



# Cisco Secure Firewall Management Center and Security Analytics and Logging (SaaS) Integration Guide

**First Published:** 2020-07-21

**Last Modified:** 2022-11-08

## Integrating Secure Firewall Management Center and Cisco Security Analytics and Logging (SaaS)

If you require additional space to store Secure Firewall Threat Defense events, you can send threat defense events to the Stealthwatch Cloud for storage using Cisco Security Analytics and Logging (SaaS), and optionally make your threat defense event data available for security analytics using Stealthwatch Cloud. Depending on the license, you can view the events in Cisco Defense Orchestrator (CDO) or Stealthwatch.

This integration is specifically for threat defense devices managed by management center. This document does not apply to devices that are not running threat defense software, to devices managed by Secure Firewall device manager, or to non-threat defense devices managed by management center.

For more information about Cisco Security Analytics and Logging (SaaS), see <https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html>.

## Comparison of Cisco Security Analytics and Logging Remote Event Storage Options

Similar but different options for storing event data externally to your management center:

On Premises	SaaS
You purchase, license, and set up the storage system behind your firewall.	You purchase licenses and a data storage plan and send your data to the Cisco cloud.
Supported event types: <ul style="list-style-type: none"><li>• Connection</li><li>• Security-related connection</li><li>• Intrusion</li><li>• File and Malware</li><li>• LINA</li></ul>	Supported event types: <ul style="list-style-type: none"><li>• Connection</li><li>• Security-related connection</li><li>• Intrusion</li><li>• File and Malware</li></ul>

On Premises	SaaS
Supports both syslog and direct integration.	Supports both syslog and direct integration. See <a href="#">Comparison of Methods for Sending Events to the Cloud, on page 2</a> .
<ul style="list-style-type: none"> <li>• View all events on the Secure Network Analytics Manager.</li> <li>• Cross-launch from management center event viewer to view events on the Secure Network Analytics Manager.</li> <li>• View remotely stored connection and Security-related connection events in management center</li> </ul>	View events in CDO or Secure Network Analytics, depending on your license. Cross-launch from management center event viewer.
For more information, see links in the Data Storage chapter in the <i>Secure Firewall Management Center Administration Guide</i> or online help.	

## Comparison of Methods for Sending Events to the Cloud

Sending via Syslog	Sending Directly
<ul style="list-style-type: none"> <li>• Requires Secure Event Connector (SEC)</li> <li>• Beneficial for high log emission rates from firewalls as each SEC can support up to 100,000 events per second</li> <li>• SEC can be set up for CDO or non-CDO-managed devices.</li> <li>• Reduces the event processing strain on the firewall, thereby freeing its resources for the firewall function.</li> <li>• Centralization is not always possible or desirable, especially for geographically distributed environments.</li> <li>• Requires a separate installation</li> </ul>	<ul style="list-style-type: none"> <li>• Ideal for branch offices as it supports geographically distributed environments.</li> <li>• Requires Smart Licensing.</li> </ul> <p>Not supported if you are using a Cisco Smart Software Manager On-Prem server (formerly known as Smart Software Satellite Server) or air-gapped deployment.</p> <ul style="list-style-type: none"> <li>• No separate installation or service is needed.</li> <li>• The strain on the firewall resources is relatively higher.</li> </ul>

## Requirements and Prerequisites for SAL (SaaS) Integration

The following requirements apply to both methods of sending events to SAL (SaaS).

Requirement or Prerequisite Type	Requirement
Devices and manager	<p>Management Center managing threat defense devices</p> <p>To send via syslog: version 6.4 or later</p> <p>To send directly: version 7.0</p> <p>The required version applies to the management center and all managed threat defense devices.</p> <p>Your system must be deployed and successfully generating events.</p>
Regional cloud	<p>Determine which regional cloud you will send events to.</p> <p>Events cannot be viewed from or moved between different regional clouds.</p> <p>If you use a direct connection to send events to the cloud for integration with SecureX or Cisco SecureX threat response, you must use the same regional CDO cloud for this integration.</p> <p>If you send events directly, the regional cloud you specify in management center must match the region of your CDO tenant.</p>
Data plan	<p>Determine the amount of cloud storage your system will require:</p> <p>See <a href="#">Calculate Storage Requirements and Purchase a Data Plan, on page 4</a>.</p>
Licensing	<ul style="list-style-type: none"> <li>• Cisco Security Analytics and Logging licenses: Any For licensing options and descriptions, see <a href="#">SAL (SaaS) Licenses, on page 4</a>.</li> <li>• CDO licenses: No additional CDO licensing is required.</li> <li>• Stealthwatch Cloud licenses: No additional licensing is required.</li> <li>• Management Center Licenses: No additional licensing is required.</li> </ul>
Accounts	<p>When you purchase a license for this integration, you will be provided with a CDO tenant account to support this functionality.</p>
Supported event types	<p>Intrusion, connection, Security-related connection, file, and malware events</p>
User roles	<p>In management center:</p> <ul style="list-style-type: none"> <li>• Admin</li> <li>• Access Admin</li> <li>• Network Admin</li> <li>• Security Approver</li> </ul>
Additional requirements when sending events directly	<p>See <a href="#">Prerequisites for Direct Integration, on page 12</a>.</p>

Requirement or Prerequisite Type	Requirement
Additional prerequisites	See the Before You Begin or Prerequisites section of each procedure.

## SAL (SaaS) Licenses

License	Details
Free trial	To get a 30 day free trial license, visit <a href="https://info.secureanalytics.com/sal-trial.html">https://info.secureanalytics.com/sal-trial.html</a> .
Logging and Troubleshooting	Store events in the Cisco cloud, and view and filter stored events using the CDO web interface.
(Optional) Logging Analytics and Detection	<p>The system can apply Stealthwatch Cloud dynamic entity modeling to your threat defense events, and use behavioral modeling analytics to generate Stealthwatch Cloud observations and alerts. You can cross-launch from CDO to a Stealthwatch Cloud portal provisioned for you, using Cisco Single Sign-On.</p> <p>When you purchase a license for SAL, you will be provided access to a CDO tenant for log viewing and a SWC instance for threat detections. Users of SAL do not need a separate CDO or SWC license to access these two portals for the outcomes that SAL provides.</p>
(Optional) Total Network Analytics and Detection	<p>The system applies dynamic entity modeling to both your threat defense events and your network traffic, and generates observations and alerts. You can cross-launch from CDO to a Stealthwatch Cloud portal provisioned for you, using Cisco Single Sign-On.</p> <p>When you purchase a license for SAL, you will be provided access to a CDO tenant for log viewing and a SWC instance for threat detections. Users of SAL do not need a separate CDO or SWC license to access these two portals for the outcomes that SAL provides.</p>

For details about SAL (SaaS) licensing options, see the *Cisco Security Analytics and Logging Ordering Guide* at <https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>.

