



Integrations

- pxGrid, on page 1
- FMC, on page 2
- FTD, on page 3
- XDR, on page 4
- SecureX, on page 12

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.

The screenshot shows the Cisco ISE configuration page for Platform Exchange Grid. The left sidebar contains navigation options: Network Organization, Sensors, Users, Events, API, License, LDAP Settings, Snort, Risk score, and Integrations. Under Integrations, pxGrid is selected. The main content area is titled 'Platform Exchange Grid' and includes a description: '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. Filling and submitting the fields below activates the sharing of endpoint assets discovered by this system with a Cisco Identity Services Engine (ISE) pxGrid controller. This information can then be leveraged by upstream security systems to monitor security, detect threats, and set network policy. Learn more [here](#).' Below the description are three sections: 'Center Certificate Authority' with a 'Download certificate' button; 'ISE Server' with a 'Register a new node' section containing 'Node Name' and 'Host Name' input fields, and a note 'Name of the pxGrid Node to be created on ISE pxGrid Server'; and 'Client certificate' with an 'Import PxGrid certificate' button. A red error message box is visible at the bottom right, stating 'Error while fetching certificate configuration. (Unknown error)'.

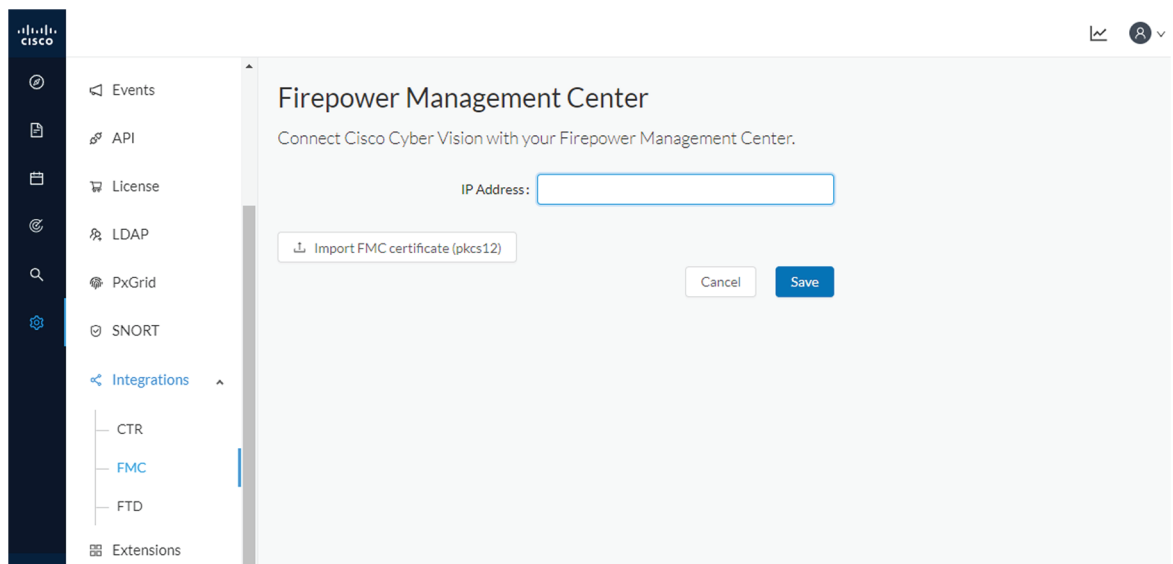
For more information about how to perform this integration, refer to the manual "Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid".

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:

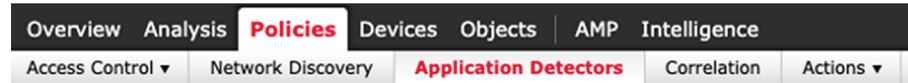
- Name
- Id
- Ip
- Mac
- And if they are available:
 - hw_version
 - model-ref
 - serial_number
 - fw_version
 - tags

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:



Third-Party Product Maps

Product Map

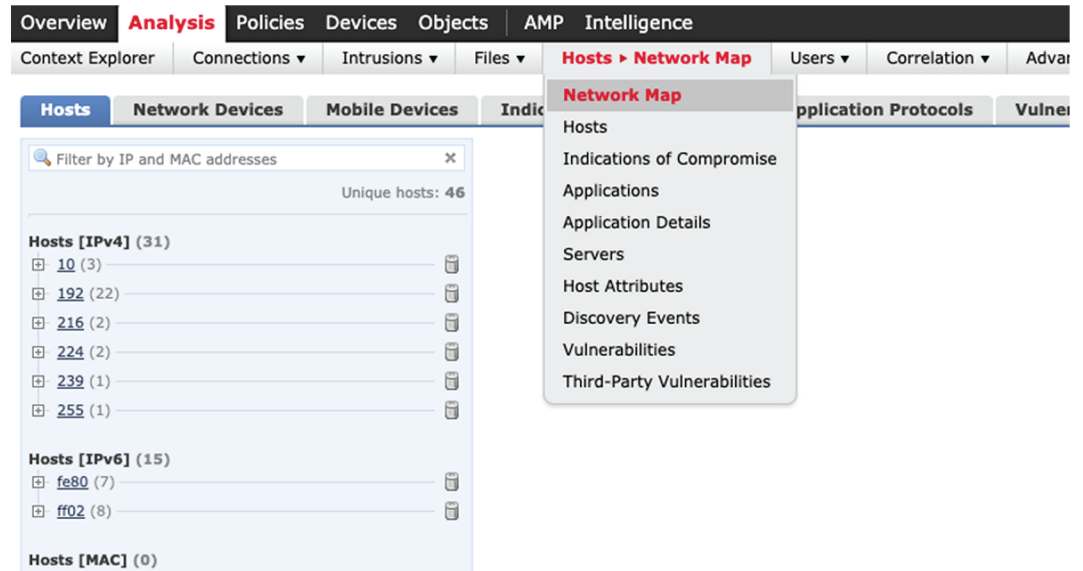
CyberVision

[Integration with Cisco Cyber Vision](#)

Third-Party Vulnerability Maps

No vulnerability mapping sets currently defined.

