Cisco Cyber Vision GUI Administration Guide, Release 5.0.0

First Published: 2022-08-02

Last Modified: 2024-07-12

CONTENTS

About this documentation

-
-

Document purpose

This user guide describes how to administrate and configure Cisco Cyber Vision.

It shows the GUI with the highest license level (Advantage) and the **Admin** and **Product** user roles.

This manual is applicable to **system version 5.0.0**.

Warnings and notices

To ensure your personal safety and to prevent damage to property, observe the following: Warnings and notices and Safety Alert symbols. These notices are graded according to the degree of danger.

Warning Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage. Take precautions.

Important Indicates risks that could involve property or Cisco equipment damage and minor personal injury. Take precautions.

Note Indicates important information on the product described in the documentation.

Warnings and notices

CHAPTER 1

System

Center shutdown/reboot

You can trigger a safe shutdown and reboot of the **Center**. Click **Admin > System**.

Use **Reboot** to fix a minor bug, such as a system overload.

Upgrade with a combined update file
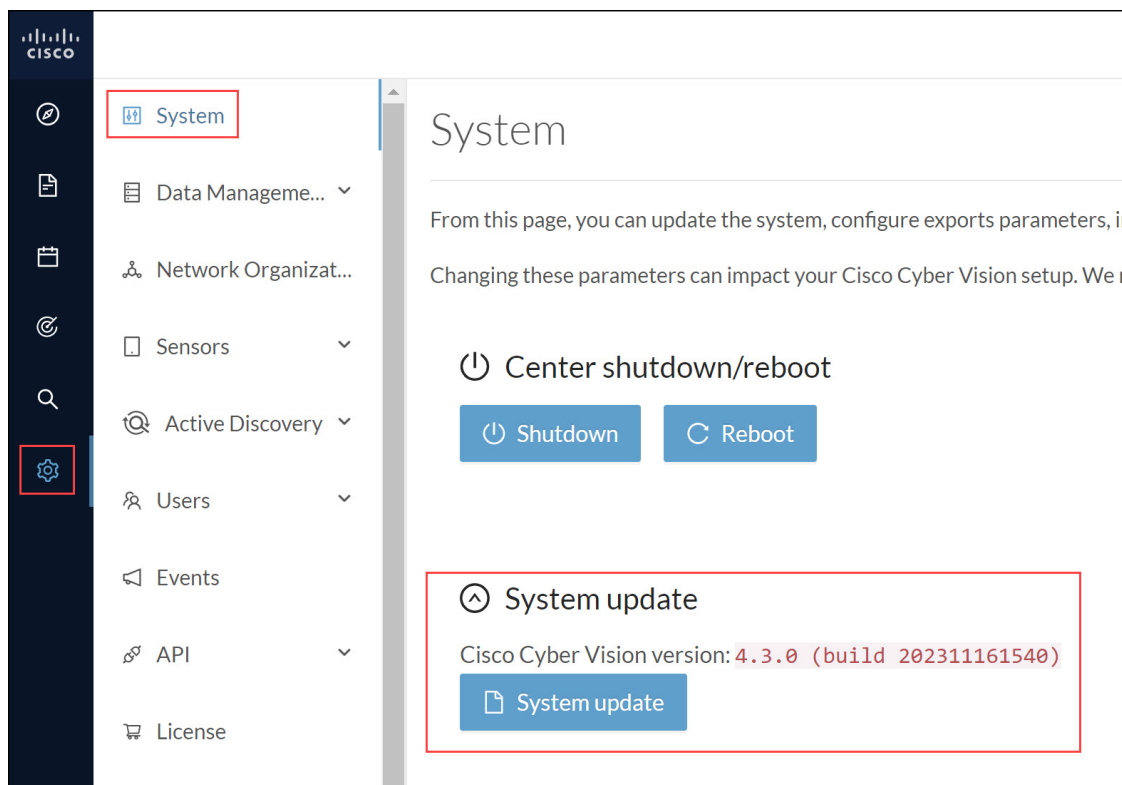
Version releases include a combined update file for the Center, the SENSOR3, SENSOR5, SENSOR7 and the Cisco IC3000 Industrial Compute Gateway. If operating conditions allow, update the Center and all these sensors at once from the GUI. Click **Admin > System**.

Note Verify all your sensors are connected and SSH is authorized between the Center and the sensors before proceeding to a combined update. Click **Admin > Sensors > Sensor Explorer**.

Important Rolling back to an older Cisco Cyber Vision version is not supported.

Requirements

- A combined update to retrieve from cisco.com.

Use the SHA512 checksum provided by Cisco to verify that the file you just downloaded is healthy.

Windows users:

Step 1 Retrieve the Cisco Cyber Vision combined update from cisco.com.

Step 2 Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List

```
PS C:\Users_____ > Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List

Algorithm : SHA512
Hash      : 1338BFB1A17110AF80D751AE7B450F2B29CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
            1B622E4B0BB8EBB9E94DB16
Path      : C:\Users_____\Downloads\CiscoCyberVision-center-3.2.3.ova
```

Step 3 In cisco.com, mouse over the file and copy the SHA512 checksum.

Software Download

Downloads Home / Security / Network Visibility a

| Details | ✕ |

Description : VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova
Release : 3.2.3
Release Date : 30-Apr-2021
FileName : CiscoCyberVision-center-3.2.3.ova
Size : 382.92 MB (401520640 bytes)
MD5 Checksum : ad553391b4f43128ef922e1a98e7e58c
SHA512 Checksum : 1338bfb1a17110af80d751ae7b450f2b ...

Release Notes for 3.2.3 Advisories

VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova
CiscoCyberVision-center-3.2.3.ova
Advisories

Step 4 Compare both checksums.

- If both checksums are identical, the file is healthy.

- If the checksums do not match, download the file again.

- If the checksums still don't match, please contact Cisco support.

To update the Center and all applicable sensors:

Step 5 Login to Cisco Cyber Vision.

Step 6 Click **Admin > System > System update**.

Step 7 Select the update file CiscoCyberVision-update-combined-<VERSION>.dat

Step 8 Confirm the update.

As the Center and sensors update, a holding page appears. When done, click Center **Reboot**. You will be logged out.
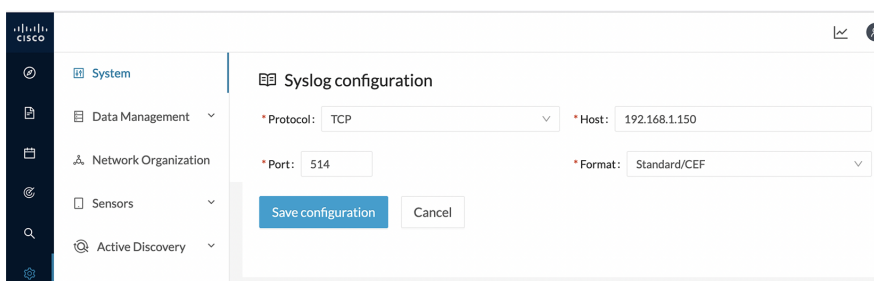
Step 9 Log in.

If sensors were offline when the update occurred, repeat the procedure until all sensors update.

Syslog configuration
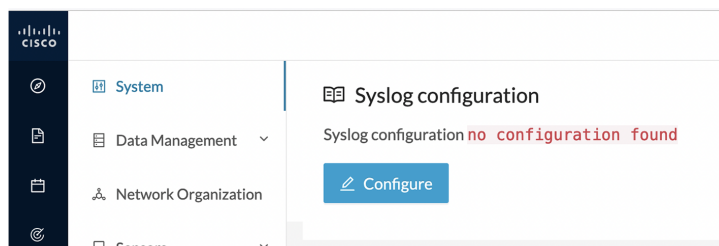
Cisco Cyber Vision provides syslog configuration so that events can be exported and used by a SIEM. The following procedure configures to which machine the syslogs will be sent.

Step 1 Click **Configure**.

Step 2 Select a protocol. Use the drop-down arrow.

If you select **TCP + TLS** connection, the **Set certificate** button displays to import a p12 file. The administrator of your SIEM solution provides this file to secure communications between the Center and the syslog collector.

Step 3 Enter the **Host** IP address of the SIEM reachable from the Administration network interface (i.e., eth0) of the Center.

Step 4 Enter the **Port** on the SIEM that will receive syslogs. Use the arrrows.

**Step 5** Select the variant of syslog **Format**.

- **Standard**: Event messages are sent in a format specific to Cisco Cyber Vision and with legacy timestamps (one-second precision).

- **CEF**: Industry standard **Common Event Format** which is understood by most SIEM solutions (no extra configuration is needed on the SIEM). This is the recommended option.

- **Standard/CEF**: Combination of both.

- **RFC3164**: Extended syslog header format with microsecond precision for timestamps.

- **RFC3164/CEF**: Combination of both.

Step 6 Click **Save configuration**.

Import/Export

Use the System interface to import and export the Cisco Cyber Vision database. Click **Admin > System**.

