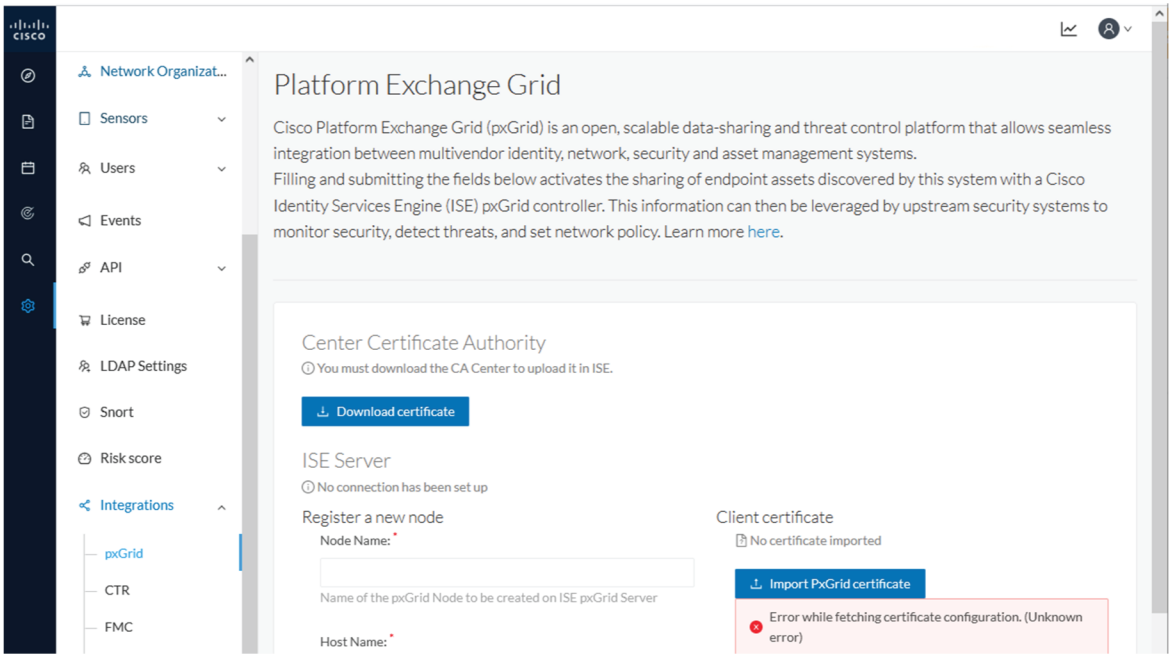
Integrations

pxGrid

From this page, you can configure ISE pxGrid Cisco Cyber Vision integration.

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems.



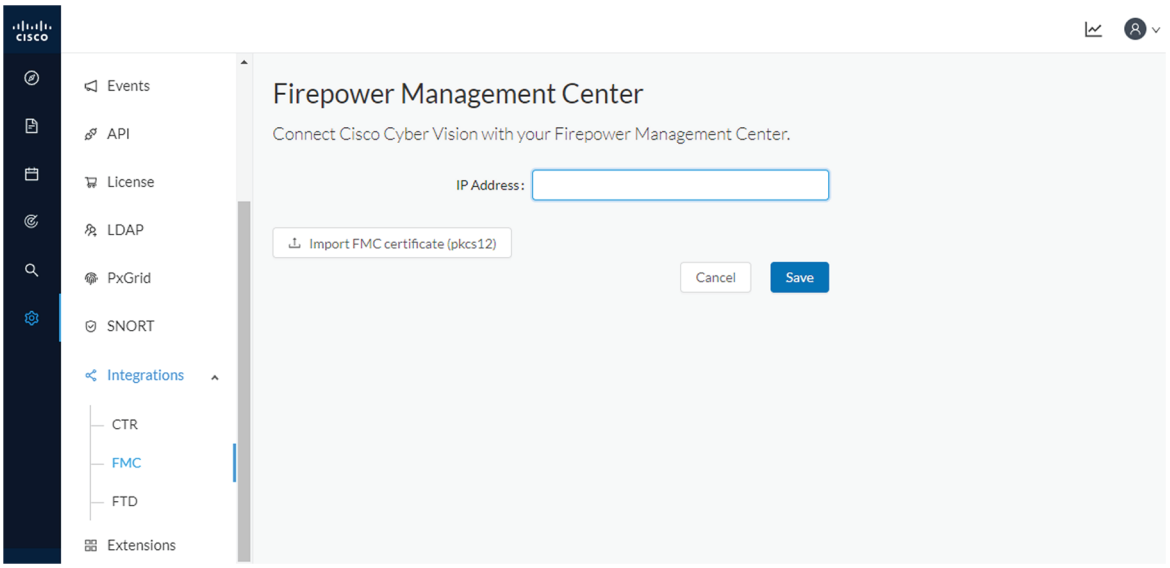
For more information about how to perform this integration, refer to the manual "Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid".