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

XDR

Cyber vision could be integrated with XDR, a cloud-native, built-in platform that connects our Cisco Secure portfolio with your infrastructure. It allows you to radically reduce dwell time and human-powered tasks.



Note SecureX will reach its end of life on July 31, 2024. However, it is still possible to utilize SecureX until then by adjusting the desired integration here.

Cisco XDR is an online platform that centralizes security events from various Cisco software equipments through an API. For instance, events such as those from Cisco Cyber Vision or firewall activities can be transmitted to Cisco XDR and correlated, then presented across diverse dashboards.

XDR integration enables three features in Cisco Cyber Vision:

- Without XDR SSO login, the **Investigate in XDR Threat Response** button will appear on components' technical sheets.
- With XDR SSO login, the **Report to XDR** button will appear on certain events of the event calendar page. This button is utilized to push the events to XDR.

- With XDR SSO login, an XDR ribbon featuring several functionalities can be activated within Cisco Cyber Vision.

This section details the configuration of XDR in Cisco Cyber Vision and different authorized features.

XDR Configuration

Before you begin

The Cisco XDR configuration in Cisco Cyber Vision requests:

- An Admin access to Cisco Cyber Vision.
- A Cisco Cyber Vision Center with internet access.
- A XDR account with an admin role.

Step 1

In Cisco Cyber Vision, navigate to **Admin > Integrations > XDR**.

Step 2

Select a Region.

The screenshot shows the Cisco Cyber Vision interface for XDR / SecureX configuration. The left sidebar lists various integration options, with 'Integrations' expanded to show 'XDR / SecureX'. The main content area has a title 'XDR / SecureX' and a description: 'XDR is a cloud-native, built-in platform that connects our Cisco Secure portfolio and your infrastructure. It allows you to radically reduce dwell time and human-powered tasks.' Below this is a 'Configuration' section. A green success message states 'XDR is enabled.' and provides instructions for users. A blue information message states 'SecureX reaches end of life on July 31, 2024' and offers a way to continue using SecureX. Below these messages, there are instructions on how to activate XDR integration features, including creating incidents from event categories and activating the XDR Ribbon. At the bottom, there is a 'Region' dropdown menu set to 'North America' and a red 'Disable XDR' button.

The button **Enable XDR** appears.

The screenshot shows a close-up of the 'Region' dropdown menu, which is currently set to 'North America'. To the right of the dropdown is a blue button labeled 'Enable XDR'.

Step 3

Click **Enable XDR** to enable the link.

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

Configuration

✔ XDR is enabled.
Users will get a notification when they log in to inform them that they can use the Ribbon once they authenticated through XDR from their profile. Go to [your profile](#) to also authenticate to XDR and activate the features listed above.

i SecureX reaches end of life on July 31, 2024
It is still possible to use SecureX until then by changing the desired integration here (the currently enabled integration must be disabled first)
Product: XDR SecureX

If you activate this option users will be able to authenticate and benefit from XDR integration's features:

- Create incidents from the events page for these categories of events:
 - Anomaly Detection
 - Control Systems Events
 - Signature based Detection
- Activate XDR Ribbon and benefit from the associated features

Moreover, without using XDR authentication, users will be able to use the Investigate button from Cyber Vision technical sheet of components to be which will lead them to CTR.

Region

Disable XDR

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

Step 4

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

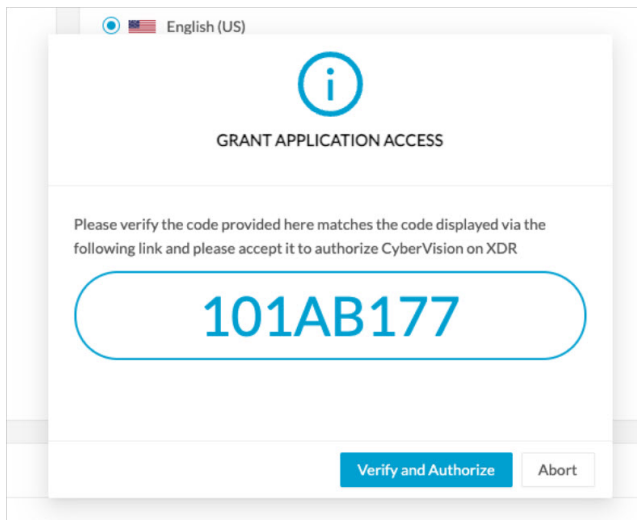
A new XDR menu appears on the right.

The screenshot shows the 'My settings' page with the following details:

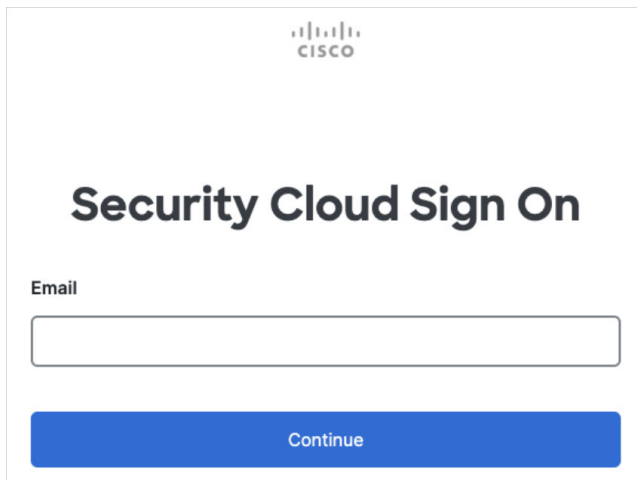
- General:** Email: admin@sentryo.net, Role: Admin, Firstname: admin, Lastname: admin.
- Language:** English (US) is selected. Other options include Deutsch, Español (España), Français, 日本語, 한국어, and Türkçe.
- Password:** Fields for Current password, New password, Suggested password (5m!Dw!qY_n2, vBL), and Confirm new password.
- Notification:** A checkbox for 'Restore default parameters'.
- XDR:** A 'Log in' button with the text 'Before activating the ribbon, please log in the XDR site.'
- Footer:** A 'Save settings' button.

