Integrate with Cisco Cyber Vision

pxGrid

From **Platform Exchange Grid** 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.

To access the **Platform Exchange Grid** page, choose **Admin** > **Integrations** > **pxGrid** from the main menu.

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".

XDR

Cisco Cyber Vision can be integrated with XDR, a cloud-native, built-in platform that connects the Cisco Secure portfolio with your infrastructure. This integration allows you to significantly reduce dwell time and human-powered tasks.

Note SecureX reached its end of life on July 31, 2024.

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

Procedure

Step 1 From the main menu, choose **Admin** > **Integrations** > **XDR**.

Step 2 Click the dropdown arrow of the **Region** field.

Step 3 Select the region from dropdown list.

Step 4 Click **Enable XDR** to enable the link.

Once you enable the link, the button turns red to indicate **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 5 Click the user menu located in the top right corner of the GUI.

Step 6 Click **My Settings**.

A new **XDR** menu appears on the right of the **My settings** page.

Step 7 Click the **Log in** button.

A **Grant Application Access** popup appears with an authentication code.

Step 8 Click **Verify and Authorize**.

The browser opens a new page with the **Security Cloud Sign On** window to grant Cisco Cyber Vision access to **XDR**.

Step 9 Enter **Email** and click **Continue**.

Step 10 Click **Authorize Cyber Vision**.

A **Client Access Granted** popup appears.

Step 11 In **Cisco Cyber Vision Center** > **My Settings**, the XDR menu indicates that Cisco Cyber Vision is connected to XDR.

Step 12 Use the **Ribbon status** toggle button to enable the XDR ribbon.

Once you enable the **Ribbon status** toggle button, message appears.

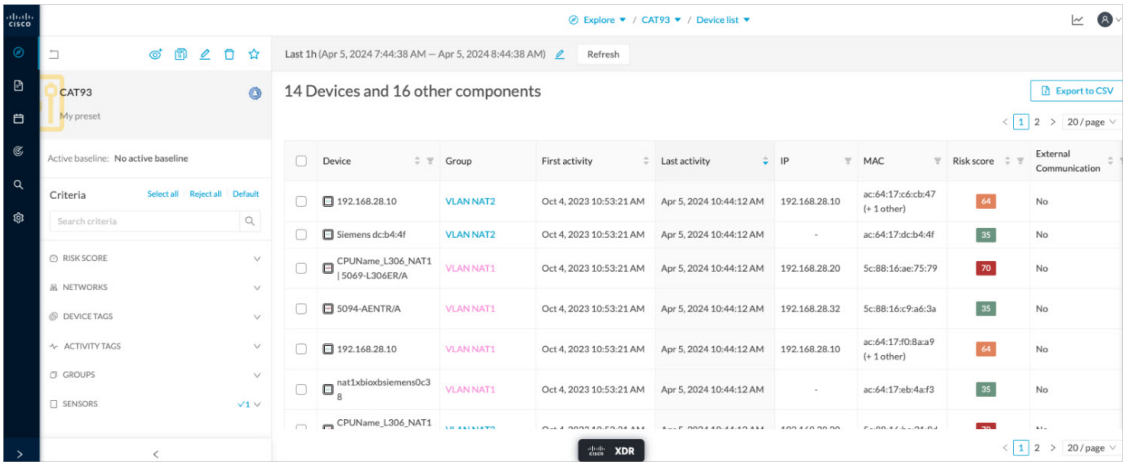
Step 13 To log out, click **Logout of XDR**.

Step 14 Click **Save settings**.

