



Cisco Secure Cloud Analytics

Cisco XDR Integration Guide



Table of Contents

Cisco Secure Cloud Analytics Integration with Cisco XDR	3
Secure Cloud Analytics Tiles in Cisco XDR	4
Configuring Cisco XDR Integration with Secure Cloud Analytics	6
Authorize Access for Cisco XDR from Secure Cloud Analytics	6
Enable Integration between Secure Cloud Analytics and Cisco XDR	6
Using Secure Cloud Analytics	6
Using Cisco XDR	8
Publish Alerts to Cisco XDR	10
Enable Publishing Alert Types	10
Manually Promoting Alert Instances as Incidents	10
Additional Resources	12
Contacting Support	13
Change History	14

Cisco Secure Cloud Analytics Integration with Cisco XDR

The Cisco XDR 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, Cisco XDR delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration.

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

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

Refer to the [Secure Cloud Analytics](#) web page for more information on setting up a **Secure Cloud Analytics** free trial.

After you create a Cisco XDR account, see <https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm> for more information on the ribbon.

Secure Cloud Analytics Tiles in Cisco XDR

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 Cisco XDR 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 and if they are active or inactive.

Traffic Over Time Chart

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

Configuring Cisco XDR Integration with Secure Cloud Analytics

To configure Cisco XDR integration, complete the following:

- enable Cisco XDR user integration in Secure Cloud Analytics, allowing the Cisco XDR ribbon to be displayed in Secure Cloud Analytics.
- enable the portal integration from Cisco XDR to Secure Cloud Analytics.

You must have a Cisco XDR account. Refer to the [Cisco Security Cloud Sign On Guide](#) for more information.

Authorize Access for Cisco XDR from Secure Cloud Analytics

Authorizing Cisco XDR 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 Cisco XDR**, then follow the instructions to authorize access.

Enable Integration between Secure Cloud Analytics and Cisco XDR

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

Prerequisites

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

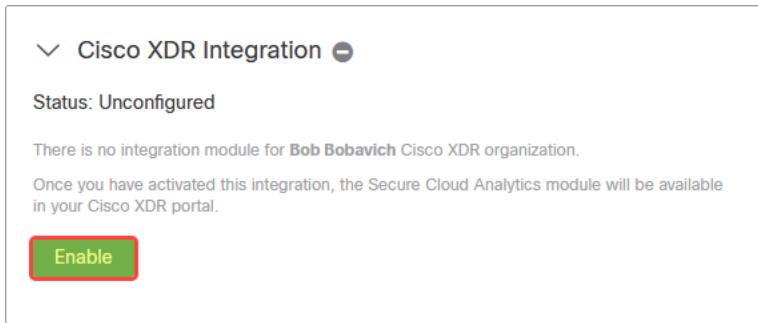
If you do not belong to both of these roles, you will not be able to enable Cisco XDR.

Using Secure Cloud Analytics

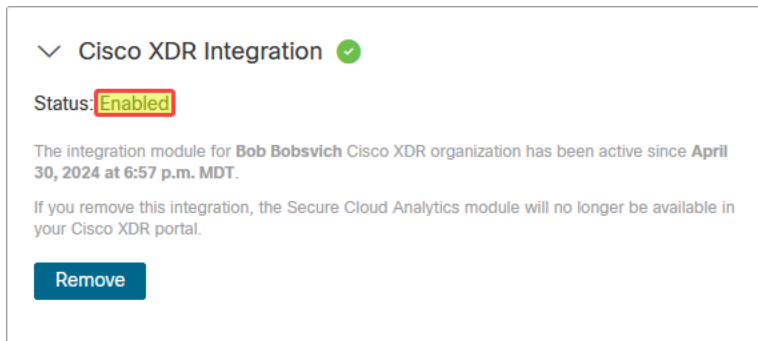
1. Log in to your **Secure Cloud Analytics** web portal as a site manager.
2. Navigate to: **Settings > Integrations > XDR**.

This will display the integrations that you are eligible to include in your **Secure Cloud Analytics** implantation.

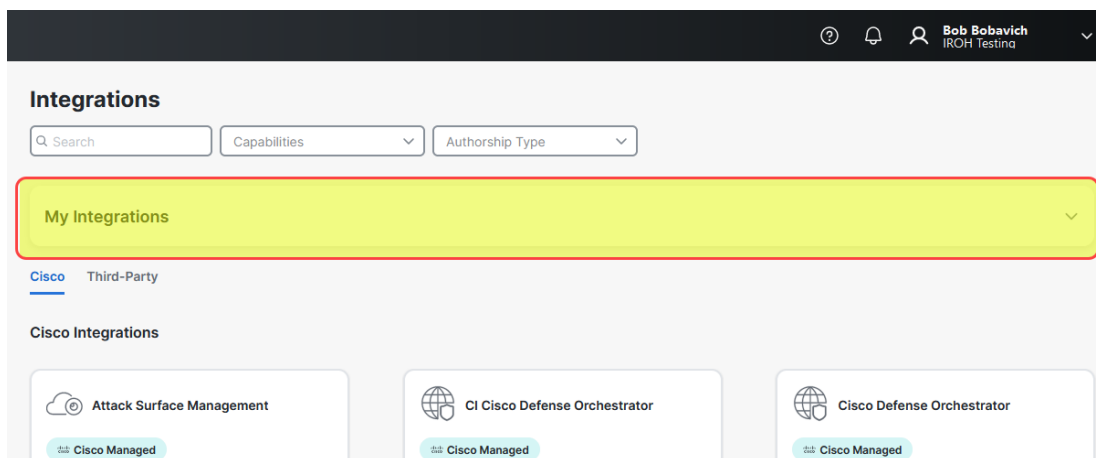
3. Click **Enable**, as shown in the figure below.