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

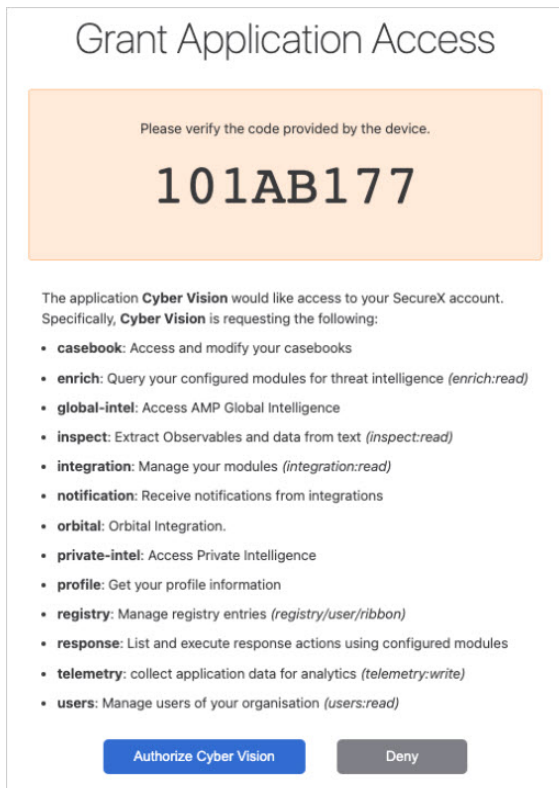
A popup appears with an authentication code.



A page opens in the browser to grant Cisco Cyber Vision access to XDR. First a login is required:

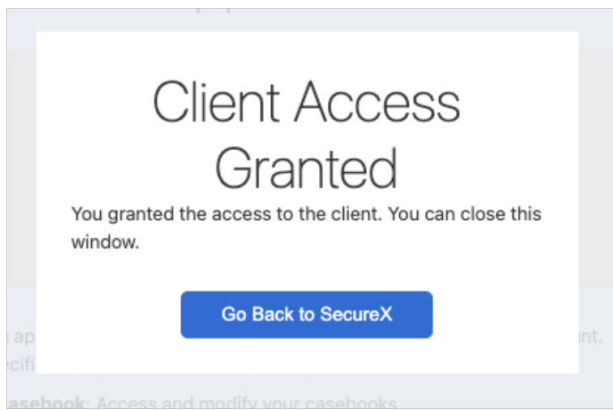


Then the authorization is required:

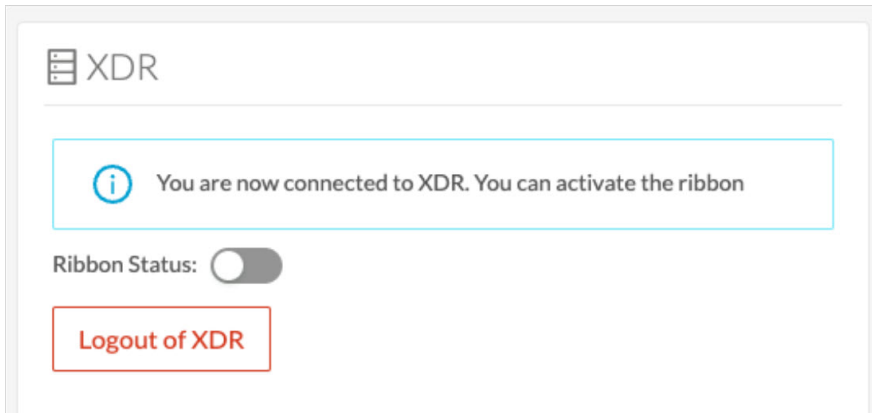


Step 6 Click **Authorize Cyber Vision**.

Step 7 A Client Access Granted popup appears.

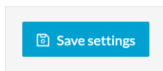
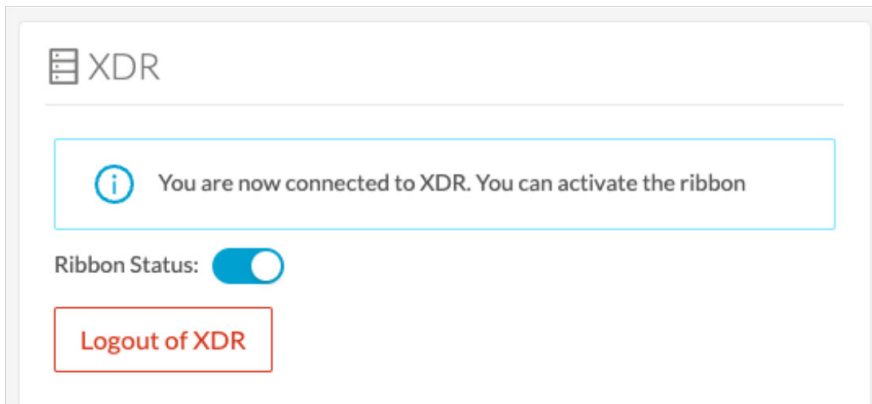


Step 8 In Cisco Cyber Vision > My Settings, the XDR menu indicates that Cisco Cyber Vision is connected to XDR. A toggle button to enable the XDR ribbon and a button to logout of XDR are displayed.