SAL (SaaS) licenses provide the right to use a Cisco Defense Orchestrator tenant to view firewall logs and a Stealthwatch Cloud (SWC) instance for analytics, without holding separate licenses for either of these products.

To purchase SAL (SaaS) licenses, contact your authorized Cisco sales representative, or see the ordering guide (link above) and look for PIDs starting with **SAL-SUB**.

Additional information about this product is here: <https://apps.cisco.com/Commerce/guest>.

## Calculate Storage Requirements and Purchase a Data Plan

You need to buy a data plan that reflects the number of events the Cisco cloud receives from your threat defenses on a daily basis. This is called your "daily ingest rate."

To estimate your data storage requirements:

- (Recommended) Participate in a free trial of Cisco Security Analytics and Logging (SaaS) before you buy it. See [SAL \(SaaS\) Licenses, on page 4](#).
- Use the Logging Volume Estimator Tool at <https://ngfwpe.cisco.com/ftd-logging-estimator>.

Data plans are available in various daily volumes, and in various yearly terms. See the *Cisco Security Analytics and Logging Ordering Guide* at <https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html> for information about data plans.



**Note** If you have a SAL (SaaS) license and data plan, then obtain a different license at a later date, that alone does not require you to obtain a different data plan. If your network traffic throughput changes and you obtain a different data plan, that alone does not require you to obtain a different SAL (SaaS) license.

## How to Send Events from Management Center to SAL SaaS

To successfully deploy this integration, follow all of the steps in one of these topics:

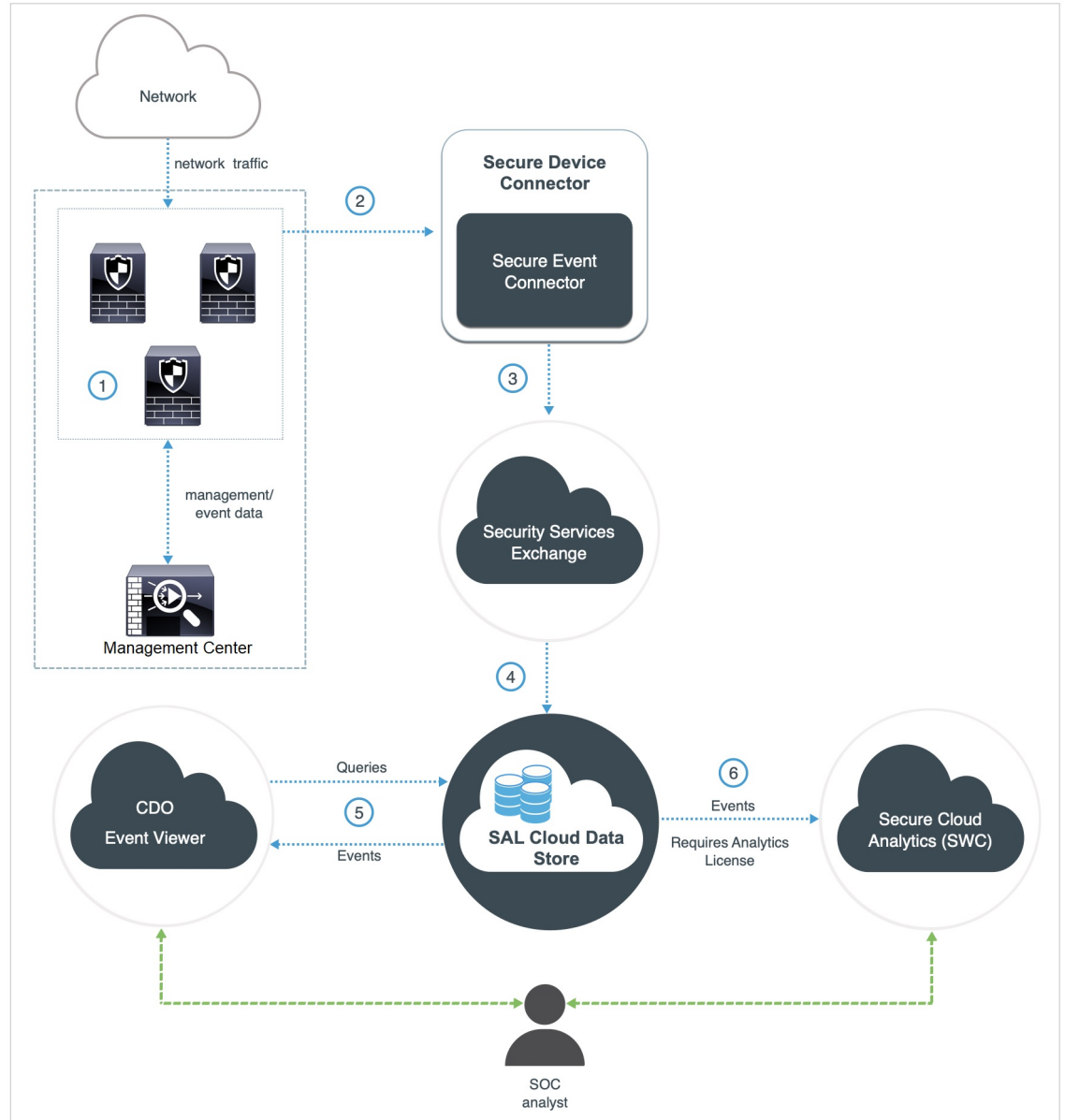
- [How to Set Up Event Data Storage in SAL \(SaaS\) Using a Direct Connection, on page 10](#)
- [How to Set Up Event Data Storage in SAL \(SaaS\) Using Syslog, on page 5](#)

## How to Set Up Event Data Storage in SAL (SaaS) Using Syslog

	Do This	More Information
Step	Review requirements and prerequisites	See <a href="#">Requirements and Prerequisites for SAL (SaaS) Integration, on page 2</a> .
Step	Obtain required licenses, accounts, and a data storage plan	Contact your authorized Cisco sales representative.
Step	Set up CDO access using multi-factor authentication	See instructions in the CDO online help for <a href="#">Signing in to CDO</a> .