The Cisco XDR module status will update to *Enabled*, as shown in the figure below.



4. Go to Cisco XDR.
5. Navigate to **Administration > Integrations** to see the Secure Cloud Analytics module.
6. Click the **My Integrations** dropdown, shown in the figure below.

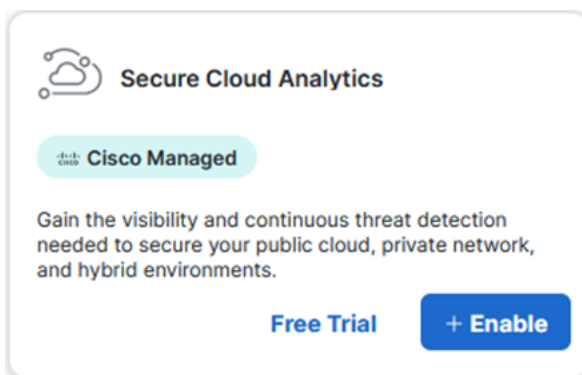


7. Scroll down in the dropdown to find your Secure Cloud Analytics module. An example is shown in the figure below.

Bob Bobavich IROH Testing			
Orbital Ramya1	Orbital	Connected	Cisco Managed
OrbitalRuslan1	Orbital	Connected	Cisco Managed
SG-Orbital	Orbital	Connected	Cisco Managed
SG-Orbital-Jan31-1458	Orbital	Connected	Cisco Managed
SGOrbitalJan31	Orbital	Connected	Cisco Managed
[object Object]	Orbital	Connected	Cisco Managed
obsrvbi-staging	Secure Cloud Analytics	Connected	Cisco Managed

Using Cisco XDR

1. Log in to Cisco XDR.
2. Go to **Administration**.
3. Go to **Integration**.
4. Under the **Cisco** tab, find the **Secure Cloud Analytics** module.
5. Click **Enable**.



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



If you have multiple Secure Cloud Analytics portals, you will need to select which portal you have connected to the Cisco XDR ribbon.

The Cisco XDR module status will be changed to *Enabled*.

▼ Cisco XDR Integration ✔

Status: Enabled

The integration module for **Bob Bobsvich** Cisco XDR organization has been active since **April 30, 2024 at 6:57 p.m. MDT**.

If you remove this integration, the Secure Cloud Analytics module will no longer be available in your Cisco XDR portal.

[Remove](#)

You will then be automatically redirected to **Cisco XDR > Integration Modules > My Integration Modules**.

 ? 🔔 👤 Bob Bobsvich IROH Testing 			
Orbital Ranya1	Orbital	✔ Connected	Cisco Managed
OrbitalRuslan1	Orbital	✔ Connected	Cisco Managed
SG-Orbital	Orbital	✔ Connected	Cisco Managed
SG-Orbital-Jan31-1458	Orbital	✔ Connected	Cisco Managed
SGOrbitalJan31	Orbital	✔ Connected	Cisco Managed
[object Object]	Orbital	✔ Connected	Cisco Managed
obsrvbl-staging	Secure Cloud Analytics	✔ Connected	Cisco Managed

Publish Alerts to Cisco XDR


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

- alert type
- Secure Cloud Analytics alert ID
- reference to the Secure Cloud Analytics alert
- if integrating multiple Secure Cloud Analytics portals with Cisco XDR, 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 Alert Types



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

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

Manually Promoting Alert Instances as Incidents

1. Log in to your Secure Cloud Analytics web portal.
2. Navigate to **Monitor > Alerts**.
3. Navigate to the desired alert.
4. Click the desired alert.

5. Scroll to the **Post to Cisco XDR** button.
6. Click **Post to Cisco XDR**.

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/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>

Change History

Revision	Revision Date	Description
1.0	June 24, 2020	Initial version.
1.1	December 10, 2020	Updated with additional Cisco XDR 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 Cisco XDR and Contacting Support sections.
5.0	June 21, 2024	Changed the branding from SecureX to Cisco XDR. Clarified some procedures. Created the topic Enable Publishing Alert Types .

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)