FMC

FMC administration page permits to configure a link between Cisco Cyber Vision with your Firepower Management Center. This connection will permit to send regularly (every 10 seconds) the components discovered by Cisco Cyber Vision. Every 10 seconds a list of new discovered components will be sent with the following properties in Cisco Cyber Vision:

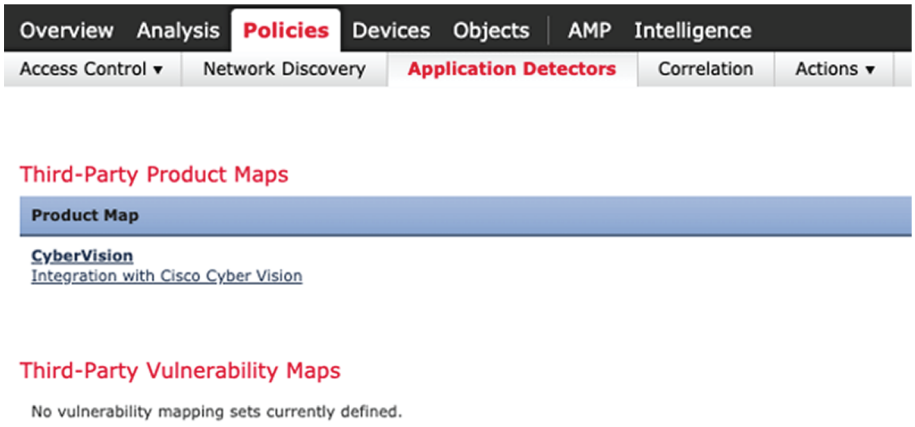
- Name
- Id
- Ip
- Mac
- And if they are available:
  - hw_version
  - model-ref
  - serial_number
  - fw_version
  - tags

The configuration of this connection consists of adding the IP address of FMC, then importing a certificate in Cisco Cyber Vision.

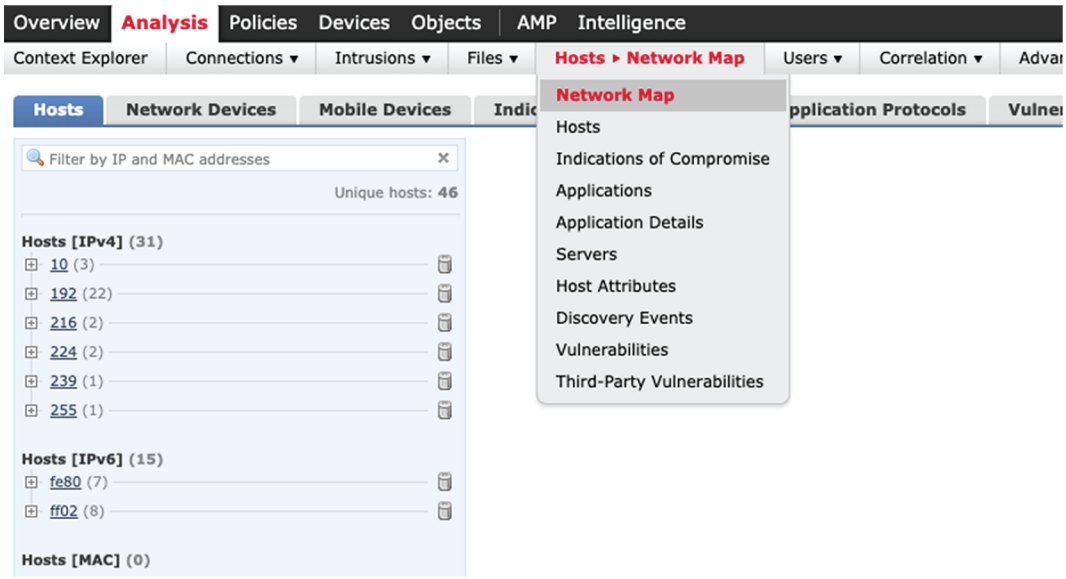


In FMC, to download the necessary certificate, please navigate to "System" then to "Integration" and open the "Host Input Client" tab. In the tab create a new Client with the button "Create Client". Add the Cisco Cyber Vision Center IP address as host name, then download the pkcs12 certificate.