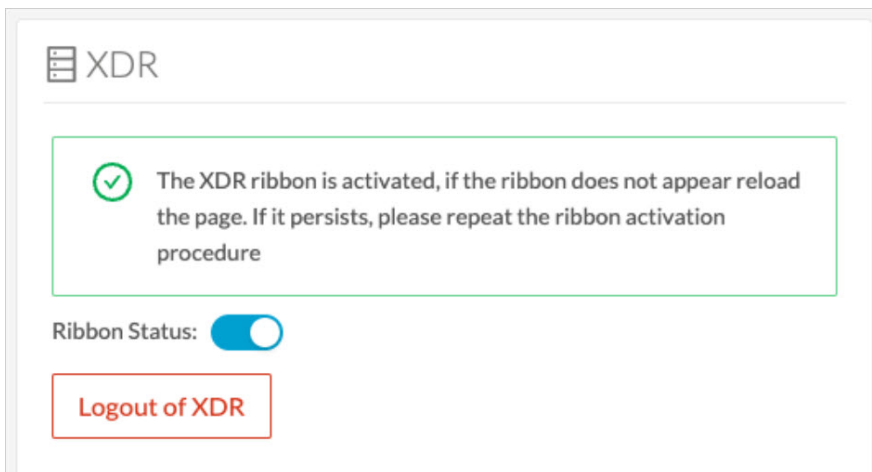


Step 9 Use the **Ribbon status** toggle button to enable the XDR ribbon.

Step 10 Click **Save settings**.



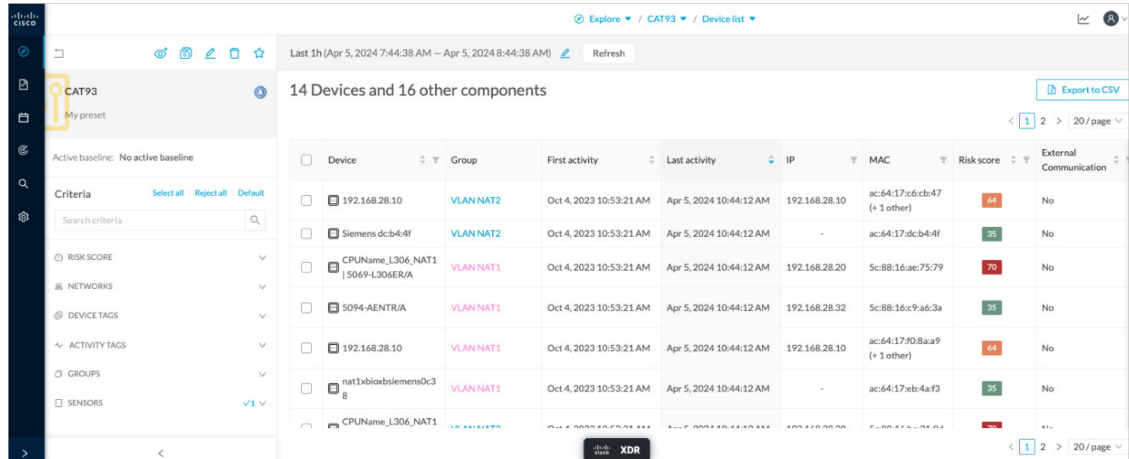
A message indicating that the XDR ribbon is enabled appears.



XDR ribbon

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

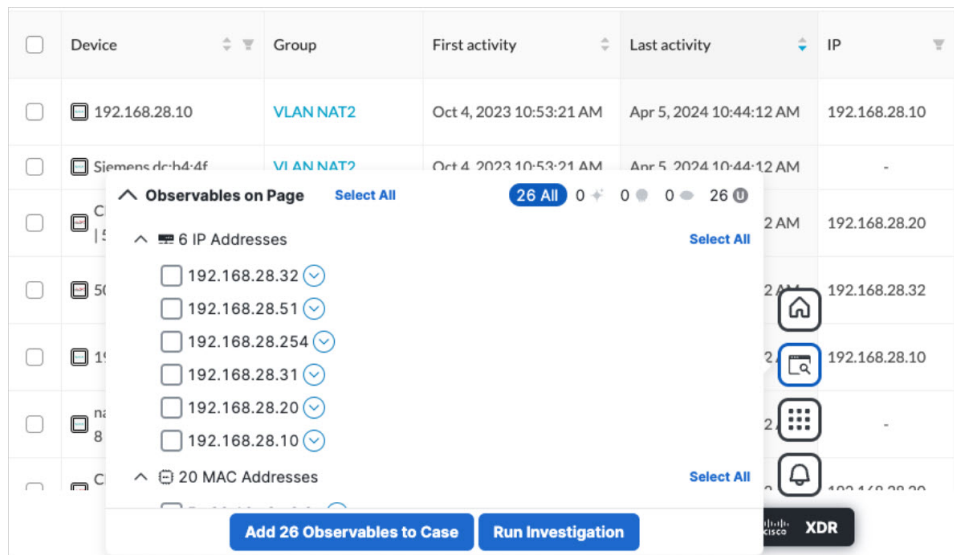
The XDR ribbon in the Device List view:



Device	Group	First activity	Last activity	IP	MAC	Risk score	External Communication
192.168.28.10	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10	ac:64:17:c6:cb:47 (+ 1 other)	64	No
Siemens dc:b4:4f	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-	ac:64:17:cb:4:4f	35	No
CPUName_L306_NAT1 5069-L306ER/A	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.20	5c88:16:ae:75:79	70	No
5094-AENTRJA	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.32	5c88:16:c9:a6:3a	35	No
192.168.28.10	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10	ac:64:17:d0:8aa9 (+ 1 other)	64	No
nat1xbloxsiemens0c38	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-	ac:64:17:eb:4a:f3	35	No
CPUName_L306_NAT1	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.20	5c88:16:c9:a6:3a	35	No

The [Cisco XDR Getting Started Guide](#) explains how to use the XDR ribbon.

