the link to view the Cisco Cloud configuration. (The link is in the same **Cisco Cloud** box.)

Security Services Exchange opens in a new browser window.

c) Sign in using the credentials that you use to access your Cisco SecureX threat response account.

d) Click **Devices**.

e) Verify that your management center and its managed devices appear on the list.

What to do next

Continue with the remaining steps in How to Send Events Directly to the Cisco Cloud, on page 12.

Verify that Events Reach Security Services Exchange (Via Direct Connection)

Before you begin

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

Procedure

Step 1 If you are not already working in Security Services Exchange, Access Security Services Exchange, on page 14.

Step 2 Click **Events**.

Step 3 Look for events from your device.

If you do not see expected events, see the tips in Troubleshoot a Direct Integration, on page 20 and look again at How to Send Events Directly to the Cisco Cloud, on page 12.

Troubleshoot a Direct Integration

Problems accessing the cloud

- If you activate your cloud account immediately before attempting to configure this integration and you encounter problems implementing this integration, wait for 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.

Device interface shows the integration as enabled, but the device does not appear on the Devices page in the cloud

- The device may be licensed using a Smart Account or virtual account that is not linked to your cloud account. Do one of the following:
  - In Security Services Exchange, link the account from which the device was licensed.

    See Link Smart Licensing Accounts, on page 16.
  - License the device from a linked account:

    Disable the integration on the Secure Firewall Management Center or Secure Firewall device manager, unregister the current license from the device, re-license the device from a linked account, then re-enable the integration in the Secure Firewall device manager or Secure Firewall Management Center.

- Make sure you are looking at the same regional cloud that you selected in your settings. If you didn't select a region when you started sending events to the cloud, try the North America cloud first.

Device managed by the Secure Firewall Management Center is not listed correctly on the Security Services Exchange Devices page

(Releases earlier than 6.4.0.4) Manually give the device a unique name: Click the **Edit** icon for each row in the Devices list. Suggestion: Copy the IP address from the Description.

This change is valid only for this Devices list; it does not appear anywhere in your deployment.

(Releases from 6.4.0.4 to 6.6) Device name is sent from the Secure Firewall Management Center to Security Services Exchange only at initial registration to Security Services Exchange and is not updated on Security Services Exchange if the device name changes in the Secure Firewall Management Center.

On the Devices page in Security Services Exchange, previously registered devices unexpectedly show as Unregistered

If these devices are threat defense devices managed by Secure Firewall device manager, and you enabled integration with Cisco Defense Orchestrator after you registered your devices with Security Services Exchange for integration with or Cisco SecureX threat response, and you have not yet merged your accounts, complete the procedure in Link Your Cisco Defense Orchestrator and SecureX or Cisco XDR Tenant Accounts, on page 14.

Expected events are missing from the Events list

- Make sure you are looking at the correct regional cloud and account.
- Make sure that your devices can reach the cloud and that you have allowed traffic through your firewall to all required addresses.
- Click the **Refresh** button on the **Events** page to refresh the list and verify that the expected events appear.
- If you are using Secure Firewall device manager, check your access rule logging settings.
- Check your configurations for automatic deletion (filtering out events) in the **Eventing** settings on the **Cloud Services** page in Security Services Exchange.
- For more troubleshooting tips, see the online help in Security Services Exchange.

Some events are missing

- If you send all connection events to the cloud, SecureX and Cisco SecureX threat response integrations uses only security connection events.
- If you are using custom Security Intelligence objects in the Secure Firewall Management Center including global block or allow lists and Secure Firewall threat intelligence director, you must configure Security Services Exchange to auto-promote events that are processed using those objects. See information in the Security Services Exchange online help about promoting events to incidents.

Failed to save the SecureX configuration

If the Secure Firewall Management Center page fails to save the SecureX configuration,

- Verify that the Secure Firewall Management Center has connectivity to the cloud.

- Ensure that you modify SecureX configuration from the global domain.

