



Cisco Secure Cloud Analytics

SecureX Integration Guide



Table of Contents

Cisco Secure Cloud Analytics Integration with Cisco SecureX	3
Secure Cloud Analytics Tiles in SecureX	4
Configuring SecureX Integration with Secure Cloud Analytics	6
Authorize Access to SecureX from Secure Cloud Analytics	6
Enable Integration in Secure Cloud Analytics or SecureX	6
Using Secure Cloud Analytics	6
Using SecureX	8
Publish Alerts to SecureX	10
Enable Publishing Alerts	10
Additional Resources	11
Contacting Support	12
Change History	13

Cisco Secure Cloud Analytics Integration with Cisco SecureX

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and the customer's infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications. By connecting technology in an integrated platform, SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration.

You can integrate Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) with SecureX to view additional context about your Secure Cloud Analytics deployment from the SecureX dashboard, and to use the SecureX ribbon from within your Secure Cloud Analytics web portal.

If you are logged into the SecureX ribbon, you can also create Cisco SecureX threat response (formerly Cisco Threat Response) incidents based on alerts, and pivot from IP addresses to other SecureX product integrations. See the [Secure Cloud Analytics Initial Deployment Guide](#) for more information on using these features.

See <https://info.observable.net/SecureX-Trial-Request.html> for more information on a free trial.

After you create a SecureX account, see <https://securex.us.security.cisco.com/help/ribbon> for more information on the ribbon.

Secure Cloud Analytics Tiles in SecureX

Secure Cloud Analytics is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic, it creates observations about the traffic, which are facts about behavior on the network, and automatically identifies roles for network entities based on their traffic patterns. Observations on their own do not carry meaning beyond the fact of what they represent. Based on the combination of observations, roles, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system.

Secure Cloud Analytics also identifies observations of interesting behavior (highlighted observations) which you can review from the web portal UI. Though these observations do not signify malicious behavior on their own, they may represent otherwise notable traffic on your network.

The following describes the Secure Cloud Analytics tiles that you can display on the SecureX dashboard, which represent Secure Cloud Analytics findings.

Alert Overview Chart

The **Alert Overview Chart** tile displays a multilevel pie chart that shows, based on the selected time frame, in the outer ring:

- new Secure Cloud Analytics alerts created within the time frame
- open Secure Cloud Analytics alerts created before the time frame, and not yet closed within the time frame
- closed Secure Cloud Analytics alerts closed during the time frame

and in the inner ring:

- assigned Secure Cloud Analytics alerts
- unassigned Secure Cloud Analytics alerts

Alert Quick View

The **Alert Quick View** tile displays the current number of open Secure Cloud Analytics alerts and unassigned Secure Cloud Analytics alerts.

Device Count Chart

The **Device Count Chart** tile displays the number of unique entities that Secure Cloud Analytics detected transmitting traffic on your network during a given time frame, displayed as a vertical bar chart.

Observation Count

The **Observation Count** tile displays the total number of observations that Secure Cloud Analytics generated in a given time frame, and the total number of highlighted observations in that time frame. The [Observations](#) and [Highlighted Observations](#) links take you to the portal UI to view more information about these observations.

Cisco Secure Cloud Analytics Sensor Status

The **Cisco Secure Cloud Analytics Sensor Status** tile displays a list of your configured Cisco Secure Cloud Analytics sensors (formerly Stealthwatch Cloud Sensor), and if they are active or inactive.

Traffic Over Time Chart

The **Traffic Over Time Chart** tile displays the amount of inbound traffic, inbound encrypted traffic, outbound traffic, and outbound encrypted traffic monitored by Secure Cloud Analytics for the selected time frame as a stacked bar chart.

Configuring SecureX Integration with Secure Cloud Analytics

To configure SecureX integration, complete the following:

- authorize access to SecureX from Secure Cloud Analytics
- enable integration in Secure Cloud Analytics or SecureX

You must have a SecureX account. See

<https://www.cisco.com/c/en/us/td/docs/security/secure-sign-on/sso-quick-start-guide.html> for more information.

Authorize Access to SecureX from Secure Cloud Analytics

Authorizing SecureX access enables the ribbon in Secure Cloud Analytics.

Procedure

1. Log in to your Secure Cloud Analytics web portal.
2. Click the + in the ribbon at the bottom of the page to expand it.
3. Click **Get SecureX**, then follow the instructions to authorize access.

Enable Integration in Secure Cloud Analytics or SecureX

You can enable the SecureX integration from either the [Secure Cloud Analytics web portal](#) or from [SecureX](#).

Prerequisites

- You are a site manager in Secure Cloud Analytics.
- You are an org admin in SecureX.