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



Device	Group	First activity	Last activity	IP
192.168.28.10	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10
Siemens dc:b4:4f	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-
CPUName_L306_NAT1 5069-L306ER/A	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.20
5094-AENTRJA	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.32
192.168.28.10	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10
nat1xbloxsiemens0c38	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-
CPUName_L306_NAT1	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.20

XDR event integration

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

The XDR button appears on three categories of event:

- Anomaly Detection

- Control Systems Events
- Signature Based Detection

The Report to XDR button on a Control Systems Events:

Time	Severity	Category	Description
October 17, 2023 10:03:42 AM	critical	Control Systems Events	Init has been detected from 192.168.28.10 (VLAN NAT1) (@ 192.168.28.10) IP: 192.168.28.10 MAC: ac:64:17:f0:8a:a9 to nat1xbioxbsiemens0c38 (VLAN NAT1) (@ nat1xbioxbsiemens0c38) IP: 192.168.28.30 MAC: ac:64:17:eb:4af3

source	destination	Flow	Source component	Destination component
192.168.28.10	nat1xbioxbsiemens0c38	Flow information unavailable	Device: 192.168.28.10 Name: 192.168.28.10 MAC: ac:64:17:f0:8a:a9 IP: 192.168.28.10 Tags: Controller, Web Server Vulnerabilities detected: 11	Device: nat1xbioxbsiemens0c38 Name: nat1xbioxbsiemens0c38 MAC: ac:64:17:eb:4af3 IP: 192.168.28.30 Tag: IO Module

[Report to XDR](#)

XDR component button

Once XDR 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 XDR Threat Response if you use this button.

Component

SIEMENS nat1xb1515.profinetxainterf ace319a

192.168.28.10

VLAN NAT1 None

IP: -

MAC: ac:64:17:f0:8a:ab

[Edit](#)

[Investigate in Cisco XDR](#)

First activity: Oct 4, 2023 10:53:21 AM

Last activity: Apr 5, 2024 10:57:42 AM

Tags: Controller

Activity tags: Multicast, Link Layer Discovery Protocol, Profinet

External Resources for XDR 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:

North America

- Cisco XDR Platform: <https://visibility.amp.cisco.com/iroh/>
- Cisco XDR Private Intelligence: <https://private.intel.amp.cisco.com/ctia/>
- Cisco XDR Automation: <https://automate.us.security.cisco.com/api/>

Europe

- Cisco XDR Platform: <https://visibility.eu.amp.cisco.com/iroh/>
- Cisco XDR Private Intelligence: <https://private.intel.eu.amp.cisco.com/ctia/>

- Cisco XDR Automation: <https://automate.eu.security.cisco.com/api/>

Asia Pacific, Japan, and China

- Cisco XDR Platform: <https://visibility.apjc.amp.cisco.com/iroh/>
- Cisco XDR Private Intelligence: <https://private.intel.apjc.amp.cisco.com/ctia/>
- Cisco XDR Automation: <https://automate.apjc.security.cisco.com/api/>

Web client:

- conure.apjc.security.cisco.com
- conure.us.security.cisco.com
- conure.eu.security.cisco.com

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

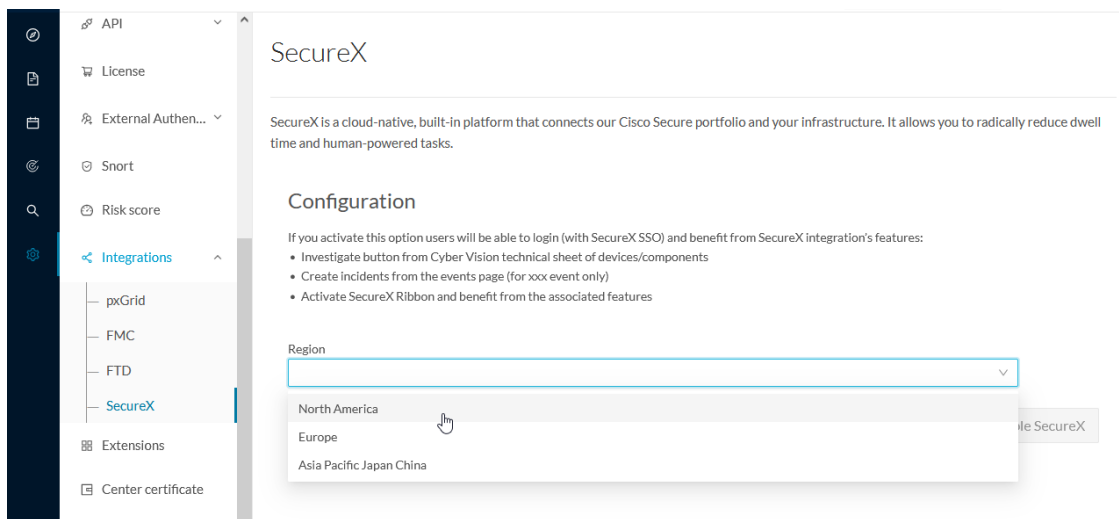
Before you begin

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.



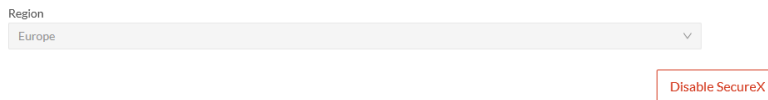
The button **Enable SecureX** appears.