Then, in FMC, menu "Policies", "Application Detectors" add a new Product Map with the button "Create Product Map Set". Please create the new product Map with the exact name and case as presented below:



The created hosts could be consulted in FMC, menu "Analysis", tab "Hosts – Network Map":



FTD

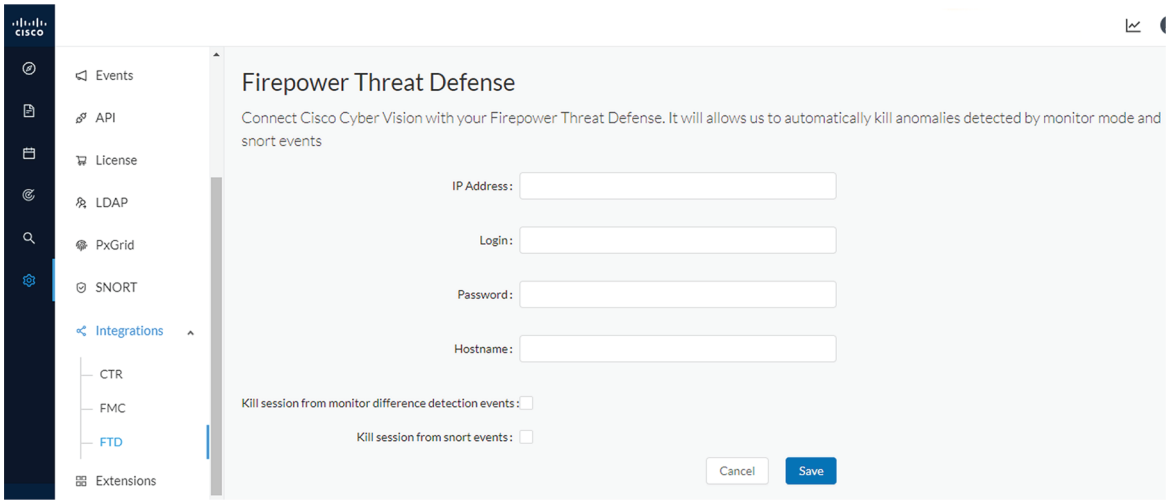
FTD administration page permits to connect Cisco Cyber Vision with your Firepower Threat Defense. It will allow to automatically kill anomalies detected by monitor mode and snort events. The corresponding session found in FTD will be killed.

Every 10 seconds Cisco Cyber Vision will browse the new monitor and SNORT events and send the corresponding action to the firewall. To enable that functionality, the user needs to add the following parameters in the FTD administration page:

- Ip address of the firewall

- Login: admin login, an ssh connection will be established between the center and the firewall
- Password: corresponding password
- Hostname: is the name of the device, by default "firepower"

Two option are available: kill session from monitor difference detection events and kill session from snort events.



SecureX

Cisco SecureX is an online platform that centralizes security events from different Cisco software equipments through an API. For example, events like Cisco Cyber Vision events or firewall events can be sent to Cisco SecureX and correlated to be presented through different dashboards.

SecureX integration enables three features in Cisco Cyber Vision:

- without SecureX SSO login, the button **Investigate in SecureX Threat Response** will appear in components' technical sheet.
- with SecureX SSO login, the button **Report to SecureX** will appear in some events of the event calendar page. This button is used to push the events to SecureX.
- with SecureX SSO login, a SecureX ribbon with several features can be activated in Cisco Cyber Vision.

This section describes how to configure SecureX in Cisco Cyber Vision and the different features authorized.