	Do This	More Information
Step	Set up an on-premises Secure Device Connector (SDC) on a VMWare virtual machine	<p>This component is required solely to enable installation of the SEC, which is the component to which your devices will send events.</p> <p>Use one of the following, as described in the CDO online help:</p> <ul style="list-style-type: none"> <li>• (Preferred) <a href="#">Use the CDO-provided VM image</a>.</li> <li>• <a href="#">Create an SDC without using the CDO-provided image</a>.</li> </ul> <p><b>Important!</b> Don't skip the procedure prerequisites. However, ignore any information about onboarding, which does <i>not</i> apply to this integration.</p>
Step	Install the Secure Event Connector (SEC) on the SDC virtual machine you just created.	<p>This is the component to which your devices will send events.</p> <p>See the CDO online help for instructions to <a href="#">Install the Secure Event Connector</a>.</p> <p><b>Important!</b> Don't skip the procedure prerequisites. However, ignore any information about onboarding, which does <i>not</i> apply to this integration.</p>
Step	Configure your management center to have managed devices send syslog events to the SEC.	<a href="#">Send Security Event Syslog Messages from Threat Defense Devices, on page 8</a>
Step	Verify that your events are being sent successfully	See <a href="#">View and Work with Events, on page 23</a> .
Step	(Optional) If you are sending connection events to the cloud and you don't want to store them on the management center, disable that storage on the management center.	In the management center online help, see information about connection events in the Database Event Limits topics.
Step	(Optional) Configure cross-launches from management center to CDO so you can easily pivot from events displayed in management center to related events in the cloud.	See the online help in management center.
Step	(Optional) Configure general settings in CDO	<p>For example, you can make your data unavailable to Cisco support staff.</p> <p>In the CDO online help, see <a href="#">General Settings</a>.</p>
Step	(Optional) Create CDO user accounts for colleagues to view and work with your events.	In the CDO online help, see <a href="#">Create a New CDO User</a> .

## Overview of Sending Events to SAL (SaaS) Using Syslog



1	The management center-managed devices generate events.
2	The threat defense devices send supported events as syslog messages to a Secure Event Connector (SEC) installed on a virtual machine on your network.
3	The SEC forwards the events to Security Services Exchange (SSE), a secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.
4	The SSE forwards the events to the Cisco Security Analytics and Logging (SAL) Cloud Data Store.

5	The CDO Event Viewer queries SAL Cloud Data Store for events and provides the SOC analyst with additional context.
6	(Only with Analytics License) Cisco Secure Cloud Analytics (formerly SWC) receives the events from the SAL Cloud Data Store and provides the SOC analyst access to the analytics features of the product.



**Note** Most features in the CDO portal are not applicable to this integration. For example, CDO does not manage your devices, so your devices are not onboarded to CDO.

## Send Security Event Syslog Messages from Threat Defense Devices

This procedure documents the best practice configuration for sending syslog messages for security events (connection, Security-related connection, intrusion, file, and malware events) from threat defense devices managed by management center.



**Note** Many threat defense syslog settings are not applicable to security events. Configure only the options described in this procedure.

### Before you begin

- In management center, configure policies to generate security events and verify that the events you expect to see appear in the applicable tables under the Analysis menu.
- Gather the syslog server IP address, port, and protocol (UDP or TCP):  
Sign in to CDO. Then, from the user menu at the top right side of the CDO browser window, select **Secure Connectors**. Click **Secure Event Connector** and you will see the required information at the right side.
- Ensure that your devices can reach the syslog server(s).
- See additional information in the "Connection Logging" chapter in the Management Center online help.

### Procedure

**Step 1** Sign in to your management center web interface.

**Step 2** Configure syslog settings for your threat defense device:

- Click **Devices > Platform Settings**.
- Edit** the platform settings policy associated with your threat defense device.
- In the left navigation pane, click **Syslog**.
- Click **Syslog Servers** and click **Add** to enter server, protocol, interface, and related information.

Use the IP address, port, and protocol that you gathered from CDO above.

EMBLEM format and secure syslog are not supported for this integration.




If you have questions about options on this page, see the "Configure a Syslog Server" topic in the management center online help.

- e) Click **Syslog Settings** and configure the following settings:
  - **Enable Timestamp on Syslog Messages**
  - **Timestamp Format**
  - **Enable Syslog Device ID**
- f) Click **Logging Setup**.
- g) Make sure **Send syslogs in EMBLEM format** is NOT selected.
- h) **Save** your settings.

**Step 3** Configure general logging settings for the access control policy (including file and malware logging):

- a) Click **Policies > Access Control**.
- b) Edit the applicable access control policy.
- c) Click **Logging**.
- d) Select **FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device**.
- e) (Optional) Select a **Syslog Severity**.
- f) If you will send file and malware events, select **Send Syslog messages for File and Malware events**.
- g) Click **Save**.

**Step 4** Enable logging for Security-related connection events for the access control policy:

- a) In the same access control policy, click the **Security Intelligence** tab.
- b) In each of the following locations, click **Logging** (  ) and enable beginning and end of connections and **Syslog Server**:
  - Beside **DNS Policy**.
  - In the **Block List** box, for **Networks** and for **URLs**.
- c) Click **Save**.

**Step 5** Enable syslog logging for each rule in the access control policy:

- a) In the same access control policy, click the **Rules** tab.
- b) Click a rule to edit.
- c) Click the **Logging** tab in the rule.
- d) Enable both beginning and end of connections.
- e) If you will log file events, select **Log Files**.
- f) Enable **Syslog Server**.
- g) Verify that the rule is "**Using default syslog configuration in Access Control Logging**."  
Do NOT configure overrides.
- h) Click **Add**.
- i) Repeat for each rule in the policy.