Regularly export the database to back up the industrial network data on Cisco Cyber Vision or if you need to transfer the database to a different **Center**.
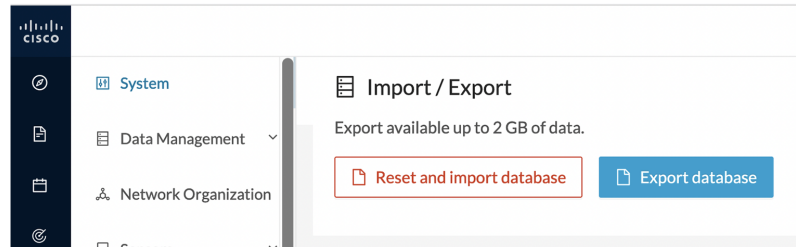
Exports database file limitation is up to 2 GB of data. This avoids side effects related to slow database exports. If the database is larger than 2 GB, you get an error message. In this case, connect to the Center using SSH and perform a data dump. Use the command: `sbs db dump`.

Network data, events, and users are retained, as well as all customizations (e.g., groups, component names).

Only configurations created in Cisco Cyber Vision's GUI persist. If you change **Center**, perform a basic configuration of the Center and then configure Cisco Cyber Vision again. Refer to the corresponding Center Installation Guide.

Note   The **Import** process may take one hour for big databases. Refresh the page to check that the import remains active (i.e., no error message).

Knowledge DB

Cisco Cyber Vision uses an internal database which contains the list of recognized vulnerabilities, icons, threats, etc.

Important   To remain protected against vulnerabilities, always update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version.

To update the Knowledge DB:

Step 1   Download the latest.db file available from cisco.com.

Step 2   Click **Admin > System > Import a Knowledge DB**. Find the file, click **Open** to upload the file.
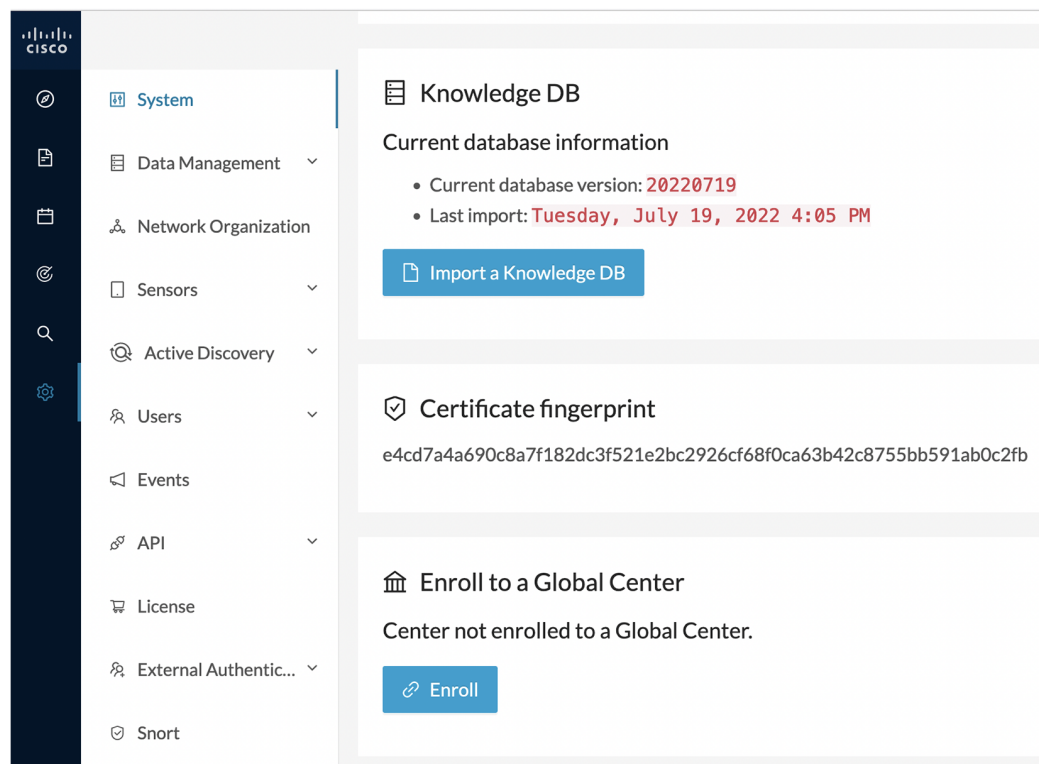
Importing the new database rematches your existing components against any new vulnerabilities and updates the network data.
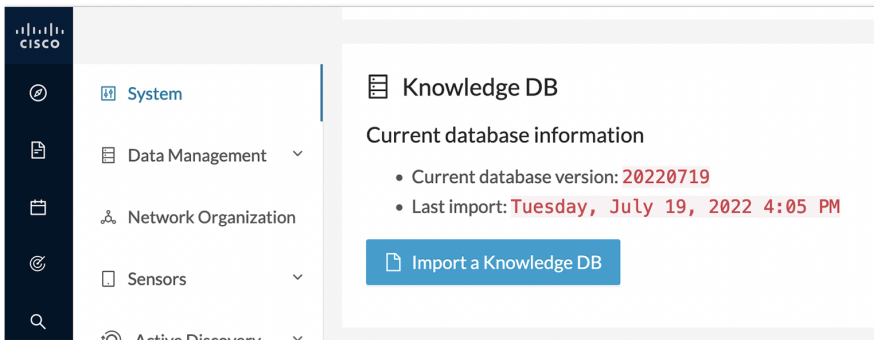
Certificate fingerprint

Use the certificate fingerprint to register a **Global Center** with its synchronized Centers and vice versa.

Click **Admin > System > Enroll to a Global Center** to enroll a Center with its synchronized Centers.

For more information, refer the Centers Installation Guides.

Cisco Cyber Vision Telemetry

Telemetry monitors your system to provide anonymous diagnostics and usage data, helps us to understand and enhance product usage. Cisco Cyber Vision telemetry data communication occurs as HTTPS traffic through Port 443 with https://connectdna.cisco.com/.

Telemetry is enabled by default. To disable this feature, follow these steps:

Step 1   From the left pane, click **Admin > System**.

Step 2   To disable the telemetry, click **ON** button.

The switch will be turned **OFF**.
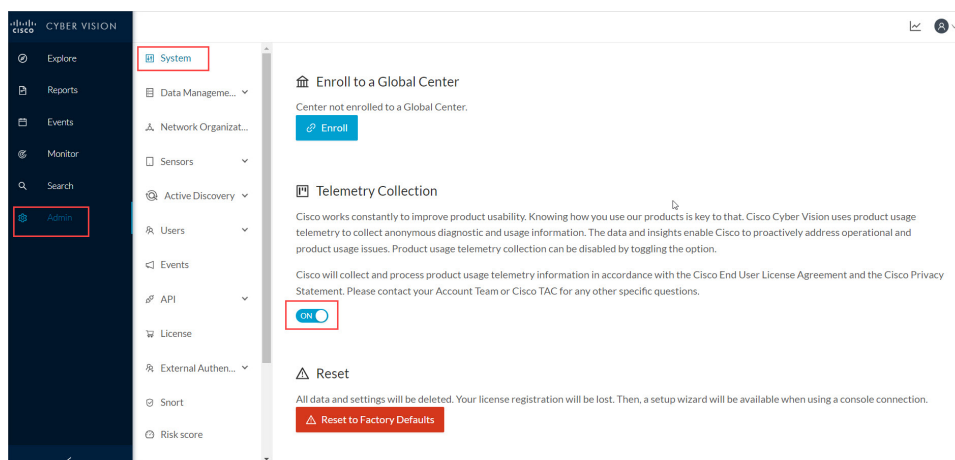
Reset to factory defaults

Only use **Reset to Factory Defaults** *as a last resort*, after all other troubleshooting attempts fail. Get help from Cisco product support.
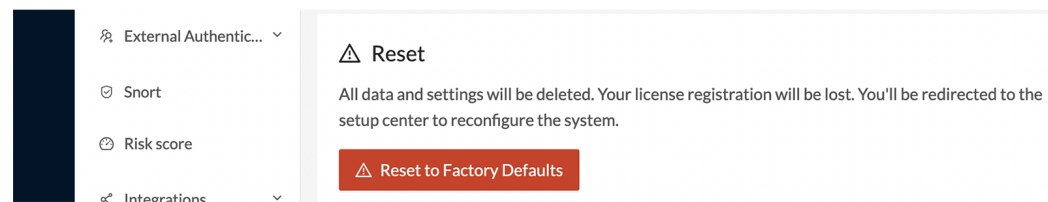
A **Reset to Factory Defaults** deletes the following:

• Some Center configuration data elements.

• The GUI configuration (such as user accounts, the setup of event severities, etc.).

• Data collected by the sensors.

• The configuration of all known sensors (such as IP addresses, capture modes, etc.).

Root password, certificates and configurations from the Basic Center configuration persist.

After a **Reset to Factory Defaults** occurs, the GUI refreshes with the Cisco Cyber Vision installation wizard. Refer to the corresponding Center Installation Guides.

CHAPTER 2

Data management

The **Data Management** interface allows you to do the following: manage data stored on Cisco Cyber Vision by Clear data to optimize the Center performances, Expiration settings, and Ingestion configuration. To access Data Management, click **Admin > Data Management.**

The Cisco Cyber Vision update procedure will not purge data automatically. The Center's 3.2.x database will be migrated to the new 4.0.0 schema. All components, activities, flows, events, etc. will be migrated. Since the migration process can take hours (from 1 to 24 hours), you can perform a data purge in release 3.2.x to shorten the migration process. Launch the purge either from the Clear data page or from the Command Line Interface (CLI), using the following command. Also, different options are offered.

```
sbs-db --help
```

Once migrated, the database content is managed with version 4.4.1 new data retention policies. Expiration settings apply. By default, the system will purge the following:

- Events after 6 months

- Flows after 6 months

- Variables after 2 years

☞

Important You have 3 days once the migration from 3.2.x to 4.0.0 is done to set Expiration settings as needed, before the default settings are applied by the system.