SecureX configuration

Before you begin

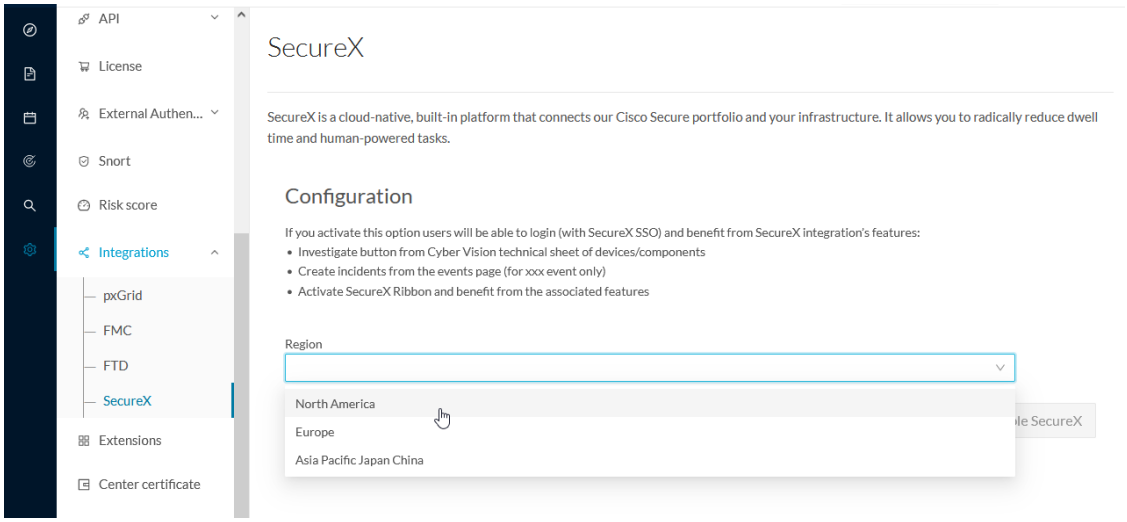
The Cisco SecureX configuration in Cisco Cyber Vision requests:

- An Admin access to Cisco Cyber Vision.

- A Cisco Cyber Vision Center with internet access.
- A SecureX account with an admin role.

Step 1 In Cisco Cyber Vision, navigate to **Admin** > **Integrations** > **SecureX**.

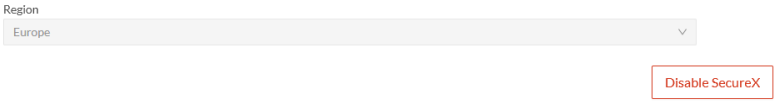
Step 2 Select a Region.



The button **Enable SecureX** appears.

Step 3 Click **Enable SecureX** to enable the link.

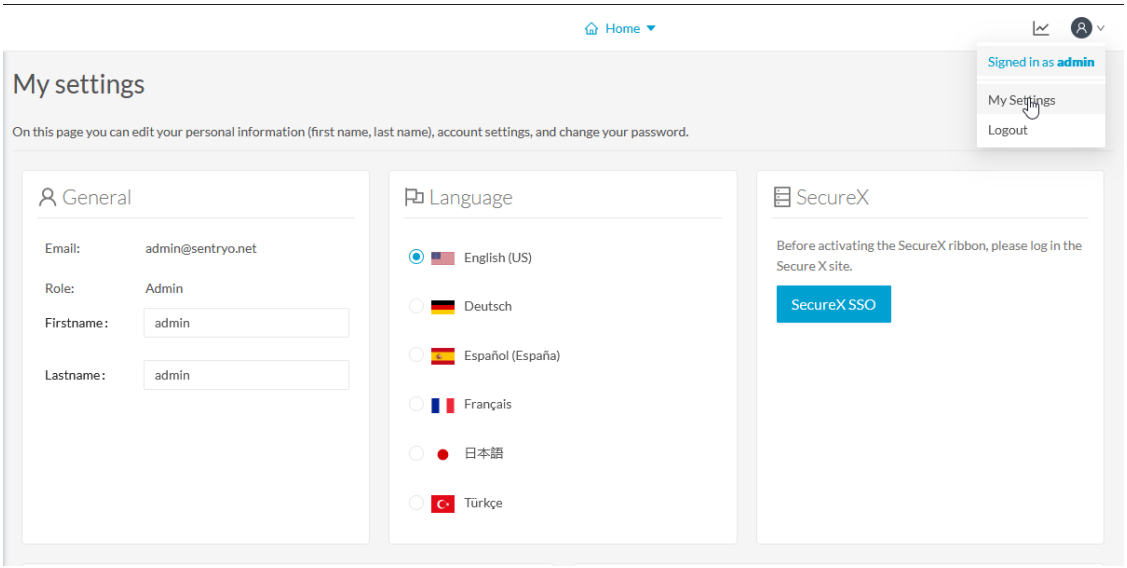
Once the link enabled, the button turns red to disable SecureX.