XDR Ribbon

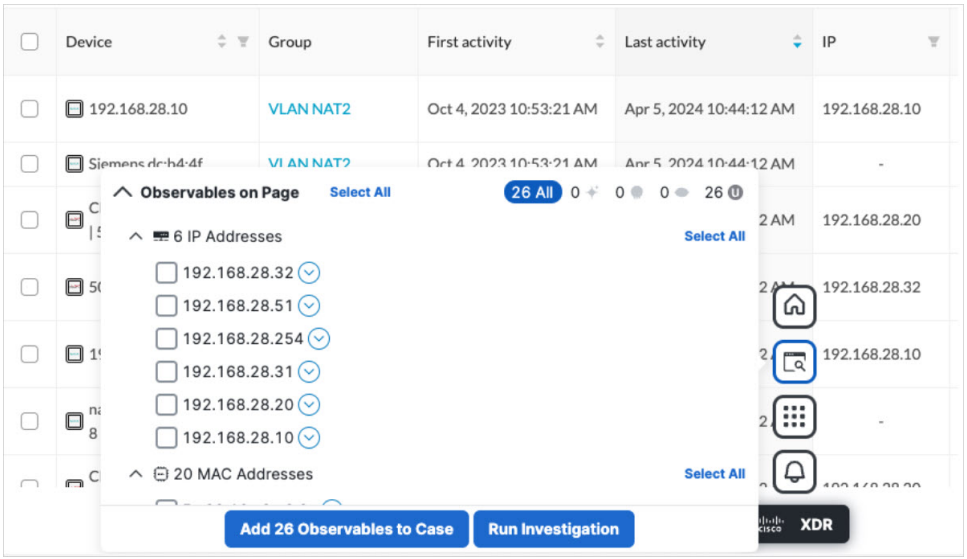
Once configured and activated, the XDR ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.

The XDR ribbon in the Device List view:



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:



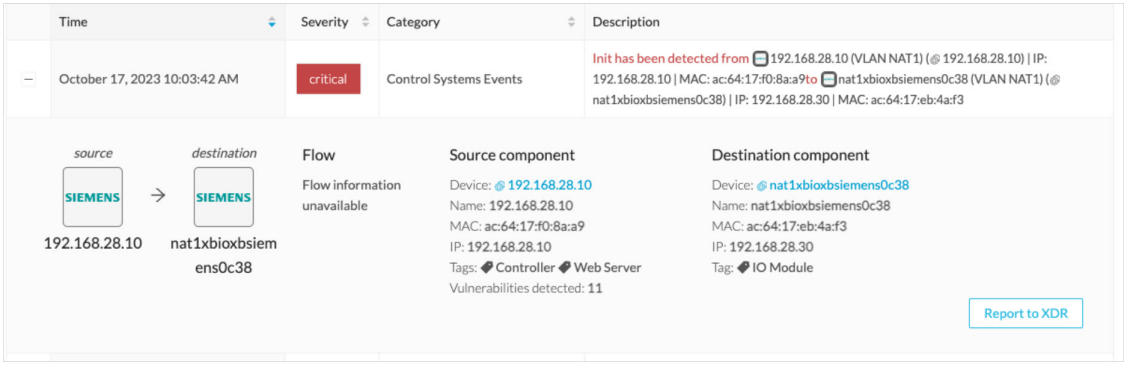
XDR Event Integration

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:

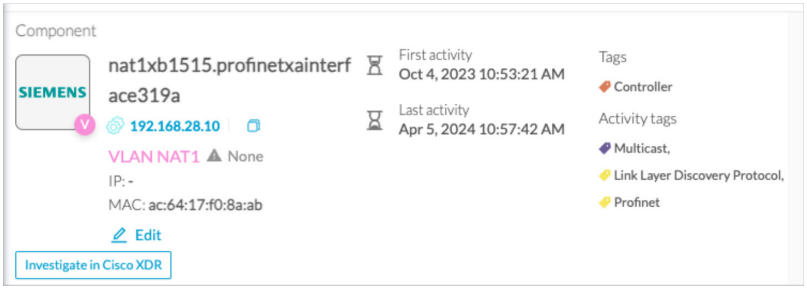
- Anomaly Detection
- Control Systems Events
- Signature Based Detection

The Report to XDR button on a Control Systems Events:



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.



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