Send Events to the Cloud Directly

About Direct Integration

From release 6.4 onwards, 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 SecureX.

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

Requirements for Direct Integration

Requirement Type	Requirement
Secure Firewall Device	Threat defense devices managed by management center.
Secure Firewall Version	Managed Devices: • US cloud: 6.4 or later • EU cloud: 6.5 or later • APJC cloud: 6.5 or later Management Center version 7.0.2, version 7.2 and later.

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 view in SecureX. For details, see Cisco Secure Firewall Licensing Information. • You cannot perform this integration using 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 3.

Connectivity	The management center and the 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
	  • https://securex.us.security.cisco.com
	• EU cloud:
	  • api.eu.sse.itd.cisco.com
	  • https://eventing-ingest.eu.sse.itd.cisco.com
	  • https://mx*.eu.sse.itd.cisco.com
	  • https://securex.eu.security.cisco.com
	• Asia (APJC) cloud:
	  • api.apj.sse.itd.cisco.com
	  • https://eventing-ingest.apj.sse.itd.cisco.com
	  • https://mx*.apj.sse.itd.cisco.com
	  • https://securex.apjc.security.cisco.com

Requirement Type	Requirement
Requirement for appliance and device status features	If you want to view SecureX tiles that show system information such as whether your appliances and devices are running optimal versions: • You must send data to the cloud using a direct connection. • You must enable Cisco Success Network in your management center. To verify or enable this setting, go to **Integration** > **SecureX**. For more information, see Configure Cisco Success Network Enrollment. It takes up to 24 hours for appliance and device status tiles to update after you enable Cisco Success Network.
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 SecureX Access.

  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 SecureX.

  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 SecureX 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 SecureX.

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

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

About SecureX One-Click Integration Solution

When you enable SecureX using the one-click integration solution:

- The management center and the managed devices get registered to SSE using the SecureX organization.
- Device licensing and management of your system's cloud connections switches from Cisco Smart Licensing to your SecureX organization.
- The management center and managed devices send firewall events to cloud using theSecureX account.
- SecureX one-click integration solution allows you to view all firewall events in the SecureX platform without needing to manually link your Smart License with the SecureX.

When you enable the SecureX integration feature, the management center and the manged devices establishes a direct integration with the SecureX platform. The SecureX ribbon appears with every page in the management center, enabling you to quickly switch from management center to SecureX and cross-launch into other Cisco security products.

About SecureX Orchestration

SecureX Orchestration is a process automation platform for building workflows and atomic actions in SecureX with a low-to-no code approach. These workflows can interact with various resources and systems from Cisco or a third party.

Enabling this feature in management center allows the automated workflows created by SecureX users to interact with your management center resources.

For more information about the SecureX Orchestration feature, see the SecureX online help.

How to Send Events Directly to the Cisco Cloud

	Do This	More Information
Step	Decide on the type of events to send, the method of sending those events, and the regional cloud to use.	See the topics under Introduction to Integrating Secure Firewall Management Center and SecureX.
Step	Meet the requirements for direct integration.	See Requirements for Direct Integration.
Step	Configure the Cisco cloud region to send events.	See Configure the Management Center Devices to Send Events to the Cisco Cloud.
Step	Configure Secure Firewall Management Center-managed devices to send events to the cloud and select the types of events.	See Configure the Management Center Devices to Send Events to the Cisco Cloud.
Step	Enable SecureX integration with the management center.	See Integrate Secure Firewall Management Center and SecureX.
Step	Enable SecureX Orchestration if you want to allow the automated workflows created by SecureX users to interact with your management center.	See Integrate Secure Firewall Management Center and SecureX.
Step	Enable Cisco Success Network if you want to view SecureX tiles that show system information such as whether your appliances and devices are running optimal versions.	See Configure Cisco Success Network Enrollment.
Step	(Optional) Enable Cisco Support Diagnostics if you want to stream system health-related information to Cisco cloud and enable Cisco to proactively notify you of any issues.	See Configure Cisco Support Diagnostics Enrollment.

	Do This	More Information
Step	Add a Firepower module in your SecureX interface.	In SecureX, navigate to **Integration Modules > Available Integration Modules** and add a Firepower module. For more information about this module, see the online help in SecureX.

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

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

Before you begin

- In the management center:
  - Go to the **System > Configuration** page and give your management center a unique name to clearly identify it 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 works correctly. Create necessary policies and ensure that the generated events appear as expected in the management center web interface under the **Analysis** menu.
- Make sure you have your cloud credentials and can sign in to the SecureX regional cloud on which your account was created.