By completing the steps above, you are now able to use the button **Investigate in SecureX Threat Response** that will appear in the components' technical sheet. To install and use the SecureX ribbon and the Report to SecureX button, complete the steps herebelow.

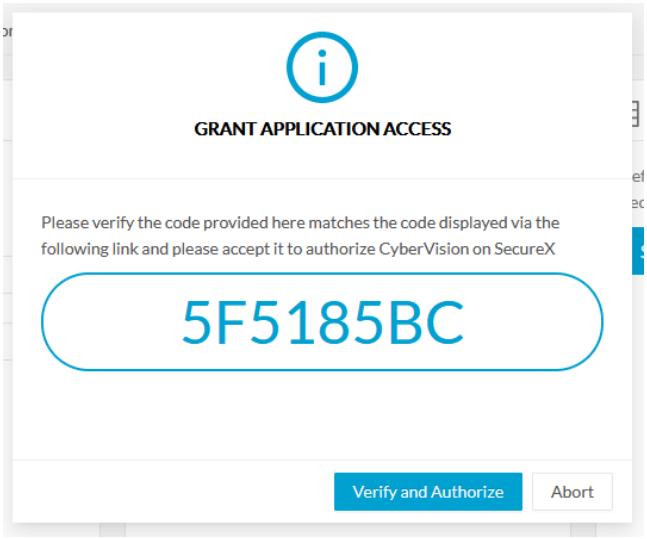
Step 4 Navigate to the user menu on the top right corner of the GUI and click **My Settings**.

A new SecureX menu appears on the right.

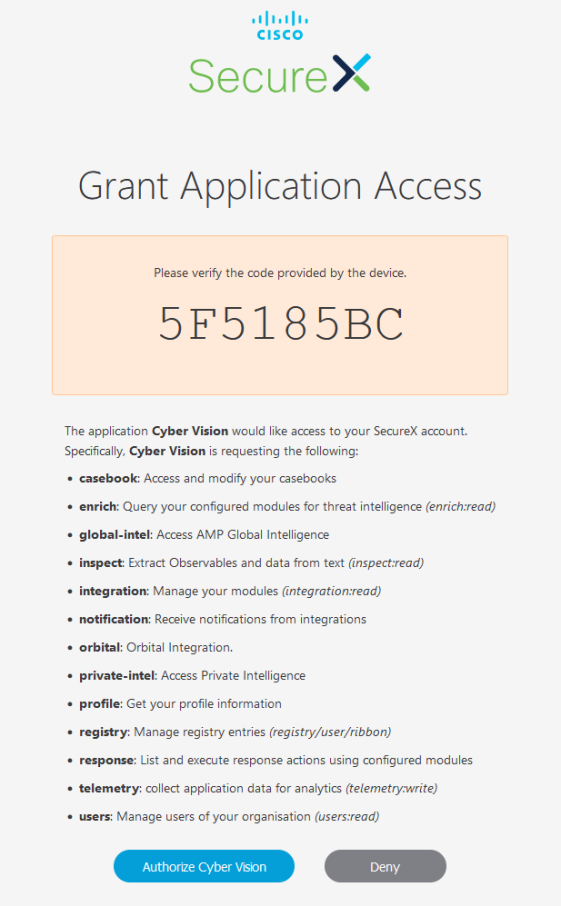


Step 5 Click the **SecureX SSO** button.

A popup appears with an authentication code.

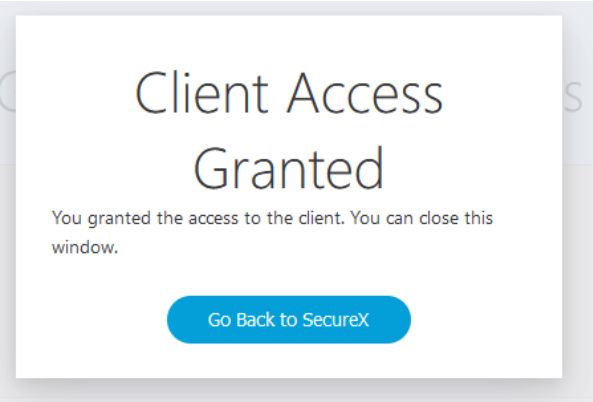


A page opens in the browser to grant Cisco Cyber Vision access to SecureX.