Step 3

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

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

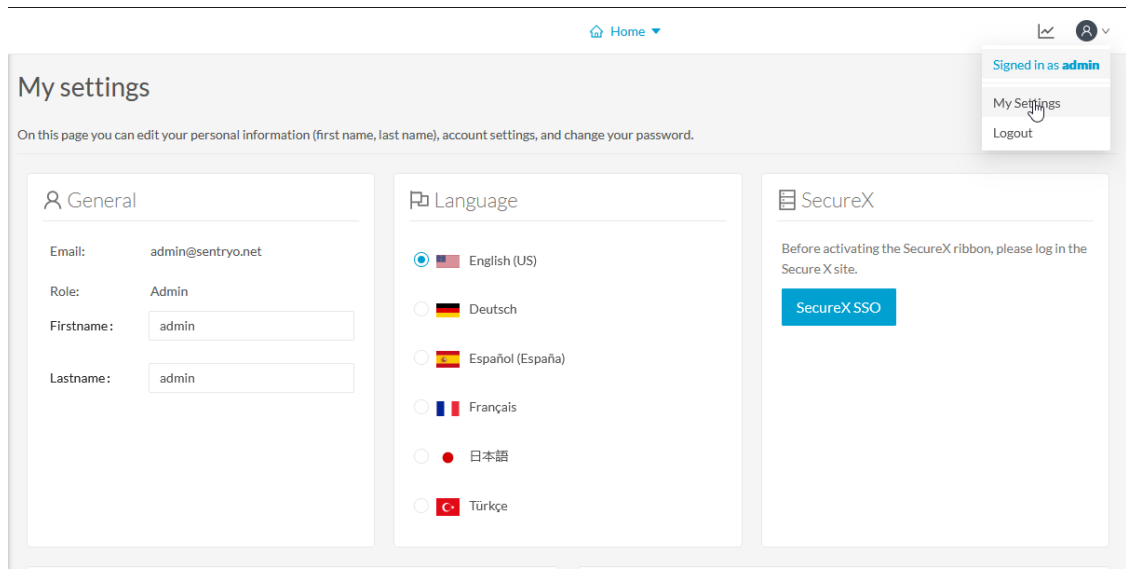


By completing the steps above, you are now able to use the button **Investigate in SecureX Threat Response** that will appear in the components' technical sheet. To install and use the SecureX ribbon and the Report to SecureX button, complete the steps herebelow.

Step 4

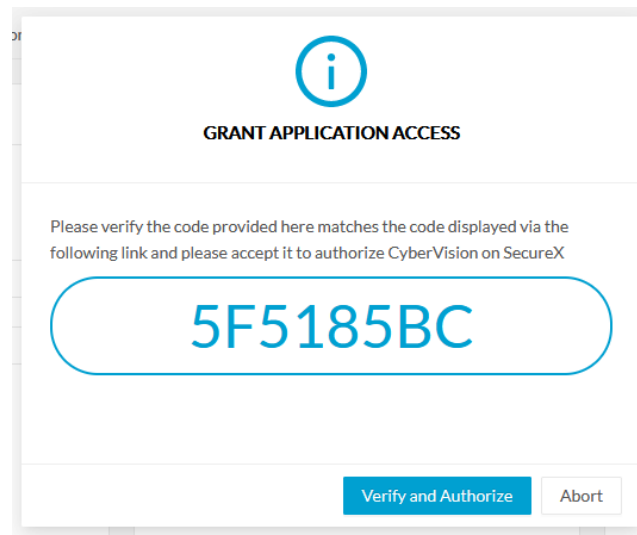
Navigate to the user menu on the top right corner of the GUI and click **My Settings**.

A new SecureX menu appears on the right.

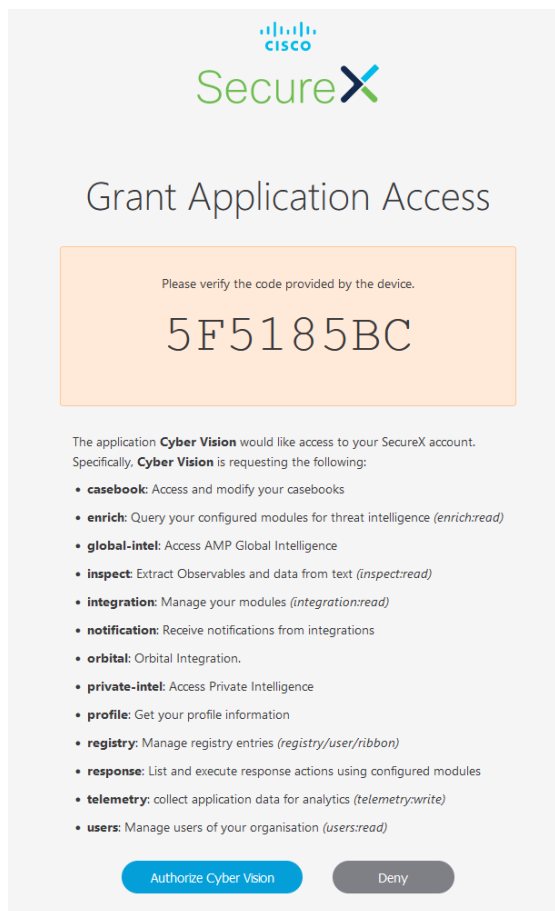


Step 5 Click the **SecureX SSO** button.

A popup appears with an authentication code.