**Step 6** If you will send intrusion events:

- a) Navigate to the intrusion policy associated with your access control policy.
- b) In your intrusion policy, click **Advanced Settings > Syslog Alerting > Enabled**.

Verify that the policy is using the default settings configured for access control logging.

- c) Click **Back**.
  - d) Click **Policy Information** in the left navigation pane.
  - e) Click **Commit Changes**.
- 

#### What to do next

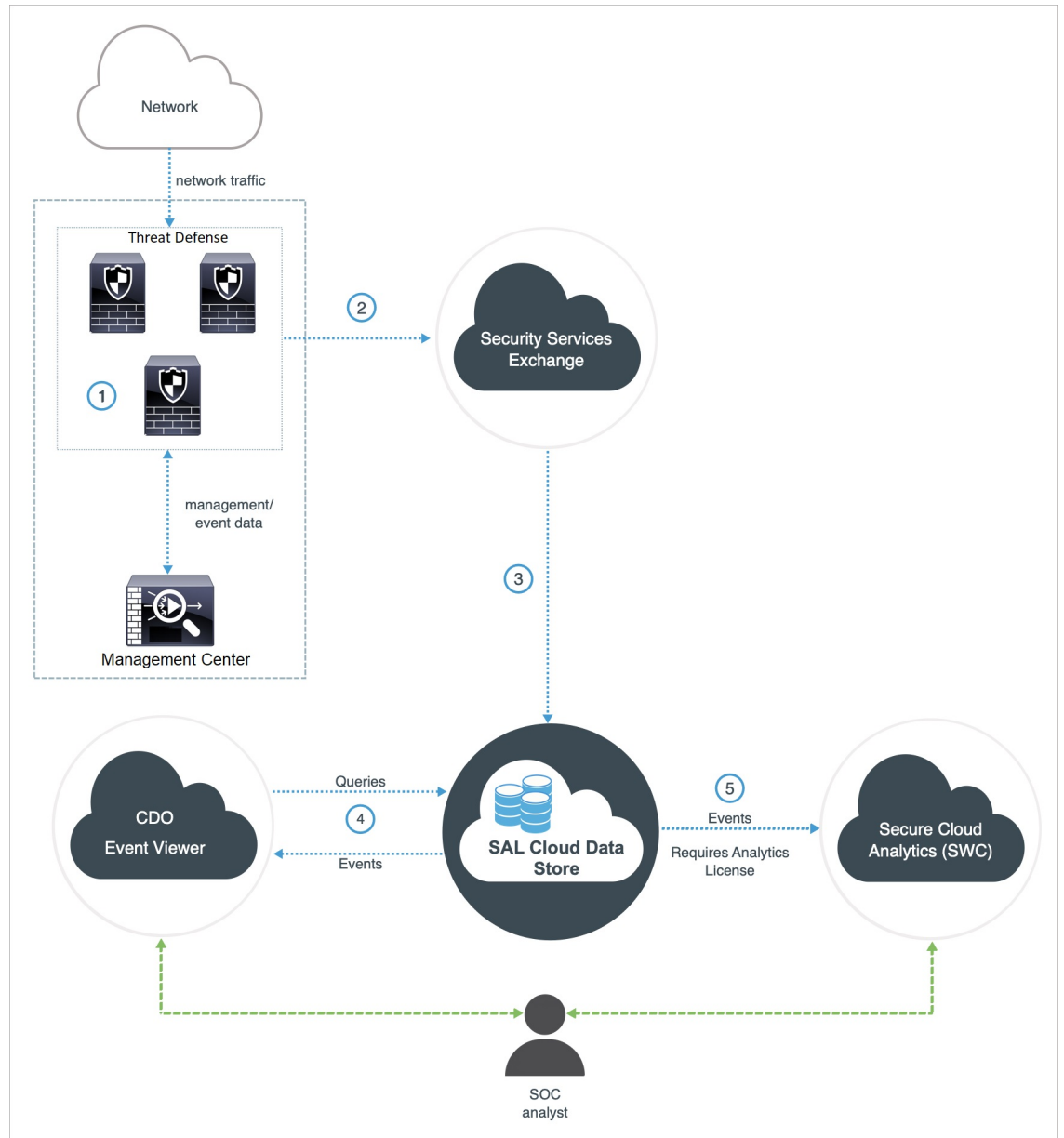
- If you are done making changes, deploy your changes to managed devices.

## How to Set Up Event Data Storage in SAL (SaaS) Using a Direct Connection

This section describes how to set up event data storage in SAL (SaaS) using a direct connection.

### How Does It Work

The following diagram shows how the direct integration works.



1	The management center-managed devices generate events.
2	The threat defense devices send supported events to Security Services Exchange (SSE), a secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.
3	The SSE forwards the events to the Cisco Security Analytics and Logging (SAL) Cloud Data Store.
4	The CDO Event Viewer queries SAL Cloud Data Store for events and provides the SOC analyst with additional context.

5	(Only with Analytics License) Cisco Secure Cloud Analytics (formerly SWC) receives the events from the SAL Cloud Data Store and provides the SOC analyst access to the analytics features of the product.
---	---

## Key Components of This Integration

Component	Description
Threat Defense	A next generation firewall with capabilities such as protection from malware and application-layer attacks, integrated intrusion prevention, and cloud-delivered threat intelligence.
Management Center	An administrative nerve center for select Cisco security products running on multiple platforms. It provides unified management of threat defense software for port and protocol control, application control, IPS, URL filtering, and malware protection functions.
Security Services Exchange	A secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.
CDO	A cloud-based multidevice manager you can use to manage security policy changes across various security products. This platform enables the efficient management of policies in branch offices and other highly distributed environments to achieve a consistent security implementation.
Cisco Secure Cloud Analytics (formerly Secure Network Analytics Cloud)	A cloud platform that applies dynamic entity modeling to threat defense events, generating detections based on this information. This provides a deeper analysis of telemetry gathered from your network, allowing you to identify trends and examine anomalous behavior in your network traffic.
SecureX	A simplified platform experience, connecting Cisco's integrated security portfolio with your existing infrastructure. It helps you unify visibility, enable automation, and strengthen security across your network, endpoints, cloud, and applications.
Cisco SecureX threat response	A cloud platform that helps you detect, investigate, analyze, and respond to threats using data aggregated from multiple products and sources.