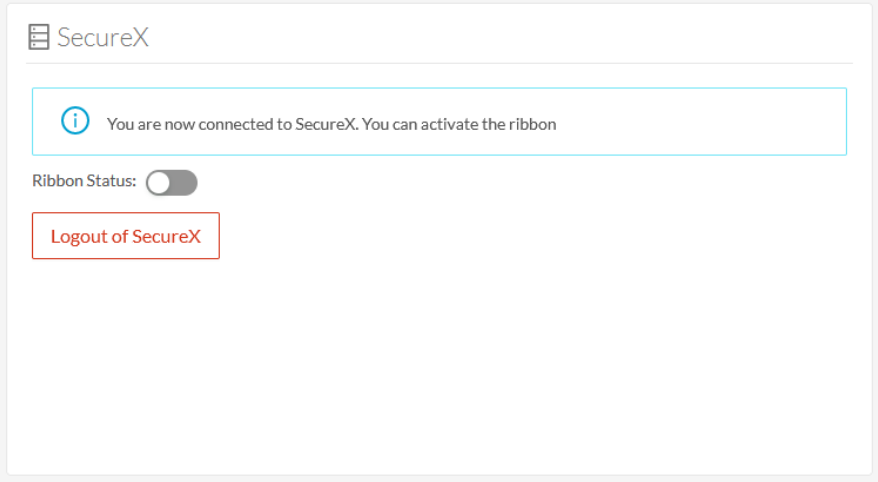


Step 6 Click **Authorize Cyber Vision**.

Step 7 A Client Access Granted popup appears.

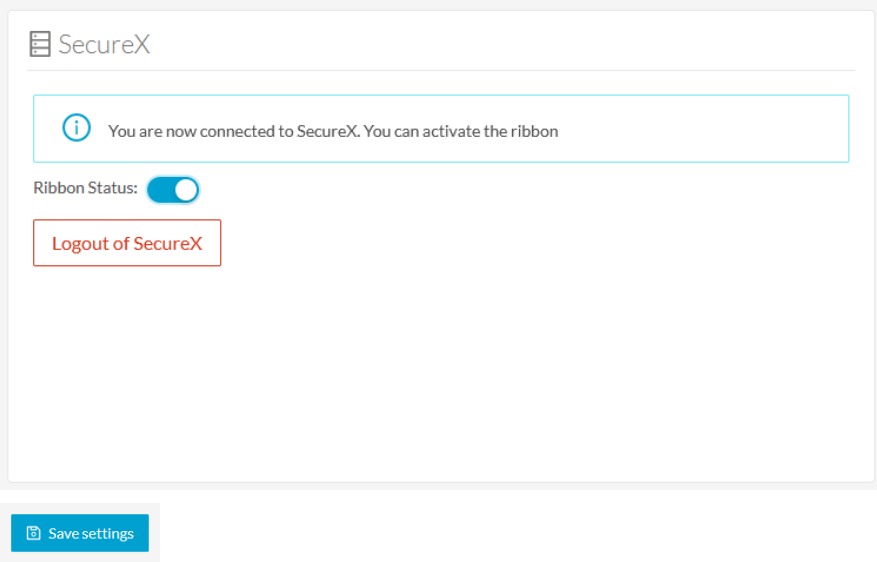


Step 8 In Cisco Cyber Vision > My Settings, the SecureX menu indicates that Cisco Cyber Vision is connected to SecureX. A toggle button to enable the SecureX ribbon and a button to logout of SecureX are displayed.

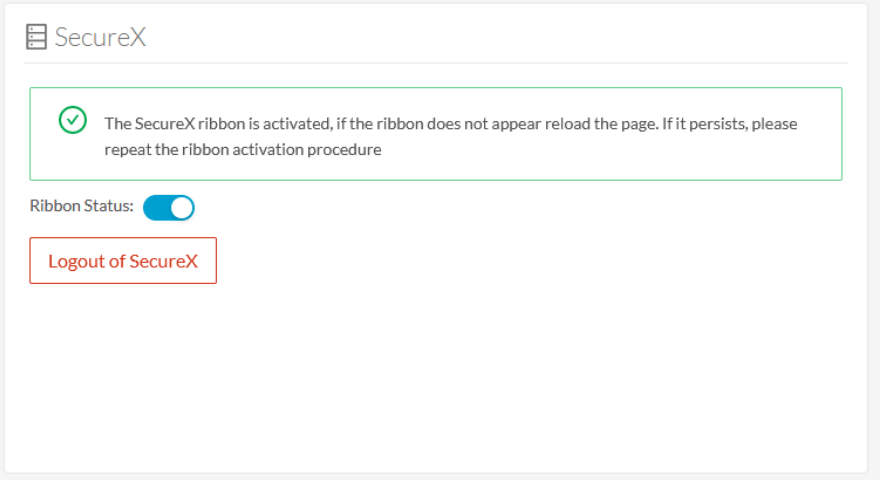


Step 9 Use the **Ribbon status** toggle button to enable the SecureX ribbon.