Clear data

Clear data stored on Cisco Cyber Vision to optimize the Center's performances. Clear data partially or totally, as follows:

- All data

- Components selection and associated data (refer to Purge components, on page 10)

- Activities, Flows and Variables

- Flows and Aariables

- Variables

To clear data, click **Admin > Data Management > Clear Data**.

Clear data **very carefully**. Clearing any data can impact monitoring of the network. Please read the implications about all data clearance below.
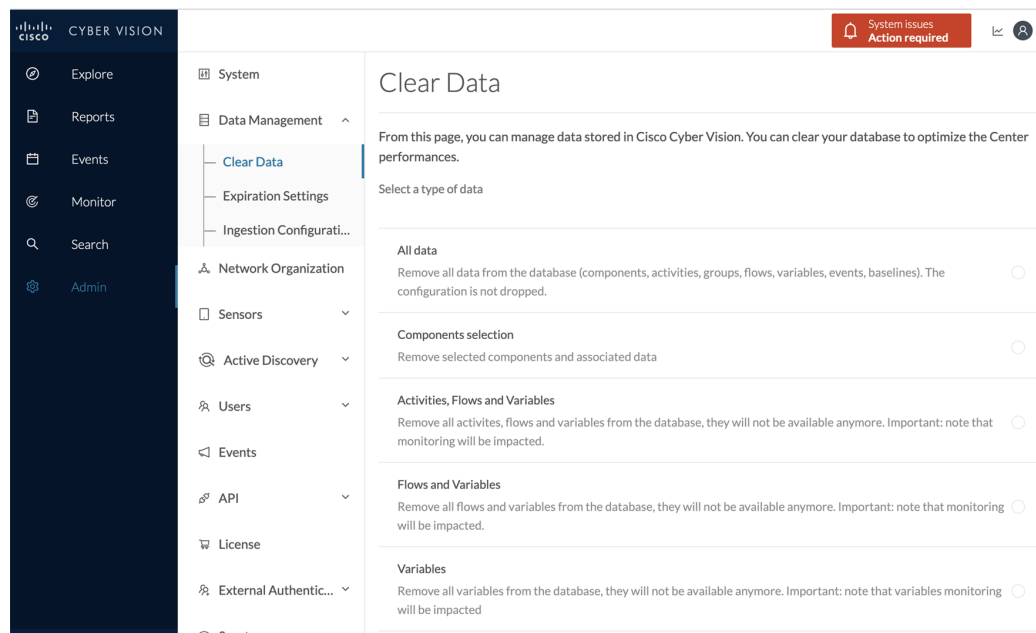

Data Clearance

Use **Clear All data** as a last resort, in case of database overload issues. This action results in the entire database content deletion. Network data such as components, flows, events and baselines are deleted from Cisco Cyber Vision and the GUI empties. All configurations are saved. Existing users and user data configuration (such as capture modes, events severity set up, syslog configuration) persist.

Purge components

In Cisco Cyber Vision, a component represents an object of the industrial network from a network point of view. It can be the network interface of a PLC, a PC, a SCADA station, etc., or a broadcast or multicast address. The system protects itself by limiting the number of components stored in the database.

When the system reaches more than 120,000 components, a popup and red banner alert appear to inform you that a purge is required. Components purge is based on several criteria.
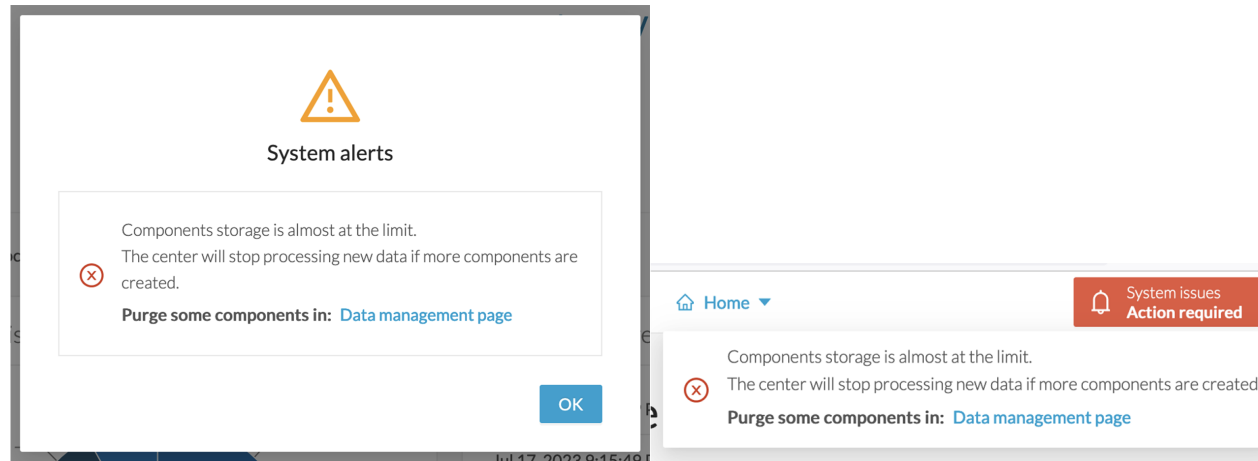
If the system reaches 150,000 components, ingestion stops. Incoming sensor data are not treated or stored and are deleted. A popup and a red banner alert appear to inform you that a purge is required.
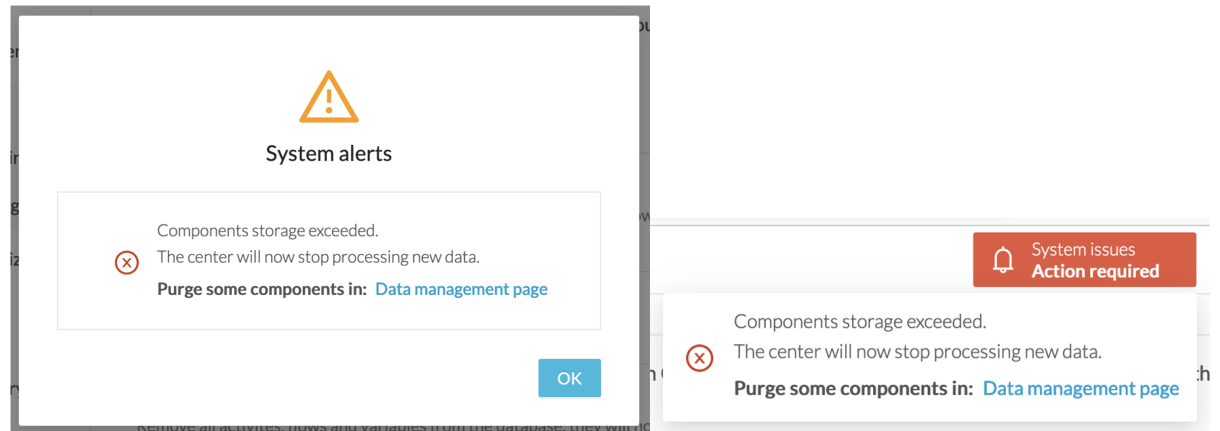
To purge components:

Step 1   Click **Admin > Data Management > Clear Data**.

Step 2   Click the **Components selection** radio button.

Step 3   Select the component type (**External, IT** or **OT**).

Step 4   Type the **IP Subnet**.

Step 5   Click the calendar icon to add an **Inactivity since** date.

Step 6   Click the calendar icon to add a **Creation time** date. Provide a **Start Time** and **End Time** (optional).

Step 7   Click **Clear data**.

Expiration settings

Follow these steps to configure the **Expiration Settings**:

1. From the left pane, click **Admin.**

2. Click **Data Management > Expiration Settings**

On this page, you can control how long data and reports stay available. You can choose expiration times for reports and their versions. Use the dropdown menu to select expiration periods of 3 months, 6 months, 1 year, 2 years, or 3 years. You can also limit the maximum number of report versions from 1 to 100.

Note   Selecting a high value might fill up storage rapidly and affect system performance. Recommended value: 10 versions.
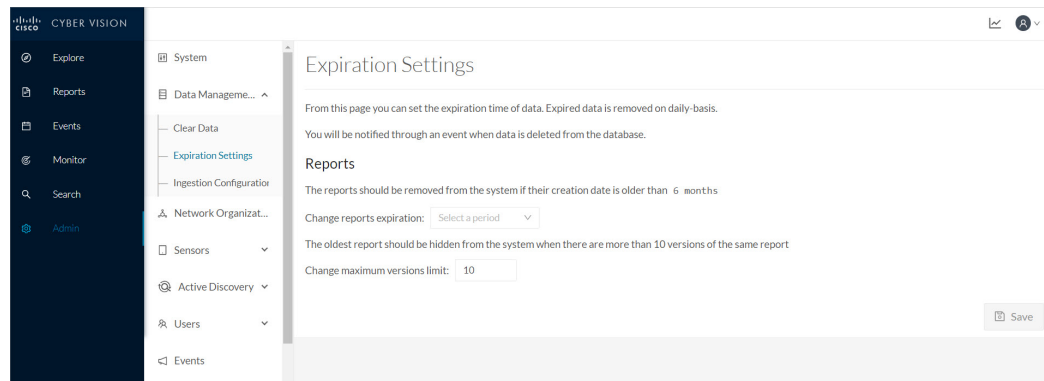
Ingestion configuration

The ingestion configuration page allows you to configure flow and variable traffic storage.