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

Step 1 Determine the Cisco regional cloud you want to use for sending firewall events. See Guidelines and Limitations for Choosing a Regional Cloud.

Note If SecureX is enabled and the management center is registered to the selected regional cloud, changing the regional cloud disables SecureX. You can enable the SecureX again after changing the regional cloud.

Step 2 In your management center, go to **Integration** > **SecureX**.

Step 3 Select a regional cloud from the **Current Region** drop-down.

Step 4 Enable the Cisco cloud event configuration and select the event types that you want to send to the cloud.

a. Check the **Send events to the cloud** check box to enable the configuration.

b. Select the event types that you want to send to the cloud.

Note Multiple integrations can use the events you send to the cloud. See the following table:

Integration	Supported Event Options	Notes
Cisco Security Analytics and Logging (SaaS)	All	High priority connection events include: • Security-related 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 all connection events, Cisco SecureX and Cisco SecureX threat response support only Security events.

Note
- If you enable **Intrusion Events**, the management center device sends the event along with the impact flag.
- If you enable **File and Malware Events**, in addition to the events sent from the threat defense devices, the management center devices send retrospective events.

Step 5 Click **Save**.

Integrate Secure Firewall Management Center and SecureX

This procedure describes how to integrate the management center with SecureX, enabling you to view your firewall events in the SecureX platform.

Before you begin

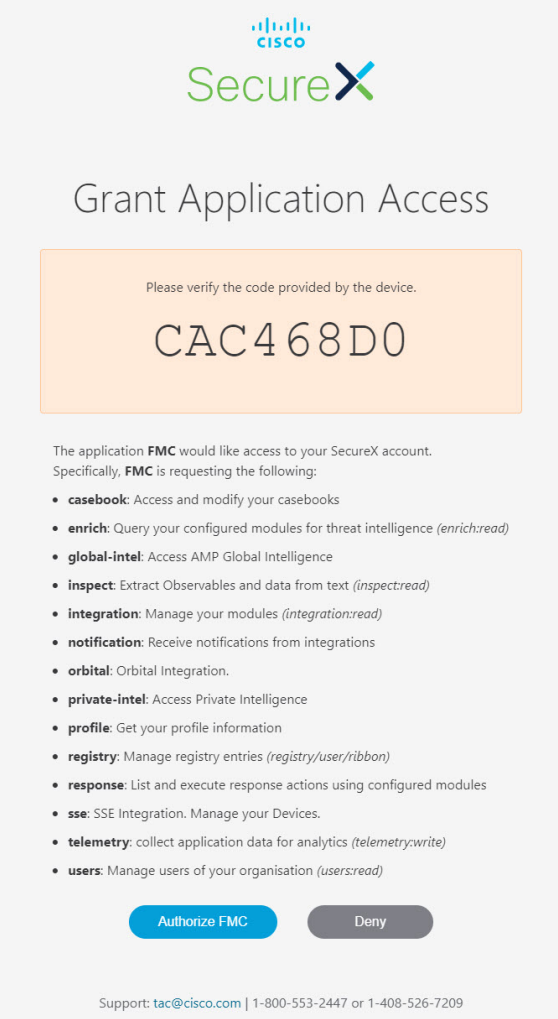
- Ensure that your SecureX Sign-On account is active.
- Ensure that you have administrator privileges in your SecureX account before making configuration changes.
- Ensure that you are modifying the configuration from the global domain.
- Ensure that the **Cisco SecureX threat response** and **Eventing** services are enabled in SSE. Verify this setting under **Security Services Exchange** > **Cloud Services**.
- Ensure that you have selected the regional cloud and enabled Cisco cloud event configuration. For more information, see Configure the Management Center Devices to Send Events to the Cisco Cloud, on page 6.

Step 1 In your management center, go to **Integration** > **SecureX**.

Step 2 Under **SecureX Enablement**, click **Enable SecureX**. The SecureX login page opens in a new browser window.

Step 3 Switch to the SecureX window and sign in to SecureX using the SecureX Sign-On account.

Step 4 Verify whether the code that is displayed on the SecureX page matches with the code that is displayed on your management center page and click **Authorize FMC**.



Note By authorizing, you are allowing Secure Firewall Management Center with the listed scopes to access your SecureX account.

Step 5 Return to your management center web interface.