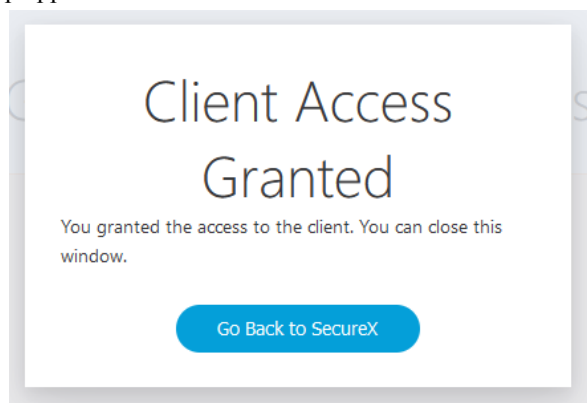


A page opens in the browser to grant Cisco Cyber Vision access to SecureX.

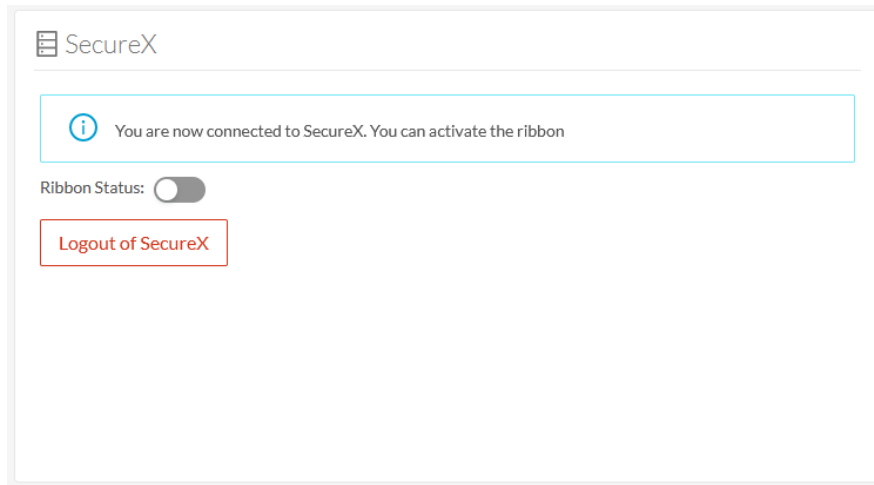


Step 6 Click **Authorize Cyber Vision**.

Step 7 A Client Access Granted popup appears.

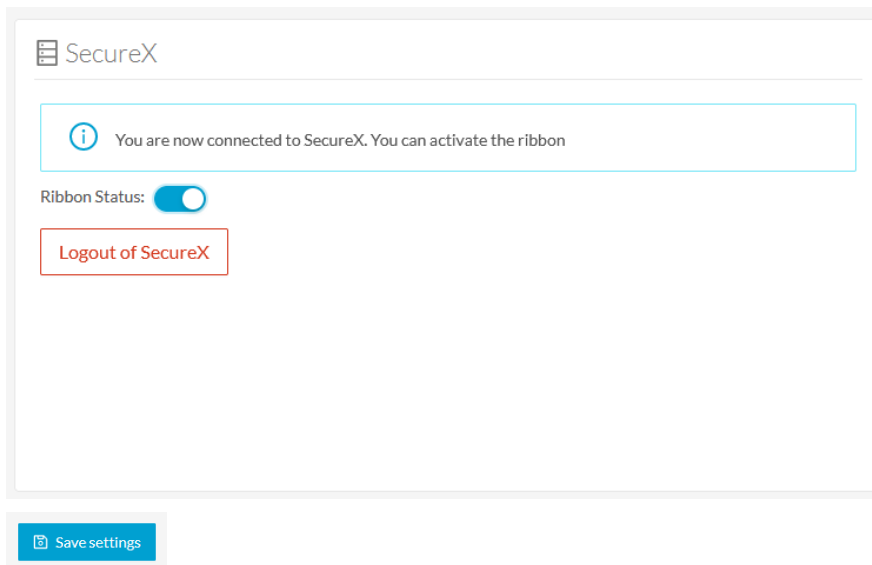


Step 8 In Cisco Cyber Vision > My Settings, the SecureX menu indicates that Cisco Cyber Vision is connected to SecureX. A toggle button to enable the SecureX ribbon and a button to logout of SecureX are displayed.

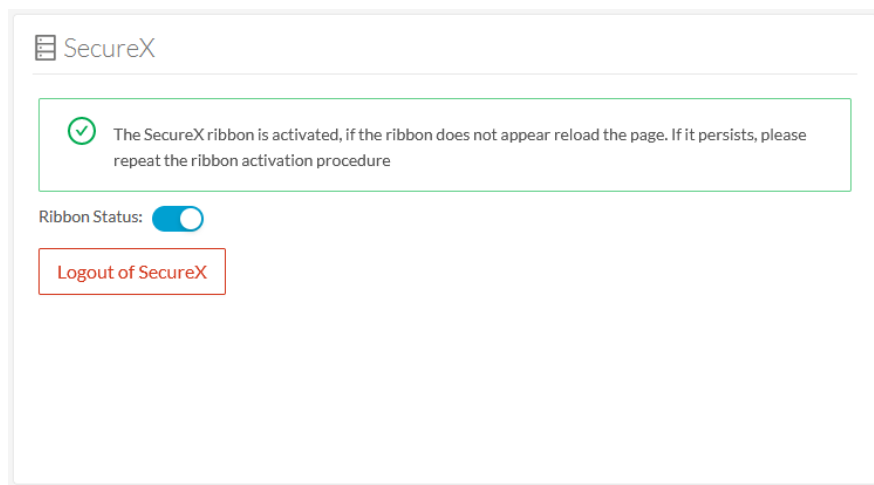


Step 9 Use the **Ribbon status** toggle button to enable the SecureX ribbon.

Step 10 Click **Save settings**.



A message indicating that the SecureX ribbon is enabled appears.