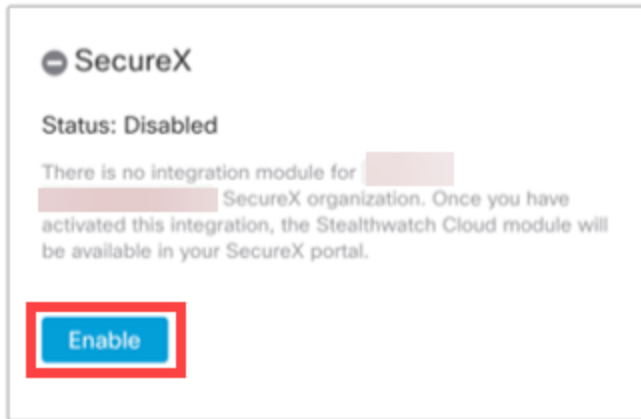
If you are not both of these roles, you will only have read access.

Using Secure Cloud Analytics

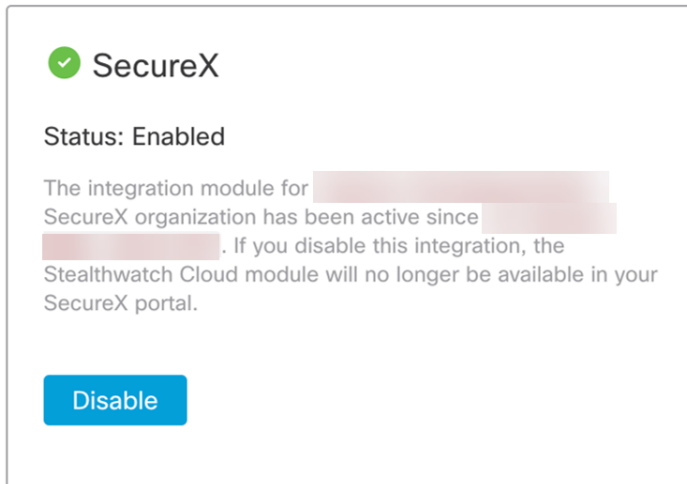
Procedure

1. Log in to your Secure Cloud Analytics web portal as a site manager.
2. Select **Settings > Integrations > SecureX**.

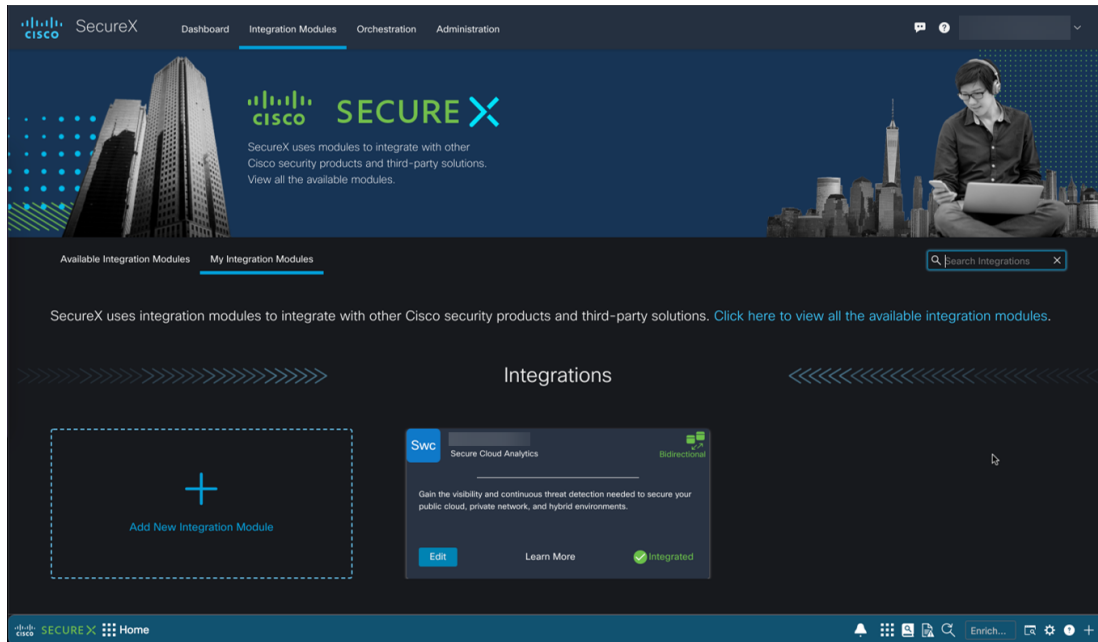
3. Click **Enable**.



4. The SecureX module status will update to Enabled.



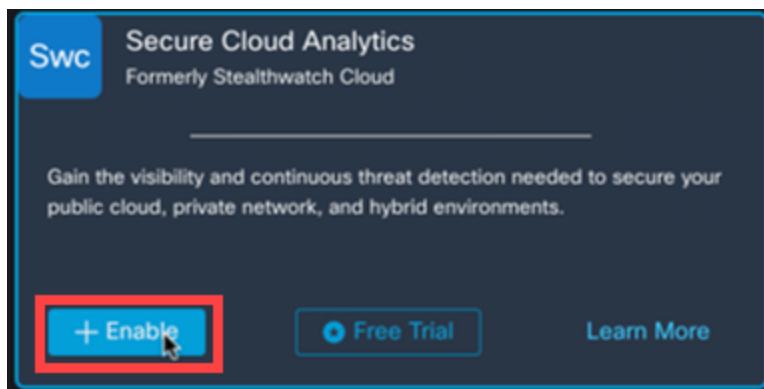
5. Go to SecureX. Select **Integration Modules > My Integration Modules** to see the Secure Cloud Analytics module.