Step 6 Configure the orchestration feature if you want to allow the automated workflows that are created by SecureX users to interact with your management center. To configure the orchestration feature, do the following:

a. Check the **Enable SecureX Orchestration** check box.

b. Choose the required role for the SecureX user to interact with management center resources using API. Choose a role from the **Assigned Role** drop-down list.

Note If you do not assign a role, Access Admin role is set by default.

Step 7 Click **Save** to save the configuration.

You can view the task progress under **Notifications** > **Tasks**. After successful completion of the device registration task, SecureX ribbon appears at the bottom of your management center page.

If you must use management center while the device registration task is in progress, open the management center in a new window.

What to do next

- Enable Cisco Success Network if you want to view the SecureX tiles that show system information such as whether your appliances and devices are running optimal versions.
- In your SecureX interface, add a Firepower integration module. For more information, see the SecureX online help.

Configure Cisco Success Network Enrollment

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the management center and the Cisco cloud to stream usage information and statistics. Streaming this telemetry provides a mechanism to select data of interest from the management center and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that is available for your product.
- (If you integrate with SecureX) To summarize appliance and device status in SecureX tiles and know whether all of your devices are running optimal software versions.
- To help Cisco improve our products.

The management center establishes and maintains a secure connection with the Cisco cloud at all times when you enable either Cisco Support Diagnostics or Cisco Success Network. You can turn off this connection at any time by disabling both Cisco Success Network and Cisco Support Diagnostics, which disconnect management center from the Cisco cloud. However, when you enable Cisco Support Diagnostics, both threat defense and the management center establish and maintain secure connections with the Cisco cloud.

You enable Cisco Success Network when you register the management center with the Smart Software Manager. Use the following procedure to view or change the enrollment status.

Note Cisco Success Network does not work in evaluation mode.

Note The Cisco Success Network feature is disabled if the management center has a valid Smart Software Manager On-Prem (formerly known as Smart Software Satellite Server) configuration, or uses Specific License Reservation.

Step 1 Click **Integration** > **SecureX**.

Step 2 Under **Cisco Cloud Support**, check the **Enable Cisco Success Network** check box to enable this service.

Note Read the information provided next to the **Enable Cisco Success Network** check box before you proceed.

Step 3 Click **Save**.

Configure Cisco Support Diagnostics Enrollment

Cisco Support Diagnostics is a user-enabled cloud-based TAC support service. When enabled, the management center and the managed devices establish a secure connection with the Cisco cloud to stream system health-related information.

Cisco Support Diagnostics provides an enhanced user experience during troubleshooting by allowing Cisco TAC to securely collect essential data from your device during a TAC case. Moreover, Cisco periodically collects the health data and processes it using an automated problem detection system to notify you of any issues. While the data collection service during a TAC case is available for all users with support contracts, the notification service is available only to customers with specific service contracts.

When you enable either Cisco Support Diagnostics or Cisco Success Network, the management center establishes and maintains a secure connection with the Cisco cloud. You can turn off this connection at any time by disabling both Cisco Success Network and Cisco Support Diagnostics which disconnect these features from the Cisco cloud. However, when you enable Cisco Support Diagnostics, both threat defense and the management center establish and maintain secure connections with the Cisco cloud.

Administrators can view a sample data set collected from the management center by following the steps in Producing Troubleshooting Files for Specific System Functions to generate a troubleshooting file, and then by opening the file to view it.

The management center sends the collected data to the regional cloud selected under the **Current Region** drop-down on **Integration** > **SecureX** page.

You enable Cisco Support Diagnostics when you register the management center with the Smart Software Manager. Use the following procedure to view or change Cisco Support Diagnostics enrollment status.

Step 1 Click **Integration** > **SecureX**.

Step 2 Under **Cisco Cloud Support**, check the **Enable Cisco Support Diagnostics** check box to enable this service.

Note Read the information provided next to the **Enable Cisco Support Diagnostics** check box before you proceed.

Step 3 Click **save**.

What to do next

If you have enabled Cisco Support Diagnostics, click **Integration** > **SecureX** and verify the regional cloud setting under **Cloud Region**.

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 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.

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.
- 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.

Failed to register Firewall devices to Security Services Exchange under SecureX organization

When Secure Firewall Management Center fails to register managed devices to SSE under SecureX organization, a message appears under **Notification** > **Tasks**. The management center restores the original configuration. When device registration fails, verify the following:

- Your SecureX account has administrator privileges.
- Firewall Management Center has connectivity to Security Services Exchange.

Disable and enable the SecureX configuration to register firewall devices to Security Services Exchange again.