You can choose whether to store flows and variables.

Flows and variables storage is disabled by default.
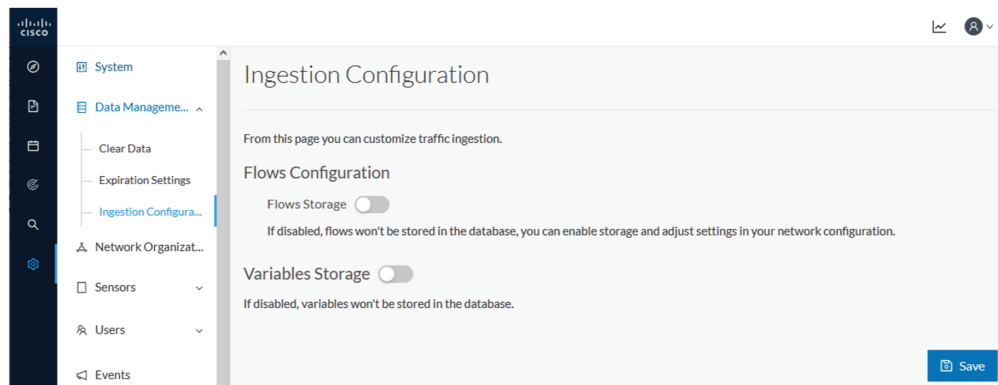
Messages can appear in Cisco Cyber Vision's user interface to indicate to the user that features may be limited due to absence of flows in the database. For example, in the activity technical sheet, at the top of the flows table:

In this case, you can click **Go to flow storage settings** and enable flow storage.

If flows storage is enabled, it is possible to choose from which subnetworks flows should be stored. These subnetworks can be set on the Network organization page. The option "others" includes flows that are not part of the industrial private network.

An automatic purge will occur on selected flows when a period of inactivity exceeds 7 days.

It is also possible to enable flows aggregation and port scan detection.

CHAPTER 3

Network organization

Network organization

This page allows you to define the subnetworks inside the industrial network by setting up IP address ranges and declaring whether networks are internal or external.

In Cisco Cyber Vision all private IP addresses are classified as OT internal. They appear in the Network Organization page **(1)**.

Every other IP address is considered as external, except for:

• Broadcast IPv4: 255.255.255.255

- IPv4 and IPv6 zero: 0.0.0.0 et 0:0:0:0:0:0:0:0

- Loopback IPv4 and IPv6: 127.0.0.1 and ::1

- Link Lock Multicast IPv4 and IPv6: 224.0.0.0/8 and ff00::/8

If you want to declare a public IP address as internal, you must add an exception by changing their network type.

Declaring a subnetwork as OT internal is useful in case public IP addresses are used in a private network of an industrial site. Conversely, declaring a set of IP addresses as external will exclude their flows from the database, and exclude their devices from the license device count and the risk score.

Overall, defining subnetworks in Cisco Cyber Vision is useful for several reasons:

- It allows you to choose afterwards how related flows should be stored through the Ingestion configuration. Excluding unnecessary flows will have positive impact on performances.

- It will impact devices' risk scores, since a private network is considered as safer than an external one.

- Cisco Cyber Vision's license will be more accurate, because devices from an external network will be excluded from the licensing device count.

By default, Cisco Cyber Vision groups identical IP addresses detected inside the industrial network into a single device, because in most cases these belong to several components of a device. However, it can happen that the same IP address is used by several devices. In this case, you can choose to select the first option when declaring a subnetwork to prevent duplicate IP addresses from grouping within this subnetwork.

The second option is to be used when components with the same IP address are found by different sensors. This happens when same addressing parameters are used on several subnetworks, for example in case of identical production lines. By using this option, components detected by different sensors will not be aggregated into a single device.

Device engine options for this network range

☐ This IP range is deployed several time, the device engine will not use IP to group components into device.

☐ Do not group component seen by different sensors. For this IP range, the device engine will only use components from one sensor to create devices.

IP ranges can be **organized into groups** which subranges can be defined like in the example below:

IP Address / subnet	VLAN ID	Network Name	Network Type	Action	
− 10.0.0.0/8		10/8 private network	IT Internal	✎	🗑
10.2.0.0/22		OT range	OT Internal	✎	🗑
10.4.0.0/22		External IP within IP range	External	✎	🗑

Here, the user specified that the IP range 10.2.0.0/22 is OT internal and that 10.4.0.0/22 is external.

Thus, flow storage can be specifly set in the Ingestion configuration, on page 13 for the IP range set here as OT internal, whereas flows and devices from the IP range set as external will be excluded from the database and the license device count and risk score.

Note   It is also possible to organize subnetworks through the API.

Define a subnetwork

To define a subnetwork:

Step 1   In Cisco Cyber Vision, navigate to Admin > Network organization.

Step 2   Click the **Add a network** button.

The Edit a network window pops up:

ADD A NEW NETWORK   ✕

IP address / subnet   VLAN ID (optional)

10.0.0.0/8

Network name

10/8 private network

Network Type

OT Internal

Device engine options for this network range

☐ This IP range is deployed several time, the device engine will not use IP to group components into device.

☐ Do not group component seen by different sensors. For this IP range, the device engine will only use components from one sensor to create devices.

Cancel   Add a network

Step 3   Enter an IP address range and its subnet.

Step 4   If possible, add a VLAN ID.

This will allow you to create overlapping networks.

Step 5   Give the network a name.

Step 6   Set the network type as OT internal, IT internal or External.

Note Setting the network type can impact Cisco Cyber Vision's performances by setting flows storage, devices' risk score and the license's device count.

Step 7 If applicable, tick the first option.

Note Enable this option in case several devices share the same IP across the monitored network.

The components won't be grouped by IP.

Step 8 If applicable, tick the second option.

Note Enable this option in case same addressing parameters are used within different subnetworks. For example in case of identical production lines.

For that particular network range, the system will not aggregate components with components with same IPs detected by sensors monitoring other subnetworks. The system will aggregate the components into devices when subnetworks monitored are using the same IP ranges for several machines or production lines.

In this case, for a specific IP range, a component with an IP of that range seen by a sensor will be grouped with a component with the same IP only if components were detected by the same sensor.

Step 9 Click **Save**.

C H A P T E R **4**

Sensors

Sensor Explorer

The Sensor Explorer page allows you to install, manage, and obtain information about the sensors monitoring your industrial network.

First, you need to know that sensors can be used in two modes, and for different purposes:

- Online mode: A sensor in online mode is placed at a particular and strategic point of the industrial network and will continually capture traffic.

  Applicable to: Cisco IE3400, IE3300 10G, Cisco IC3000, Catalyst 9300 and Cisco IR1101.

• Offline mode: A sensor in offline mode allows you to easily connect it at different points of the industrial network that may be isolated or difficult to access to occasionally make traffic captures. Traffic is captured on a USB drive. The file will then be imported in Cisco Cyber Vision.

Only applicable to Cisco IC3000.

On the Sensor Explorer page, you will see a list of your folders and sensors (when installed) and buttons that will allow you to perform several actions.

Installation modes, features, and information will be available depending on the sensor model and the mode in which it's being used.

Additional information and actions are available as you click a sensor in the list. A right side panel will appear allowing you to see this information such as the serial number, and buttons to perform other actions.

Filter and sort the sensor list

Filtering

Clicking the Filter button allows you to filter the folders and sensors in the list by label, IP address, version, location, health and processing status.

The folders and sensors list without filtering:

Folders and sensors (5)

	Label ▲	IP Address	Version	Location	Health status ⓘ	Processing status ⓘ
☐	📁 FOLDER1			Lyon		
☐	📁 FOLDER2			Paris		
☐	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
☐	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing
☐	FCY014567	192.168.49.41			Disconnected	Disconnected

(Filter   0 Selected   Move selection to   More Actions ∨   As o)

Type in the field or select from the drop down menu to reach the folder(s) or sensor(s) and click the Apply button:

The folders and sensors list after filtering by label:

Sorting

Sort icons allow you to sort sensors by label, IP address, version, location, health and processing status by alphabetical or by ascending/descending order. Sort icons appear when applied or as you hover over them.

Folders and sensors (5)

▽ Filter   0 Selected   Move selection to   More Actions ∨

☐	Label ▾	IP Address ▴	Version	Location	Health status ⓘ	Processing status ⓘ
☐	📁 FOLDER2			Paris		
☐	📁 FOLDER1			Lyon		
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data

Sensors status

There are two types of sensor status:

- The health status, which indicates at which step of the enrollment process the sensor is.

- The processing status, which indicates the network connection state between the sensor and the Center.

☐	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ	Active Discovery	Uptime
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected	Disabled	N/A
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data	Enabled	3 days
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	6 hours

Health status:

- **New**

  This is the sensor's first status when it is detected by the Center. The sensor is asking the DHCP server for an IP address.

- **Request Pending**

  The sensor has asked the Center for a certificate and is waiting for the authorization to be enrolled.

- **Authorized**

  The sensor has just been authorized by the Admin or the Product user. The sensor remains as "Authorized" for only a few seconds before displaying as "Enrolled".

- **Enrolled**

  The sensor has successfully connected with the Center. It has a certificate and a private key.

- **Disconnected**

The sensor is enrolled but isn't connected to the Center. The sensor may be shut down, encountering a problem, or there is a problem on the network.