Step 10 Click **Save settings**.



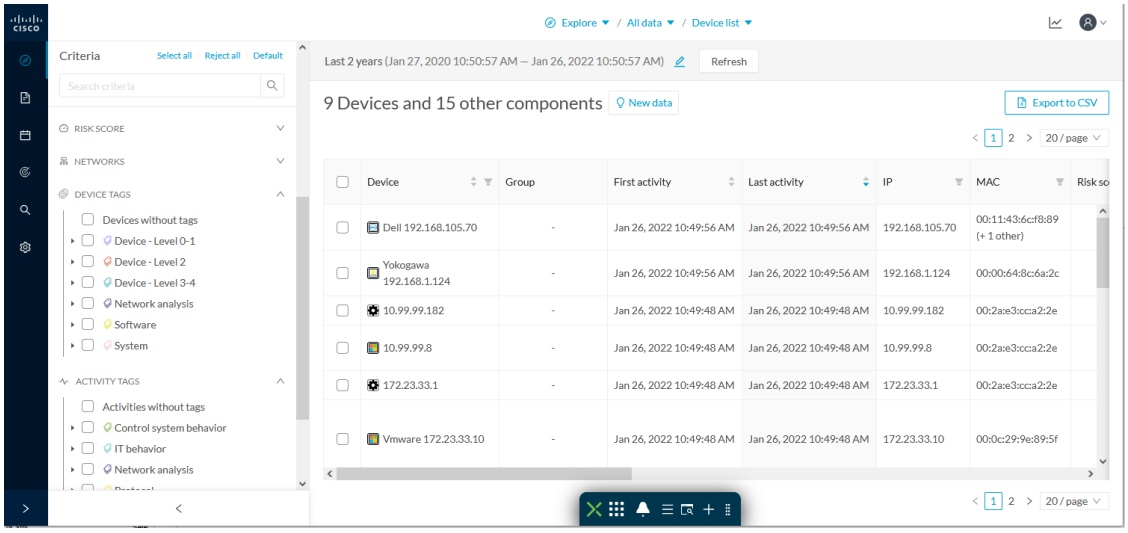
A message indicating that the SecureX ribbon is enabled appears.



SecureX ribbon

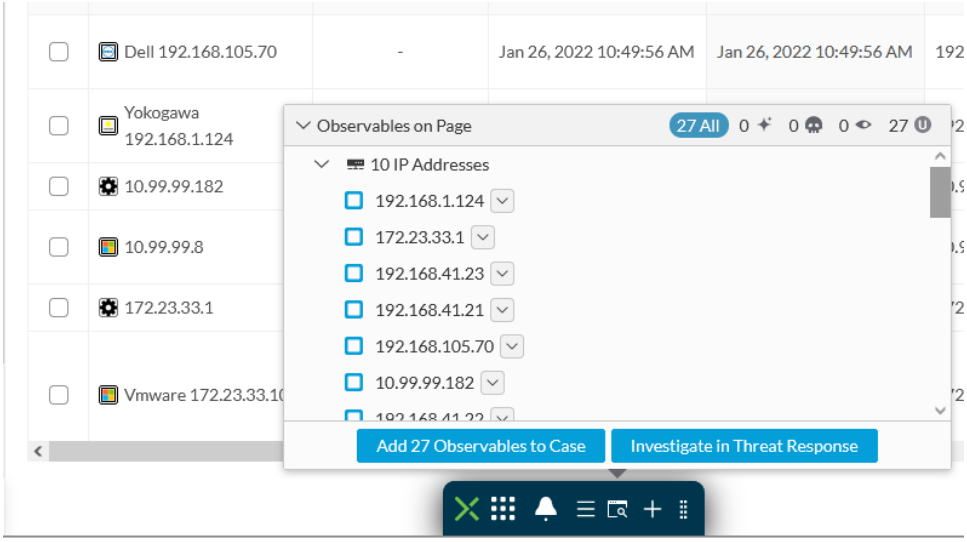
Once configured and activated, the SecureX ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.