## Prerequisites for Direct Integration

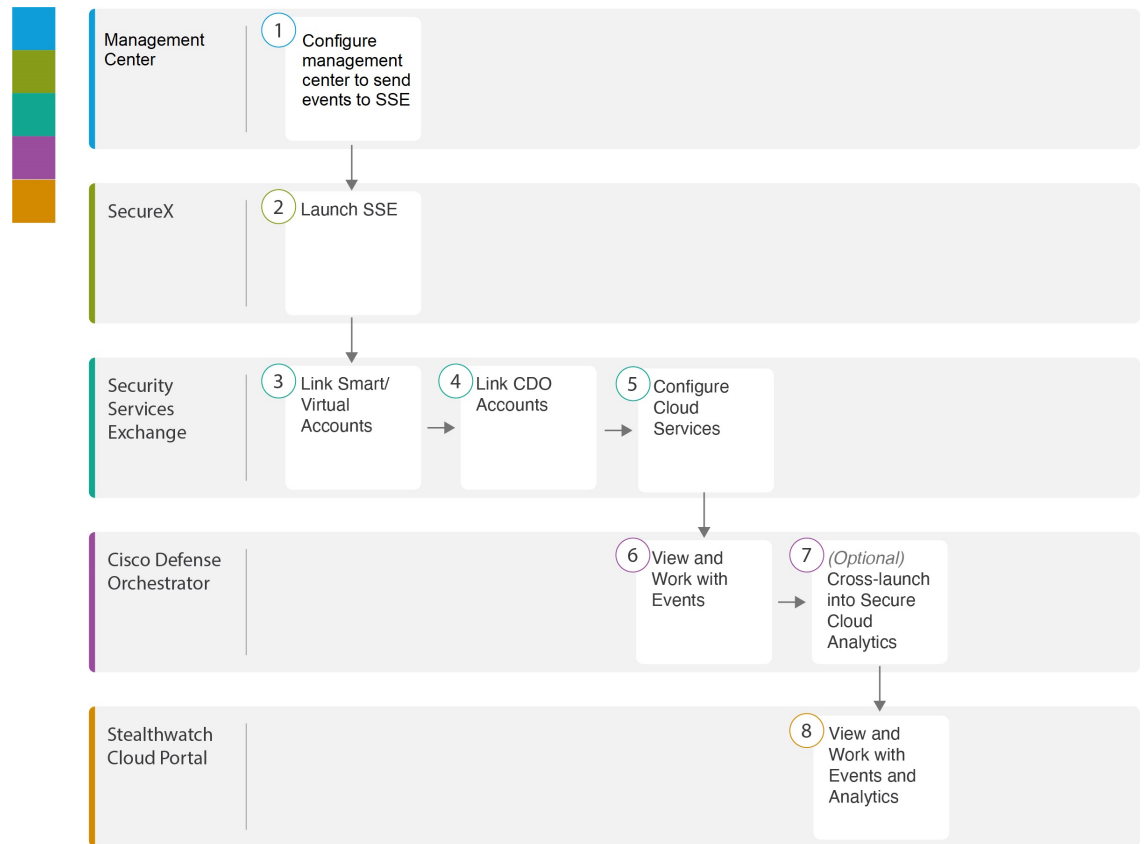
Prerequisite Type	Requirement
General requirements for sending events to SAL (SaaS)	In addition to the requirements in this table, you must satisfy the items in <a href="#">Requirements and Prerequisites for SAL (SaaS) Integration</a> , on page 2 and subtopics.

Prerequisite Type	Requirement
Licensing	<p>Register your management center with the Cisco Smart Software Manager.</p> <p>In the management center web interface, click <b>System</b> (⚙️) &gt; <b>Smart Licenses</b>, and verify that:</p> <ul style="list-style-type: none"> <li>• The <b>Usage Authorization</b> status is <b>Authorized</b>.</li> <li>• The <b>Product Registration</b> status is <b>Registered</b>.</li> </ul> <p>Keep in mind that:</p> <ul style="list-style-type: none"> <li>• This integration is not supported under a evaluation license.</li> <li>• 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.</li> </ul>
Account	<ul style="list-style-type: none"> <li>• You must have administrator privileges for the Cisco Smart Account from which your products are licensed.</li> </ul> <p>To determine your Smart Account user role:</p> <ol style="list-style-type: none"> <li>1. Go to <a href="https://software.cisco.com">https://software.cisco.com</a>.</li> <li>2. Click <b>Manage Smart Account</b>.</li> <li>3. Select a Smart Account in the top-right area (above the Help link) of the page.</li> <li>4. Click the <b>Users</b> tab.</li> <li>5. Search for your User ID.</li> </ol> <ul style="list-style-type: none"> <li>• Your management center account must have one of the following user roles: <ul style="list-style-type: none"> <li>• Admin</li> <li>• Access Admin</li> <li>• Network Admin</li> <li>• Security Approver</li> </ul> </li> </ul> <p>To determine your user role, click <b>System</b> (⚙️) &gt; <b>Users</b> in the management center web interface.</p> <ul style="list-style-type: none"> <li>• Your CDO account must have one of the following user roles: <ul style="list-style-type: none"> <li>• Admin</li> <li>• Super Admin</li> </ul> </li> <li>• Your SecureX account must have one of the following user roles: <ul style="list-style-type: none"> <li>• Admin</li> </ul> </li> </ul>

Prerequisite Type	Requirement
Connectivity	<p>The management center and managed devices must be able to connect outbound on port 443 to the Cisco cloud at the following addresses:</p> <ul style="list-style-type: none"> <li>• North America cloud: <ul style="list-style-type: none"> <li>• <a href="https://api-sse.cisco.com">api-sse.cisco.com</a></li> <li>• <a href="https://eventing-ingest.sse.itd.cisco.com">https://eventing-ingest.sse.itd.cisco.com</a></li> <li>• <a href="https://mx01.sse.itd.cisco.com">https://mx01.sse.itd.cisco.com</a></li> </ul> </li> <li>• EU cloud: <ul style="list-style-type: none"> <li>• <a href="https://api.eu.sse.itd.cisco.com">api.eu.sse.itd.cisco.com</a></li> <li>• <a href="https://eventing-ingest.eu.sse.itd.cisco.com">https://eventing-ingest.eu.sse.itd.cisco.com</a></li> <li>• <a href="https://mx01.eu.sse.itd.cisco.com">https://mx01.eu.sse.itd.cisco.com</a></li> </ul> </li> <li>• Asia (APJC) cloud: <ul style="list-style-type: none"> <li>• <a href="https://api.apj.sse.itd.cisco.com">api.apj.sse.itd.cisco.com</a></li> <li>• <a href="https://mx01.apj.sse.itd.cisco.com">mx01.apj.sse.itd.cisco.com</a></li> <li>• <a href="https://eventing-ingest.apj.sse.itd.cisco.com">eventing-ingest.apj.sse.itd.cisco.com</a></li> </ul> </li> </ul>