Processing status:

- **Disconnected**

  The sensor is enrolled but isn't connected to the Center. The sensor may be shut down, encountering a problem, or there is a problem on the network.

- **Not enrolled**

  The sensor is not enrolled. The health status is New or Request Pending. The user must enroll the sensor for it to operate.

- **Normally processing**

  The sensor is connected to the Center. Data are being sent and processed by the Center.

- **Waiting for data**

  The sensor is connected to the Center. The Center has treated all data sent by the sensor and is waiting for more data.

- **Pending data**

  The sensor is connected to the Center. The sensor is trying to send data to the Center but the Center is busy with other data treatment.

Sensors features

You will find in the Sensor Explorer page several features to manage and use your sensors. Some buttons are accessible from the Sensor Explorer page itself to manage one or more sensors. Other buttons are available when clicking a sensor in the list. A right side panel opens with additional sensor information and actions that are available or not depending on the sensor model, mode (online or offline) and the installation type performed.

FCH2309Y01Z   ✕

Label: FCH2309Y01Z ✎
Serial Number: FCH2309Y01Z
IP address: 192.168.49.23
Version: 4.1.0+202202151504
System date: Feb 16, 2022 10:07:45 AM
Deployment: Sensor Management Extension
Active Discovery: Disabled
Capture mode: All

System Health
Status: Connected
Processing status: Pending data
Uptime: 7 minutes

⌇ Go to statistics

▷ Start Recording

Last recording: Feb 10, 2022 3:36:54 PM
↓ Download (49 bytes)

🗁 Move to

↓ Download package   ✎ Capture mode

⟲ Redeploy   ◯ Enable IDS

⟳ Reboot   ⏻ Shutdown

⊖ Uninstall

- The **Start recording** button records a traffic capture on the sensor. Records can be used for traffic analysis and may be requested by Cisco support in case of malfunctions. You can download the recording clicking the link below.

✎

Note   This feature is targeted for short captures only. Performing long captures may cause the sensor overload and packets loss.

- The **Move to** button is to move the sensor through different folders. For more information, refer to Organize sensors, on page 34.

- The **Download package** button provides a configuration file to be deployed on the sensor when installing the sensor manually (online mode). Only applicable to the Cisco IC3000. Refer to its Installation Guide.

- The **Capture Mode** button can be used to set a filter on a sensor sending data to the Center. Refer to the procedure for Set a capture mode.

- The **Redeploy** button can be used to partly reconfigure the sensor, for example to change its parameters such as its IP address.

- The **Enable IDS** button can be used to enable the SNORT engine embedded in some sensors to analyze traffic by using SNORT rules. SNORT rules management is available on the SNORT administration page.

- The **Reboot** button can be used to reboot the sensor in case of a malfunction.

- The **Shutdown** button triggers a clean shutdown of the sensor from the GUI.

Note After performing a shutdown, you must switch the sensor ON directly and manually on the hardware.

- The **Uninstall** button can be used to remove an uninstalled sensor from the list or to fully uninstall a sensor. Diverse options are available according to the sensor model or deployment mode. In the case of a sensor deployed through the management extension, the IOx app can be removed from the device, whereas a reset to factory defaults can be performed in other cases. In any case, the sensor will be removed from the Center.

Install sensor

From the Sensor Explorer page, you can:

- Install a sensor manually.

- Install a sensor via the IOx extension. To use the Install via extension button you must first install the sensor management extension via the Extensions page.

- Capture traffic with an offline sensor (only applicable to Cisco IC3000).

For more information about how to install a sensor, refer to the corresponding Sensor Installation Guide.

Sensor Self Update

Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.1 provides the necessary foundation for sensor self-updates. However, the self-update feature will only be functional in future releases.

Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- • Select sensors to update.

- • The Center adds a new job to the sensor queue.

- • The sensor automatically collects and validates the update file.

- • The sensor restarts with the new version.

Update Warnings

In the Cisco Cyber Vision center on the Sensor Explorer page (Admin – Sensors – Sensor Explorer), users receive an alert to update the sensor. When this happens, the version number turns red, and a blue arrow with a tooltip indicates the sensor is upgradeable.

On the sensor's right-side, the same blue arrow and an **Update** button is visible.

Update Procedure

Step 1   Use the checkboxes on the left to select multiple sensors.

Step 2   Go to the **More Actions** and click **Update sensors**.

The sensor self-update menu appears.

Step 3 Click **OK**.

Step 4 During the update, a blue circle appears in the **Update status** column.

Step 5   After the update, the version number turns black, and a green symbol appears in the **Update status** column.

Step 6 The **Update in progress** status is visible.

Update Failure

If the update is unsuccessful, the **Update status** column displays a red cross and a message that provides the details.

Manage credentials

The Manage credentials button, which you can have access by clicking Manage Cisco devices in the Sensor Explorer page, is to register your global credentials if configured before in the Local Manager.
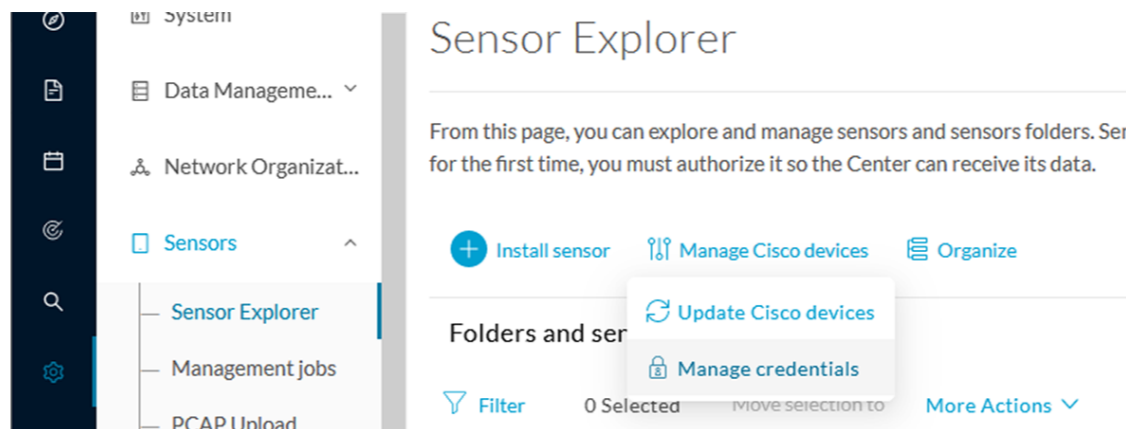
This feature can be used to register your global credentials in Cisco Cyber Vision. This will allow you to enter these credentials only once and they will be used when performing actions that require these credentials, that is installing and updating sensors via the IOx extension.

Only one set of global credentials can be used per Cisco Cyber Vision instance, which means that you cannot have several set of sensors accessible by different global credentials in a single instance. If there are several sensor administrators, they must use the same global credentials registered in Cisco Cyber Vision. However, you can have a set of sensors using a single global credentials and other sensors with their own single credentials.

Global credentials are stored in Cisco Cyber Vision but are set at the switch level in the Local Manager. Consequently, if you lose your global credentials, you must refer to the switch customer support and documentation.

The Manage credentials button can be used the first time you register your global credentials and each time global credentials are changed in the Local Manager. To do so, enter the login and password and click Save.

Once the global credentials are registered, the feature will be enabled in the Install via extension procedure. Select the Use global credentials option to use your global credentials.
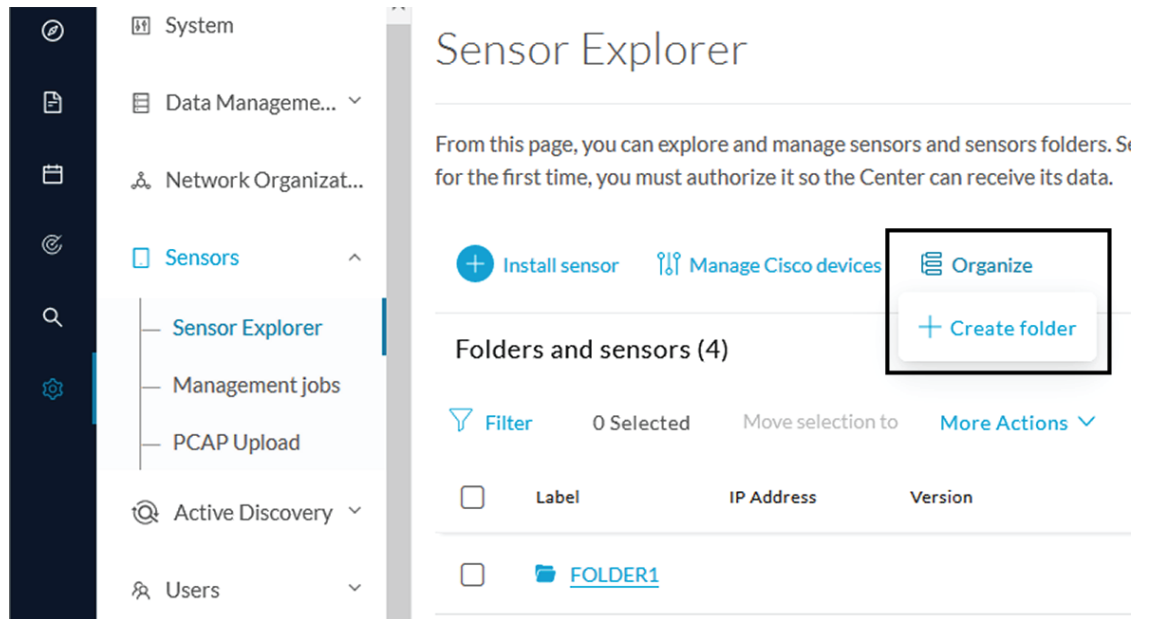
Organize sensors