Using SecureX

Procedure

1. Log in to SecureX.
2. Go to **Integration Modules**.
3. Under the **Available Integration Modules** tab, find the Secure Cloud Analytics module, and click **Enable**.



You will be automatically redirected to the SecureX integration page in Secure Cloud Analytics .

i If you have multiple Secure Cloud Analytics portals, you will need to select which portal you have connected to the SecureX security ribbon.

- The SecureX module status will be Enabled.

✓

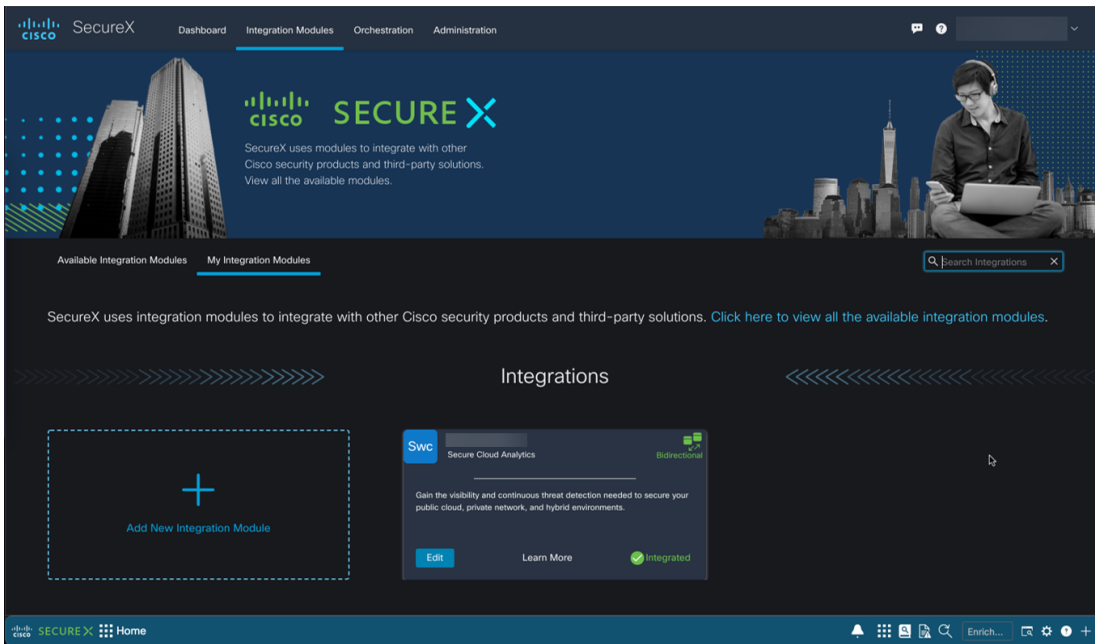
SecureX

Status: Enabled

The integration module for [REDACTED] SecureX organization has been active since [REDACTED]. If you disable this integration, the Stealthwatch Cloud module will no longer be available in your SecureX portal.

Disable

- You will be automatically redirected to **SecureX > Integration Modules > My Integration Modules**.



Publish Alerts to SecureX


From the Secure Cloud Analytics web portal, you can send alert content with the **Publish to SecureX** feature. This provides a full view of the Secure Cloud Analytics alert data in SecureX, including:

- alert type
- Secure Cloud Analytics alert ID
- reference to the Secure Cloud Analytics alert
- if integrating multiple Secure Cloud Analytics portals with SecureX, the Secure Cloud Analytics tenant in which the alert occurred
- detailed description
- next steps
- alert update timestamp
- IP addresses and hostnames known at the time of the alert
- MITRE ATT&CK tactics and techniques, if applicable
- alert assignees
- alert priority
- user tags associated with the alert

Enable Publishing Alerts



- The Talos Intelligence Watchlist Hits alert is automatically enabled to publish to SecureX.
- If an alert is disabled, you cannot publish that alert to SecureX.

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Alerts**.
3. Locate the alert you want to send to SecureX, and click the  (**Toggle**) icon in the **Publish to SecureX** column.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> to sign up for a 60-day Free Trial
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Change History

Revision	Revision Date	Description
1.0	June 24, 2020	Initial version.
1.1	December 10, 2020	Updated with additional SecureX integration information.
2.0	November 3, 2021	Updated product branding.
3.0	February 15, 2022	Updated configuration steps.
4.0	July 20, 2022	Added Publish Alerts to SecureX and Contacting Support sections.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