## Set Up Event Data Storage in SAL (SaaS) Using a Direct Connection

Perform the following tasks to set up event data storage in SAL (SaaS) using a direct integration.



		Workspace
1	Management Center	<ul style="list-style-type: none"> <li>• Configure the Management Center (version 7.1 and earlier) to Send Events to Security Services Exchange, on page 16.</li> <li>• Configure the Management Center (version 7.2 and later) to Send Events to Security Services Exchange, on page 17.</li> </ul>
2	SecureX	Launch Security Services Exchange , on page 19
3	Security Services Exchange	Link Smart or Virtual Accounts on Security Services Exchange, on page 19
4	Security Services Exchange	Link CDO Accounts on Security Services Exchange, on page 21
5	Security Services Exchange	Configure Cloud Services on Security Services Exchange, on page 23
6	CDO	View and Work with Events, on page 23
7	CDO	View and Work with Events in Cisco Secure Cloud Analytics, on page 24: Cross-launch into Secure Cloud Analytics

		<b>Workspace</b>
8	Cisco Secure Cloud Analytics	<a href="#">View and Work with Events in Cisco Secure Cloud Analytics, on page 24</a>

## Configure the Management Center (version 7.1 and earlier) to Send Events to Security Services Exchange

If your management center version is 7.1 or earlier (except version 7.0.2), follow this procedure to configure your management center to have the managed threat defense devices send events directly to SSE. If your management center version is 7.0.2, follow the steps in [Configure the Management Center \(version 7.2 and later\) to Send Events to Security Services Exchange](#).

### Before you begin

In the management center web interface, do the following:

- 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 the necessary policies and ensure that the generated events appear as expected in the management center web interface under the **Analysis** tab.

### Procedure

**Step 1** In the management center web interface, click **System > Integration**.

**Step 2** In the **Cisco Cloud Region** widget, from the **Region** drop-down list, choose a regional cloud, and click **Save**.

**Note** If the management center is already registered to the selected regional cloud, the **Save** button appears as inactive.

The region that you select in this step is also used for the Cisco Support Diagnostics and Cisco Support Network features, if applicable and enabled.

Consider the following points to choose the regional cloud:

- When possible, use the regional cloud nearest to your deployment.
- Data in different clouds cannot be aggregated or merged.
- 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.

**Step 3** In the **Cisco Cloud Event Configuration** widget, configure the management center to send events to SSE.

- Click the **Cisco Cloud Event Configuration** slider to enable the configuration.
- Enable or disable the types of events that you want to send to SSE.

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



Integration	Supported Event Options	Notes
Security Analytics and Logging	All	High priority connection events include: <ul style="list-style-type: none"> <li>• Security-related connection events.</li> <li>• Connection events related to file and malware events.</li> <li>• Connection events related to intrusion events.</li> </ul>
Cisco SecureX and Cisco SecureX threat response	Depending on your version: <ul style="list-style-type: none"> <li>• Some connection events</li> <li>• Intrusion</li> <li>• File and malware events</li> </ul>	If you send all connection events, Cisco SecureX and Cisco SecureX threat response support only Security events.

c. Click **Save**.

**Step 4** Click **Save**.

### What to do next

[Launch Security Services Exchange](#) , on page 19

## Configure the Management Center (version 7.2 and later) to Send Events to Security Services Exchange

If your management center version is 7.0.2 or 7.2 and later, follow this procedure to configure your management center to have the managed devices send events directly to SSE.

### Before you begin

In the management center web interface, do the following:

- 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 the necessary policies and ensure that the generated events appear as expected in the management center web interface under the **Analysis** tab.

### Procedure

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

**Step 2** Select a regional cloud from the **Current Region** drop-down.

**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.

Consider the following points to choose the regional cloud:

- When possible, use the regional cloud nearest to your deployment.
- Data in different clouds cannot be aggregated or merged.
- 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.

**Step 3** Enable the Cisco cloud event configuration and select the event types that you want to send to the cloud.

- Check the **Send events to the cloud** check box to enable the configuration.
- Select the event types which 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
Security Analytics and Logging	All	High priority connection events include: <ul style="list-style-type: none"> <li>• Security-related connection events.</li> <li>• Connection events related to file and malware events.</li> <li>• Connection events related to intrusion events.</li> </ul>
Cisco SecureX and Cisco SecureX threat response	Depending on your version: <ul style="list-style-type: none"> <li>• Some connection events</li> <li>• Intrusion</li> <li>• File and malware events</li> </ul>	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 data 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 4** Click **Save**.

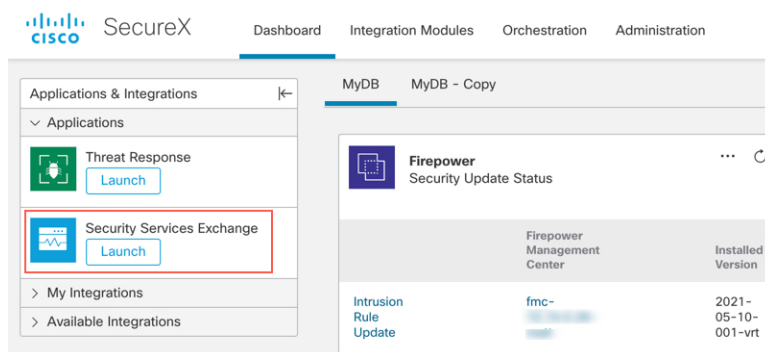
### What to do next

[Launch Security Services Exchange](#) , on page 19

## Launch Security Services Exchange

### Procedure

- Step 1** Go to <https://sign-on.security.cisco.com>.
- Step 2** Sign in using your SecureX Sign-On account.
- Step 3** If prompted, authenticate using Duo Security.
- Step 4** Choose your region to launch SecureX.
- Step 5** From the **Applications & Integrations** pane, click **Launch** under **Applications > Security Services Exchange**.