You can create folders and move your sensors into the folders for more clarity. Folders can correspond to a location, a person in charge, a set of disconnected sensors, etc.
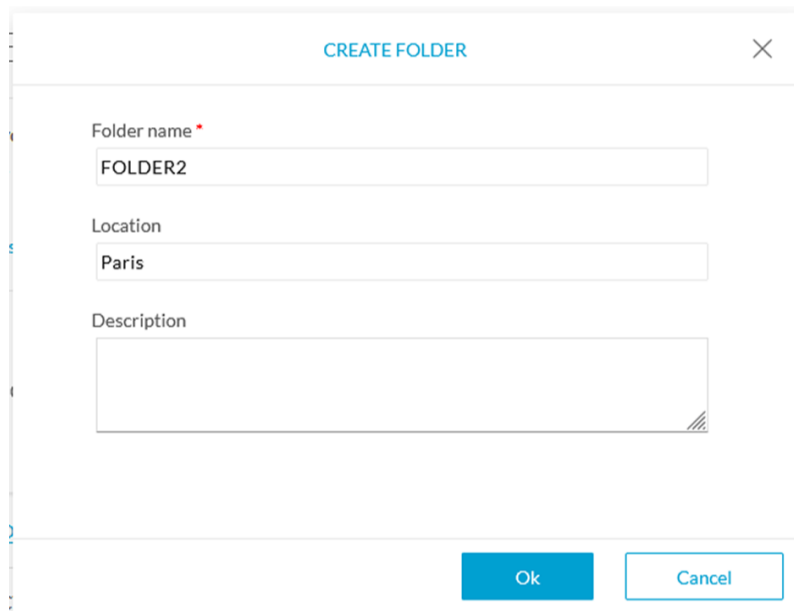
To create a folder and move a sensor in it:

1. Click the Organize button and click Create folder.

2. Write a folder name, and, if needed, a location and a description.

The new folder is displayed in the sensor list.

Folders and sensors (5)

	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
☐	📁 FOLDER1			Lyon		
☐	📁 FOLDER2			Paris		
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

3. Select a sensor in the list and click the button Move selection to.

Folders and sensors (5)

	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
☐	📁 FOLDER1			Lyon		
☐	📁 FOLDER2			Paris		
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected
☑	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

4. Select the folder you want to place the sensor in or create a new folder. Root can be used to move sensors back into the primary list.
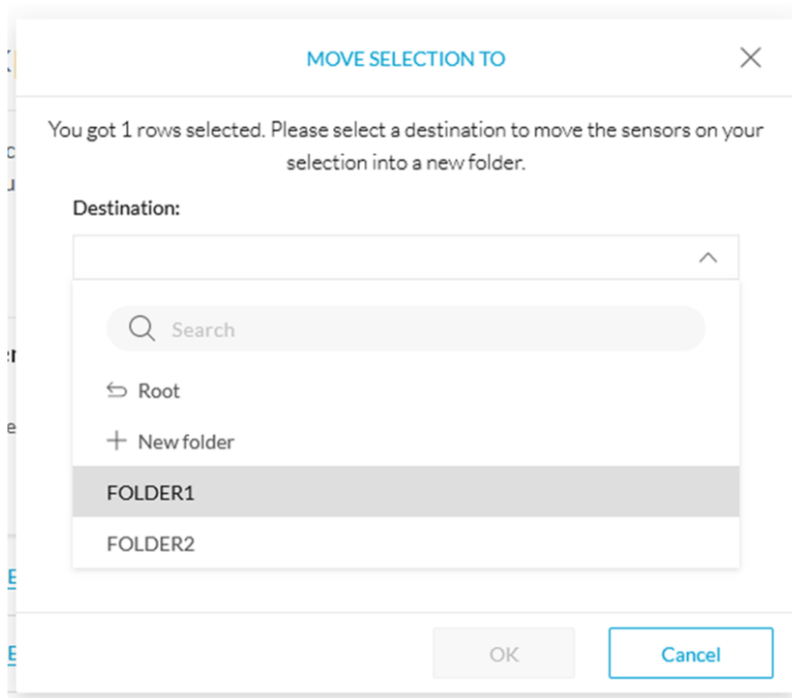
The sensor is moved into the folder. The sensor version, health status and processing status are displayed in the folder line.

If you move a sensor in a disconnected state inside this same folder, then its information will be displayed in the folder line rather than the sensor in connected state. Less secure sensor status are showcased in priority to drag your attention.

Folders and sensors (3)

▽ Filter   0 Selected   Move selection to   More Actions ⌄

	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
☐	📁 FOLDER1		– 4.1.0	Lyon	Disconnected	Disconnected
☐	📁 FOLDER2			Paris		
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data

The sensors inside a folder:

FOLDER1

◇ Lyon

✎ Edit   🗑 Delete

Folders and sensors (2)

▽ Filter   0 Selected   Move selection to   More Actions ⌄

	Label	IP Address	Version	Health status ⓘ ▾	Processing status ⓘ
☐	▭ FCY014567	192.168.49.41		Disconnected	Disconnected
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504	Connected	Pending data

Set a capture mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. You can set it by clicking an online sensor in the sensors list of the Sensor Explorer page or during a sensor installation.

Setting the capture mode on a sensor from the right side panel:

Capture modes:

The aim is mainly to focus the monitoring on relevant traffic but also to reduce the load on the Center.

For example, a common filter in a firewall can consist of removing the network management flows (SNMP). This can be done by setting a filter like "not (port 161 and host 10.10.10.10)" where "10.10.10.10" is the network management platform.

Using Capture mode Cisco Cyber Vision performance can be improved on large networks.

Capture modes operate because of filters applied on each sensor. Filters are set to define which types of incoming packets are to be analyzed by the sensors. You can set a different filter on each sensor according to your needs.

You can set the capture mode in the installation wizard when enrolling the sensors during the Center installation. This option is recommended if you already know which filter to set. Otherwise, you can change it at any time through the Sensor Explorer page in the GUI (provided that the SSH connection is allowed from the Center to the sensors).

Note
You can set a capture mode to offline sensors from a file containing the filter and registered on the USB drive. This will be then plugged on the Offline USB port of the device. For more information about setting a capture mode on an offline sensor contact the support.

The different capture modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.

- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.

- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.

- CUSTOM (advanced users): Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.

Deployment tokens

Zero Touch Provisioning allows you to automate Cisco Cyber Vision deployment on sensor batches. It is to be used with third-party tools such as Cisco Catalyst WAN Manager. Refer to its documentation on cisco.com to complete sensor deployment.

From this page, you can create, edit, enable, disable and delete deployment tokens for Zero Touch Provisioning.
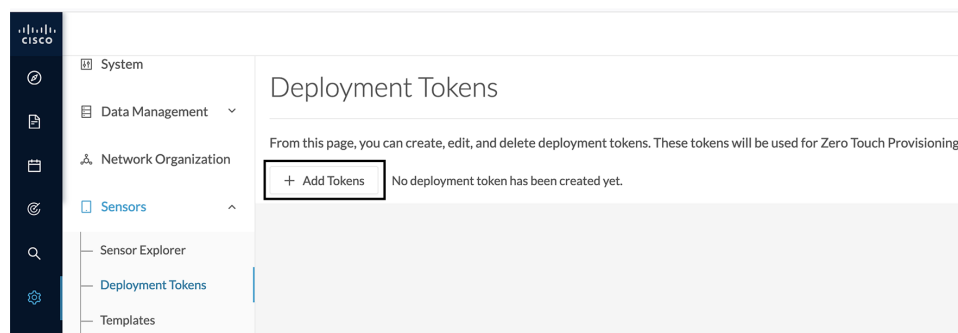
You will start with adding a deployment phase, that is a group of tokens, with a number of uses and an expiration time.

The application will request a token valid for an application type. A token contains the application name and a PSK (pre-shared key).

Once proper configuration is done on Cisco Catalyst WAN Manager, it will deploy the sensors and apply parameters which will allow each sensor to on-board itself on the Center.

Communication between the sensors and the Center will start after sensors have presented the PSK to the Center and the Center has delivered all necessary information for enrolment.

Deployment will fail:

- if the number of sensors exceed the number of tokens.

- if the deployment occurs after the expiration time.

If so, you can edit the deployment phase to modify the number of uses accordingly and extend the expiration time.