SecureX ribbon

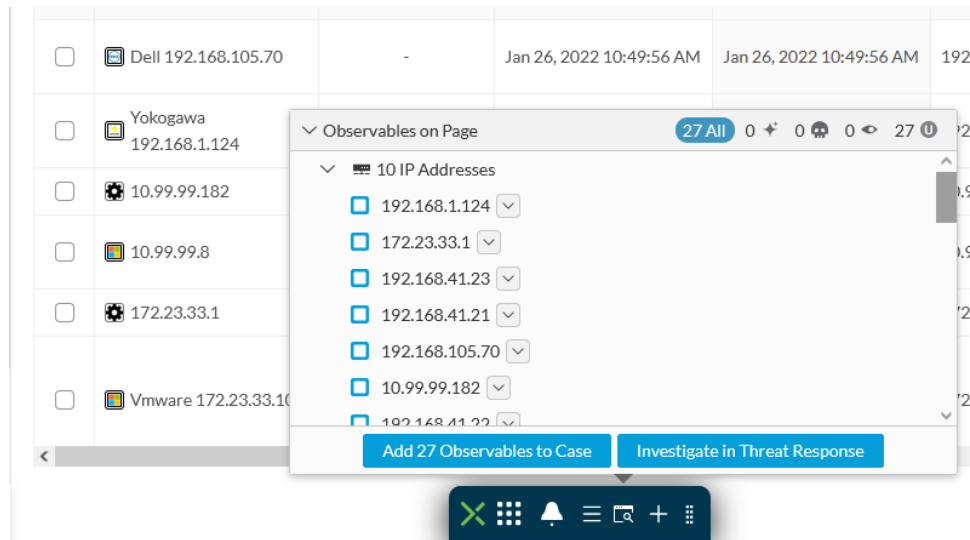
Once configured and activated, the SecureX ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.

The SecureX ribbon in the Device List view:

Device	Group	First activity	Last activity	IP	MAC	Risk so
Dell 192.168.105.70	-	Jan 26, 2022 10:49:56 AM	Jan 26, 2022 10:49:56 AM	192.168.105.70	00:11:43:6cf8:89 (+ 1 other)	
Yokogawa 192.168.1.124	-	Jan 26, 2022 10:49:56 AM	Jan 26, 2022 10:49:56 AM	192.168.1.124	00:00:64:8c6a:2c	
10.99.99.182	-	Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	10.99.99.182	00:2ae3:cca2:2e	
10.99.99.8	-	Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	10.99.99.8	00:2ae3:cca2:2e	
172.23.33.1	-	Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	172.23.33.1	00:2ae3:cca2:2e	
Vmware 172.23.33.10	-	Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	172.23.33.10	00:0c:29:9e:89:5f	

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:



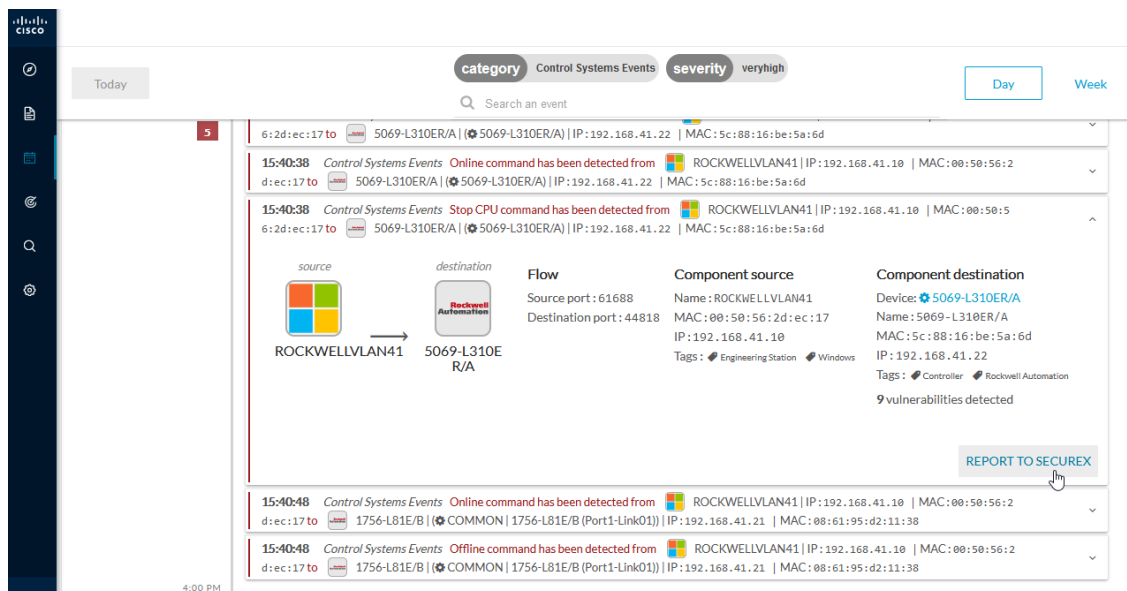
SecureX event integration

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:

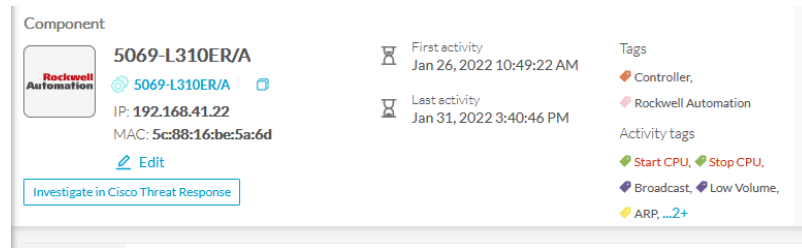
- Anomaly Detection
- Control Systems Events
- Signature Based Detection

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