The Security Services Exchange portal opens in a new tab.

### What to do next

[Link Smart or Virtual Accounts on Security Services Exchange, on page 19](#)

## Link Smart or Virtual Accounts on Security Services Exchange

To integrate products registered under different licensing Smart Accounts (or Virtual Accounts) into a single view in the cloud, you must link those licensing accounts to the account that you use to access SSE.

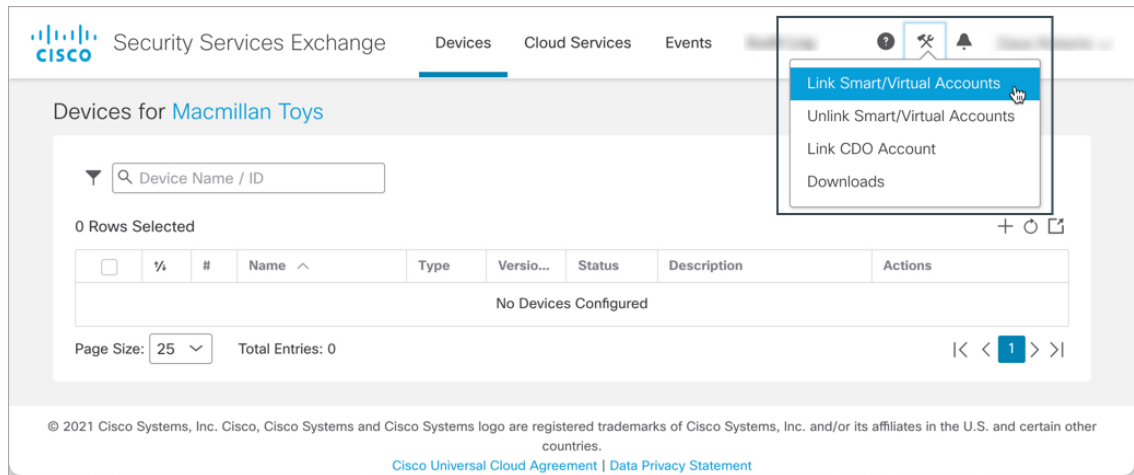
### Before you begin

- To link licensing accounts, you must have administrator-level Smart Account or Virtual Account privileges for all of the licensing accounts (from which your products are licensed) and for the account you use to access SecureX/SSE.
- If you have linked accounts already for use with Cisco SecureX threat response, you do not need to link them again for SAL (SaaS) and conversely.
- You will need your Cisco.com credentials to complete this procedure.

### Procedure

- Step 1** [Launch Security Services Exchange , on page 19.](#)

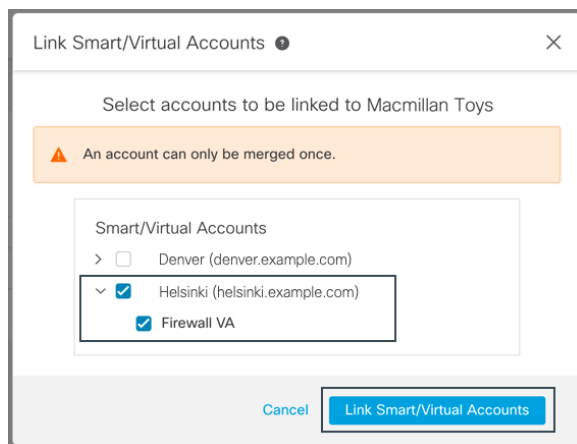
**Step 2** In the top-right corner, click the **Tools** (✂) button, and choose **Link Smart/Virtual Accounts**.



**Step 3** Click **Link more accounts**.

**Step 4** If prompted, sign in using your Cisco.com credentials.

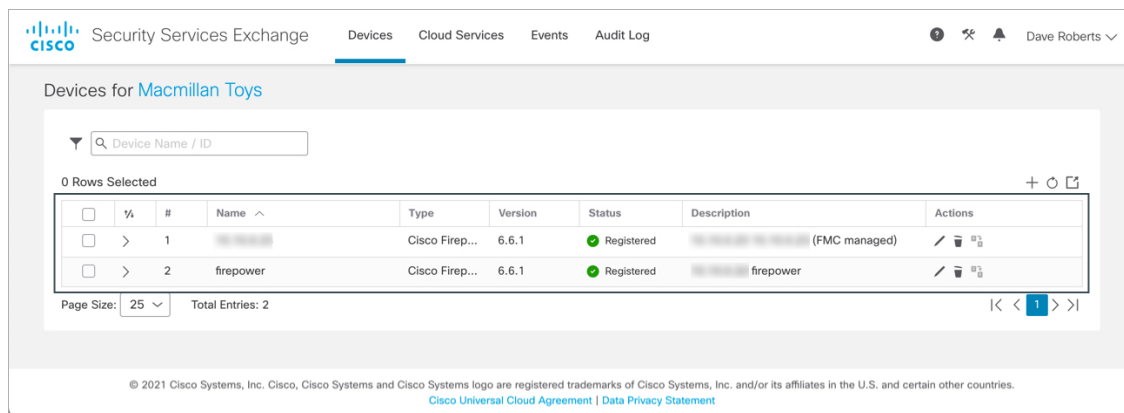
**Step 5** Select the accounts to integrate with this cloud account.



**Step 6** Click **Link Smart/Virtual Accounts**.

**Step 7** Click **OK** to continue.

**Step 8** Verify that your management center and its managed devices appear under the **Devices** tab.



### What to do next

[Link CDO Accounts on Security Services Exchange, on page 21](#)

## Link CDO Accounts on Security Services Exchange

You must merge your CDO account with the account that is associated with the device in SSE.