Table 1: Sensor applicability and correspondance table per deployment file

Sensors	Deployment files
IE3x00, IR1101, IR18xx, IE9300	cviox-aarch64.tar
IE3x00, IR1101, IR18xx, IE9300 **with Active Discovert**	cviox-active-discovery-aarch64.tar
IC3000	cviox-ic3000-x86-64.tar
IC3000 **with Active Discovery**	cviox-active-discovery-x86-64.tar
Catalyst 9300, 9400, IR8340	cviox-x86-64.tar
Catalyst 9300, 9400, IR8340 **with Active Discovery**	cviox-active-discovery-x86-64.tar

Create tokens

To create tokens for sensor Zero Touch Provisioning:

Step 1   Click **Add Tokens**.
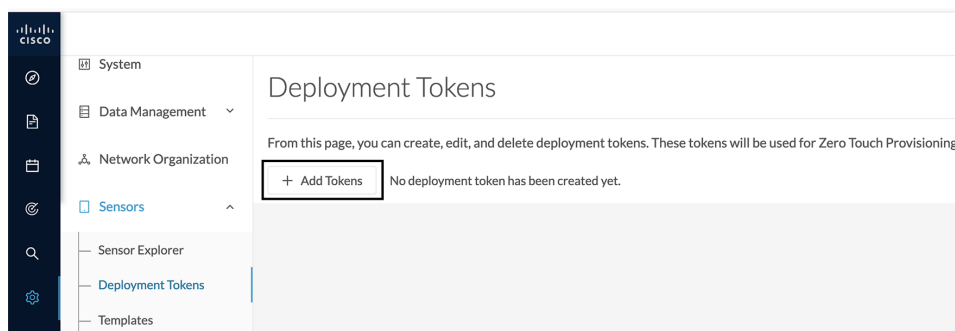
Step 2   In the Add new deployment tokens:

Add new deployment tokens ✕

* Name : Phase 1

* Number of uses : 25

* Expiration time : 2024-07-31

Enabled :

Cancel   Create

a)   Add a name to the deployment phase.
b)   Add a number of uses for the number of devices to be deployed.
c)   Set the tokens expiration time.
d)   You can enable the token to continue the deployment process.

Step 3   Click **Create**.

The deployment phase with tokens per device type appears.

⚠ The tokens will be updated each time the center is updated

Name	Tokens		Status	Creation Date	Expiration Date	Usages	Last deployment	Actions
	Image	Token						
	cviox-aarch64.tar	Show 🗍						
	cviox-active-discovery-aarch64.tar	Show 🗍						
Phase 1	cviox-active-discovery-ic3000-x86-64.tar	Show 🗍	Enabled	Jul 2, 2024	Jul 31, 2024	0/25		✎ ⊘ 🗑
	cviox-active-discovery-x86-64.tar	Show 🗍						
	cviox-ic3000-x86-64.tar	Show 🗍						
	cviox-x86-64.tar	Show 🗍						

Different buttons are available to see the tokens and copy them or edit, disable or delete the deployment phase.

| Phase 1 | cviox-active-discovery-ic3000-x86-64.tar | Show | Enabled | Jul 2, 2024 | Jul 31, 2024 | 0/25 | |

What to do next

Refer to Cisco Catalyst WAN Manager documentation in cisco.com to continue and complete sensor deployment.

Templates

This page allows you to create and set templates with protocol configurations and assign them to specific sensors.

Sensor templates contain protocol configurations which allow you:

- To enable or disable protocol DPI (Deep Packet Inspection) engines.

- To map UDP and TCP ports for each protocol's packet received by the sensor.

By enabling/disabling a protocol DPI engine you can decide which protocols will be analyzed.

Disabling a protocol DPI engine avoid false positives in Cisco Cyber Vision, that is when a protocol appears on the user interface when it's actually not the case because same UDP/TCP ports can be used by other non-standardized protocols.

Some protocols are disabled in the Default template because they are not commonly used or used in specific fields such as transportation. The Default template is applied on all compatible sensors.

As previously mentioned, UDP/TCP ports default configurations are mostly standardized, but conflicts still exist among field-specific protocols or with limited usage. Mapping UDP/TCP port numbers will allow packets to be sent to the correct DPI engine so they can be accurately analyzed and correctly represented in the user interface.

If the protocol's packet is sent to the wrong port, related information will end up in Security Insights/Flows with no tag.

A sensor can be associated with a single template only. Deployment of the template can fail:

- if the sensor is disconnected,

- if there is connection issues,

- if the sensor version is too old.

Create templates

Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Templates.

Step 2 Click **Add sensor template**.
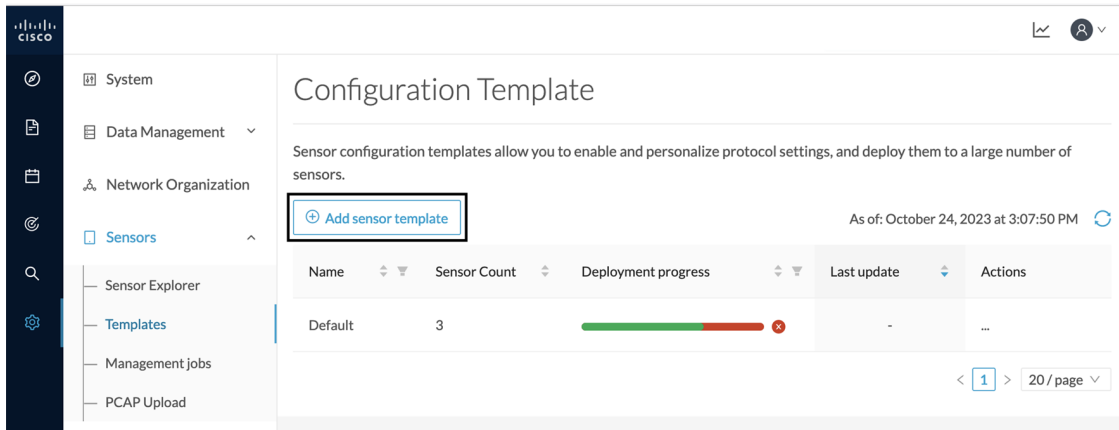
The Create sensor template window pops up.

Step 3   Add a name to the template. You can also add a description.

Step 4   Click **Next**.

The list of protocol DPI engines with their basic configurations appears.
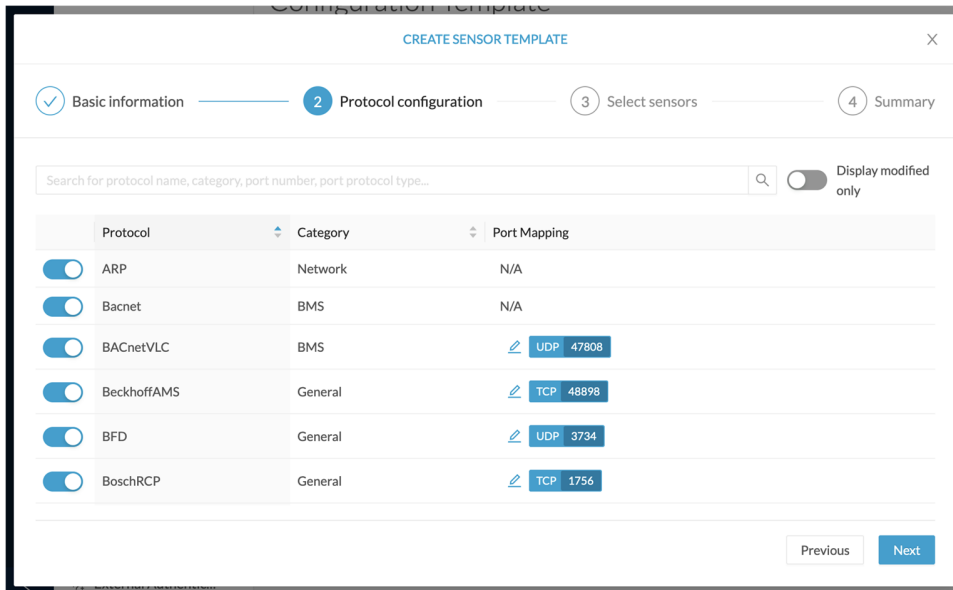
Step 5   In the search bar, type the protocol you want to configure.

In our example, we will add a port to the OPCUA default settings.
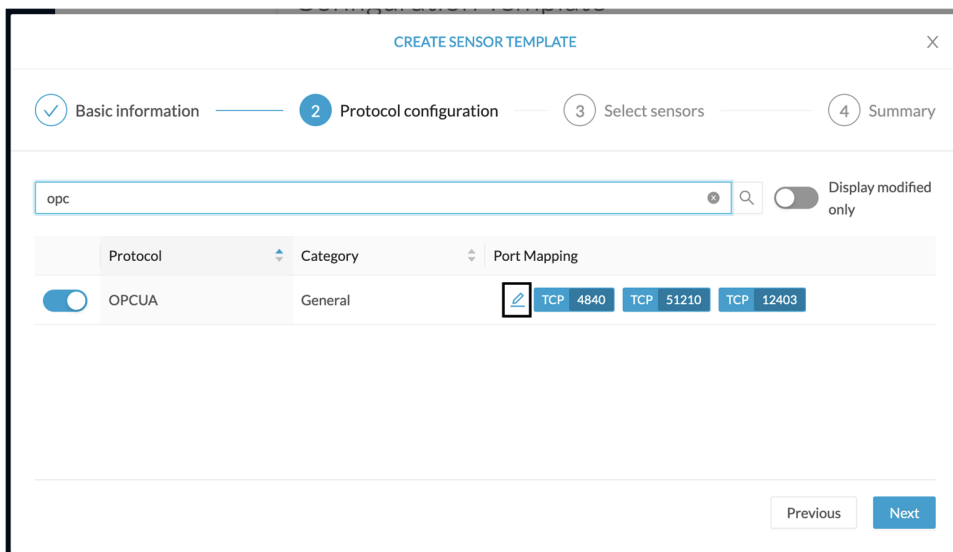
Step 6   Under the Port Mapping column, click the **pen** button to edit its settings.

The protocol's port mapping window pops up.

Step 7   Write down the port number you want to add and hit enter.