The SecureX ribbon in the Device List view:



The Cisco SecureX Getting Started Guide explains how to use the SecureX ribbon.

For example, to find observables and investigate them in SecureX Threat Response, click the **Find Observables** icon like below:



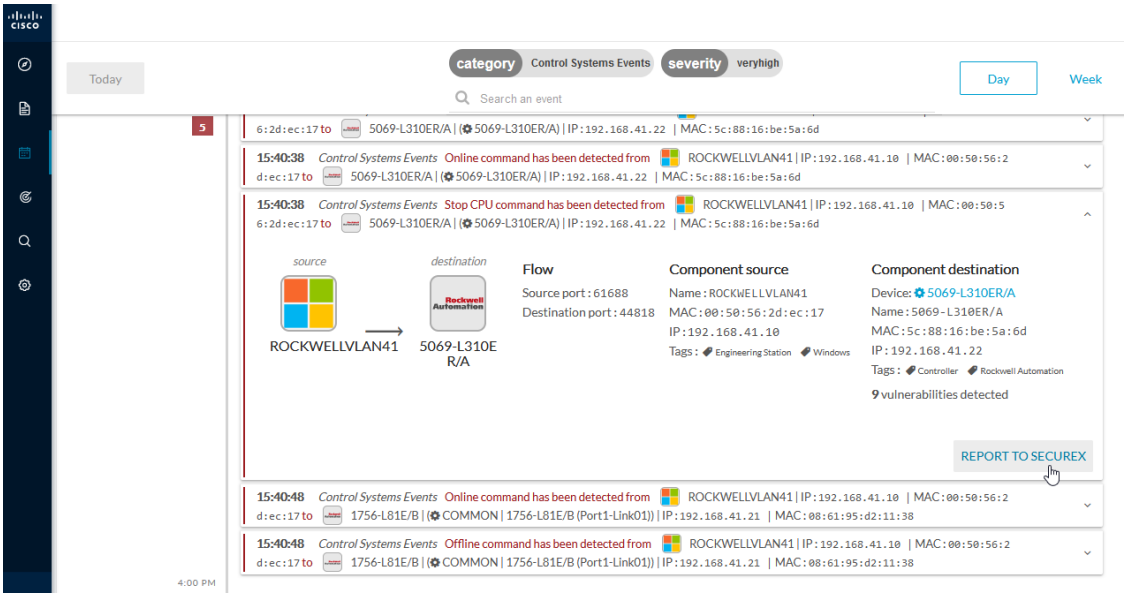
SecureX event integration

Once SecureX has been configured in Cisco Cyber Vision, a **Report to SecureX** button appears on some events of the event calendar page. Using this button will push the event to SecureX and create an incident.

The SecureX button appears on three categories of event:

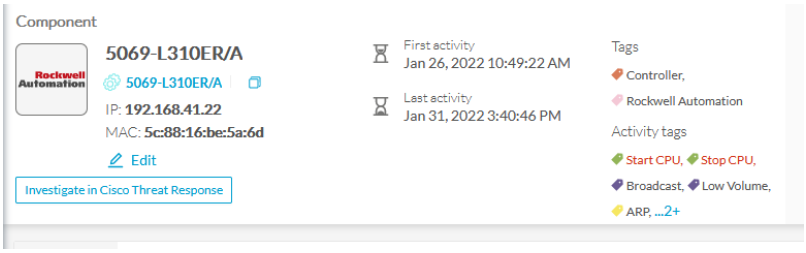
- Anomaly Detection
- Control Systems Events
- Signature Based Detection

The Report to SecureX button on a Control Systems Events:



SecureX component button

Once SecureX has been configured in Cisco Cyber Vision, the button **Investigate in Cisco Threat Response** appears on the components' technical sheet. The component's IP and MAC addresses will be investigated in SecureX Threat Response if you use this button.



External resources for SecureX integration

Herebelow is the list of all URLs called by the Cisco Cyber Vision Center in case you need to authorize them, for example in a firewall.

Center:

- private.intel.eu.amp.cisco.com
- private.intel.apjc.amp.cisco.com
- private.intel.amp.cisco.com
- intel.amp.cisco.com
- visibility.eu.amp.cisco.com
- visibility.apjc.amp.cisco.com
- visibility.amp.cisco.com

Web client:

- securex.apjc.security.cisco.com
- securex.us.security.cisco.com