Keep in mind that:

- Only one CDO tenant can be merged with one SecureX/Cisco SecureX threat response account.
- If you have accounts on more than one regional cloud, you must merge accounts separately for each regional cloud.
- If you merge accounts for a SecureX cloud, you do not need to do it again for Cisco SecureX threat response on the same cloud, and conversely.

### Before you begin

- Ensure that your CDO user account has admin or super admin privileges.
- Ensure that your SecureX or Cisco SecureX threat response account that you use for accessing SSE must have admin privileges.
- In CDO, generate a new API token for your account:
  1. Sign in to the appropriate regional CDO portal using the credentials for the account to be merged. For example, the US cloud is <https://defenseorchestrator.com> and the EU cloud is <https://defenseorchestrator.eu>.
  2. Choose the tenant account to merge.
  3. From the user menu in the top-right corner of the window, select **Settings**.
  4. In the **My Tokens** section, click **Generate API Token** or **Refresh**.
  5. Copy the token.

For more information about API tokens, see the online help in CDO at [https://docs.defenseorchestrator.com/Configuration\\_Guides/Devices\\_and\\_Services/API\\_Tokens](https://docs.defenseorchestrator.com/Configuration_Guides/Devices_and_Services/API_Tokens).

## Procedure

**Step 1** Launch Security Services Exchange , on page 19.

**Step 2** In the top-right corner, click the **Tools** (🔧) button, and choose **Link CDO Account**.

The screenshot shows the Security Services Exchange interface. At the top, there are tabs for 'Devices', 'Cloud Services', 'Events', and 'Audit Log'. The 'Devices' tab is active, showing a list of devices for 'Macmillan Toys'. A search bar is present with the text 'Device Name / ID'. A blue button says 'Need Help Activating Firepower FMC?'. A dropdown menu is open in the top right corner, showing options: 'Link Smart/Virtual Accounts', 'Unlink Smart/Virtual Accounts', 'Link CDO Account' (highlighted), and 'Downloads'. Below the menu is a table with columns: Name, Type, Version, Status, Description, and Actions. The table contains four rows of device information. At the bottom, there is a 'Page Size' dropdown set to 25 and 'Total Entries: 6'.

	Name	Type	Version	Status	Description	Actions
> 1	192.168.0.25	Cisco Fire...	6.6.1	Registered	192.168.0.25 192.168.0.25 (FMC managed)	✎ 🗑️ ⚙️
> 2	192.168.0.11	Cisco Fire...	7.0.0	Registered	192.168.0.11 192.168.0.11 (FMC man...	✎ 🗑️ ⚙️
> 3	192.168.0.12	Cisco Fire...	7.0.0	Registered	192.168.0.12 192.168.0.12 (FMC man...	✎ 🗑️ ⚙️
> 4	192.168.0.13	Cisco Fire...	7.0.0	Registered	192.168.0.13 (FMC managed)	✎ 🗑️ ⚙️

**Step 3** Paste the token that you copied from CDO.

The screenshot shows a dialog box titled 'Link CDO Account'. It contains the following text: 'For FTD (Firepower Threat Defense) devices that are managed by FDM that need to be registered both to CDO (Cisco Defense Orchestrator) and SecureX or CTR (Cisco Threat Response): Retrieve your CDO access token and paste it in the textbox below.' Below the text is a text input field containing a long alphanumeric token. At the bottom of the dialog, there are two buttons: 'Close' and 'Link CDO Account'.

**Step 4** Verify that you are linking the accounts that you intended to link, and click **Link CDO Account**.

## What to do next

[Configure Cloud Services on Security Services Exchange, on page 23](#)

## Configure Cloud Services on Security Services Exchange

### Procedure

---

- Step 1** Launch [Security Services Exchange](#) , on page 19.
- Step 2** Click the **Cloud Services** tab.
- Step 3** Verify that the Eventing services option is enabled.
- Step 4** Verify that your events appear as expected under the **Events** tab.
- 

### What to do next

- [View and Work with Events](#), on page 23
- [View and Work with Events in Cisco Secure Cloud Analytics](#), on page 24

## View and Work with Events

To view and search your events in the cloud:

### Procedure

---

- Step 1** Use your browser to go to the regional CDO cloud to which you sent your events:
- North America:  
<http://www.defenseorchestrator.com>
  - Europe:  
<http://www.defenseorchestrator.eu>
- Step 2** Sign in to CDO.
- Step 3** From the navigation bar, select **Monitoring > Event Logging**.
- Step 4** Use the **Historical** tab to view historical events data. By default, the viewer displays this tab.
- Step 5** To view the live events, click the **Live** tab.

For more information about what you can do on this page, see the CDO online help for instructions on [viewing events](#).

---

### What to do next

If you have a **Logging Analytics and Detection** or **Total Network Analytics and Detection** license, see instructions in the [CDO online help](#) to cross-launch into the Stealthwatch Cloud portal.

# View and Work with Events in Cisco Secure Cloud Analytics

To view and search your events in Cisco Secure Cloud Analytics:

## Procedure

---

**Step 1** Sign in to the appropriate regional CDO site using the credentials for the account to be merged. For example, the US cloud is <https://defenseorchestrator.com> and the EU cloud is <https://defenseorchestrator.eu>.

**Step 2** From the navigation bar, click **Monitoring > Security Analytics**.

The Stealthwatch Cloud portal opens in a new browser tab.

**Step 3** **(One-time Activity)** To ensure seamless flow of events, before using the Event Viewer, do the following in the Stealthwatch Cloud portal:

- a. Verify whether Secure Cloud Analytics is integrated with the correct CDO tenant. To view the CDO tenant, click **Settings > Sensors**.
- b. Add the subnets that you want monitor to Secure Cloud Analytics. To add subnets, click **Settings > Subnets**.

For more information, see the Secure Cloud Analytics online help.

**Step 4** To view events, click **Investigate > Event Viewer**.

For more information, see the Secure Cloud Analytics online help.

---

## FAQs

### Where can I find more information about SAL?

See also the SAL [Getting Started and Frequently Asked Questions](#).

### Do I need to onboard my devices to CDO?

No. Do NOT onboard your devices to CDO.

### If I use SecureX or Cisco Threat Response, do I need to merge my CDO account?

Only if you are sending events directly to the cloud using the process described in [How to Set Up Event Data Storage in SAL \(SaaS\) Using a Direct Connection](#), on page 10.