SecureX enablement failed due to timeout

After starting the configuration, Secure Firewall Management Center page waits 15 minutes to receive the authorization before it times out. Ensure that you complete the authorization within 15 minutes. Click **Enable SecureX** to start a new authorization request after a timeout.

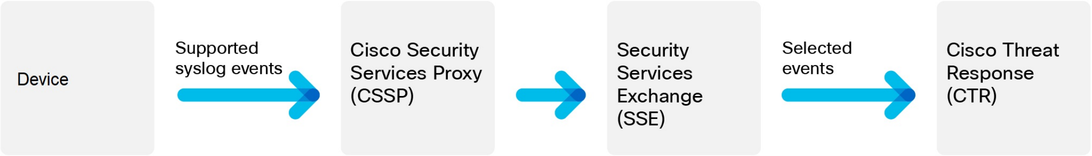
CHAPTER 4

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.



Device
Supported syslog events
Cisco Security Services Proxy (CSSP)
Security Services Exchange (SSE)
Selected events
Cisco Threat Response (CTR)

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, on page 5.

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, on page 1.
Step	Meet the requirements.	See Requirements for Integration Using Syslog, on page 23.
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 26.
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 26. • Troubleshoot a Syslog Integration, on page 27.
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 26.
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 26.
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 26.

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 27 and look again at How to Send Events to the Cisco Cloud Using Syslog, on page 24.

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.

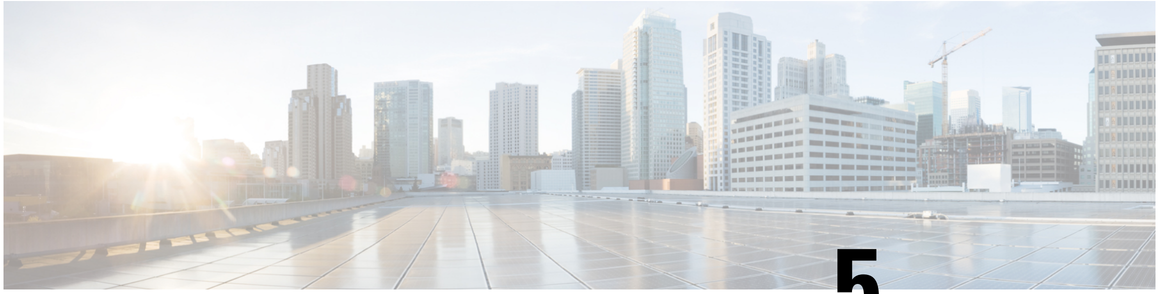
Expected events are missing from the Events list

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.



CHAPTER 5

Additional References

View Event Data in Cisco SecureX Threat Response (from Management Center)

Before you begin

- You will need your credentials to access Cisco SecureX threat response.
- Review the online help in Cisco SecureX threat response to learn how to find, investigate, and take action on threats.

Procedure

Step 1 Access Cisco SecureX threat response using one of the following methods:

- Access Cisco SecureX threat response via management center, by doing one of the following:
  - To pivot to Cisco SecureX threat response from a specific event:

    a. Navigate to a page under the **Analysis** > **Intrusions** menu that lists a supported event.

    b. Right-click a source or destination IP address and select **View in Threat Response**.
  - To view event info generally:

    a. Navigate to **System** > **Integrations** > **Cloud Services**.

    b. Click the link to view events in Cisco SecureX threat response.
- Access CTR directly:

  See links in Cisco SecureX Threat Response Regional Clouds, on page 2.

Step 2 Sign in to Cisco SecureX threat response as prompted.

Working in Cisco SecureX Threat Response

Events that are promoted to incidents are displayed on the **Incidents** page in Cisco SecureX threat response.

If an IP address that you are investigating in Cisco SecureX threat response was observed in an event, that event appears in the investigation dataset, even if the event was not promoted to incident.

For information on effectively using Cisco SecureX threat response to find, investigate, and take action on threats, see the online help in Cisco SecureX threat response.

See also SecureX threat response - FAQs.

Working in Security Services Exchange

For information about using Security Services Exchange or Cisco Security Services Proxy, see the online help in Security Services Exchange.