Step 8   Click **OK**.

The port number is added to the protocol's default settings.

Toggling ON the **Displayed modified only** button allows you to quickly find this protocol.

Step 9   Click **Next**.

Step 10   Select the sensor(s) you want to apply the template to.

Step 11   Click **Next**.

Step 12   Check the template configurations and **Confirm** its creation.

The configuration is sent to the sensors. Configuration deployment will take a few moments.

The OPCUA template appears in the template list with its two assigned sensors.

Configuration Template

Sensor configuration templates allow you to enable and personalize protocol settings, and deploy them to a large number of sensors.

⊕ Add sensor template   As of: October 24, 2023 at 3:06:55 PM ↻

Name	Sensor Count	Deployment progress	Last update	Actions
Default	1	⊗	-	...
OPCUA	2	✓	Today	...

< 1 >   20 / page ⌄

Management jobs

As some deployment tasks on sensors can take several minutes, this page shows the jobs execution status and advancement for each sensor deployed with the sensor management extension.

This page is only visible when the sensor management extension is installed in Cisco Cyber Vision.

You will find the following jobs:

• Single deployment

This job is launched when clicking the Deploy Cisco device button in the sensor administration page, that is when a new IOx sensor is deployed.

- Single redeployment

This job is launched when clicking the Reconfigure Redeploy button in the sensor administration page, that is when deploying on a sensor that has already been deployed. This option is used for example to change the sensor's parameters like enabling active discovery.

- Single removal

This job is launched when clicking the Remove button from the sensor administration page.

- Update all devices

This job is launched when clicking the Update Cisco devices button from the sensor administration page. A unique job is created for all managed sensors that are being updated.

If a job fails, you can click on the error icon to view detailed logs.

PCAP Upload

This page allows you to upload pcaps to view their data in Cisco Cyber Vision.

When selecting a pcap, two options are available:

- You can choose to use the timestamp of the pcap or the current timestamp instead. Choosing the current timestamp can be useful if the pcap timestamp is old and searching for its data in Cisco Cyber Vision is thus easier.

- You can define a preset from the pcap. Once the pcap is uploaded you'll just have to click the pcap link to be redirected to its preset.
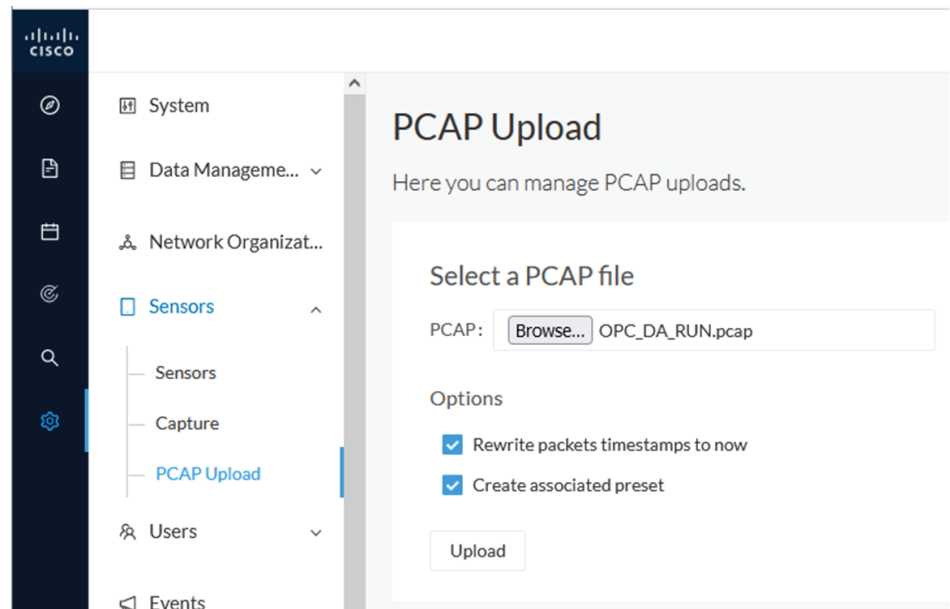
Note that during the upload that the status for the DPI and Snort are displayed.

If uploading a large file, you have the possibility to pause it. To relaunch the upload, you just need to select the same pcap again with the browse button and click Resume.

Note pcap data cannot be erased individually from Cisco Cyber Vision. You will need to use the Clear data button and it will affect the whole database. Upload pcaps with caution.

C H A P T E R 5

Active Discovery

- Active Discovery policies, on page 51

Active Discovery policies

Active Discovery is used to allow a sensor to send packets to the network to discover previously unseen devices and gather additional properties for known devices.

Active Discovery operates in Broadcast and Unicast, and responses received will be analyzed by Cisco Cyber Vision.

An Active Discovery policy is a list of settings which define protocols and their parameters that will be used to scan the industrial network. The policy will be used in a preset and be applied on a list of sensors and components.

For more information, refer to the Cisco Cyber Vision Active Discovery Configuration Guide.

CHAPTER **6**

Users

Management

You can create, edit and delete users through the users administration page.
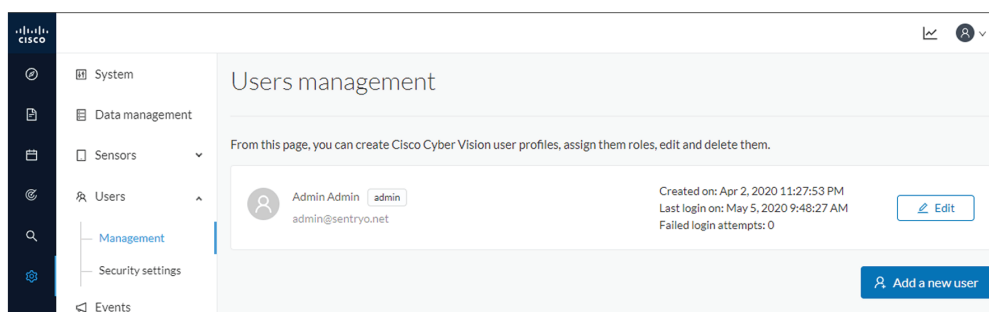
During their creation each user must be assigned with one of the following user roles (from full rights to read-only) or with a custom role (refer to Role Management).

- **Admin**

  The Admin user has full rights on the Cisco Cyber Vision platform. Users who have this role assigned oversee all sensitive actions like user rights management, system updates, syslog configuration, reset and capture modes configuration on sensors.

- **Product**

  The product user has access to several features of the system administration page (i.e. the system, sensors and events administration pages). This access level is for users who manage sensors from a remote location. In addition, they can manage the severity of events and, if enabled by the Admin user, can manage their export to syslog.

- **Operator**

This access level is for users who use the Monitor mode and manage groups but do not have to work with the platform administration. Thus, the Operator user has access to all pages, except the system administration page.

- **Auditor**

This access level provides read-only access to the Explore, Reports, Events and Search pages. Auditors can use sorting features (such as search bars and filters) that do not require persistent changes to the Cisco Cyber Vision data (unlike Autolayout), and generate reports.

You can create as many users as needed with any user rights. Thus, several administrators can use and administrate the whole platform.

However, each user must have their own account. That is:

- Accounts must be nominative.

- One email address for several accounts is not allowed (note that email will be requested for login access).

  Passwords must contain at least 6 characters and comply with the rules below. Passwords:

    - Must contain a lower case character: a-z.

    - Must contain an upper case character: A-Z.

    - Must contain a numeric character: 0-9.

    - Cannot contain the user id.

    - Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

> 👉
>
> | **Important** | Passwords should be changed regularly to ensure the platform and the industrial network security. |

Passwords' lifetime is defined in the Security settings.

You can create custom user roles in the Role Management.

You can map Cisco Cyber Vision user roles with an external directory's user groups in the LDAP settings page.

Role Management

In addition to the four Cisco Cyber Vision default roles (i.e. Admin, Auditor, Operator and Product), customized roles can be created and modified from the Role management page.

These roles will help you defining specific privileges and accesses for each group of users.

Default roles cannot be edited or deleted.

You can map Cisco Cyber Vision custom roles with an external directory's user groups in the LDAP settings page.
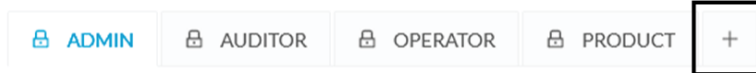
Create roles

This section explains how to create customized user roles on Cisco Cyber Vision. These can be later mapped to groups in Active Directory.

Step 1 In Cisco Cyber Vision, navigate to Admin > Users > Role Management.

Step 2 Click the + button next to default user roles.

Role management

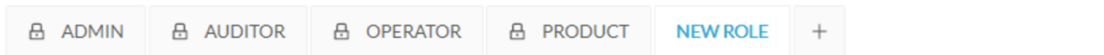From this page, you can create Cisco Cyber Vision user roles, edit and delete them.

🔒 ADMIN   🔒 AUDITOR   🔒 OPERATOR   🔒 PRODUCT   +

A new role tab appears.

Step 3 Type a role name and a description.

Role management

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.

🔒 ADMIN   🔒 AUDITOR   🔒 OPERATOR   🔒 PRODUCT   NEW ROLE   +

Role Name *

TestAD2019

Role Description *

TestAD2019

Search/Add existing permission: ⌄   ⊕ Add New Permissions

Step 4 Select an existing role from the Search/Add existing permissions drop down menu, or click the Add New Permissions button to build the new user role from scratch.
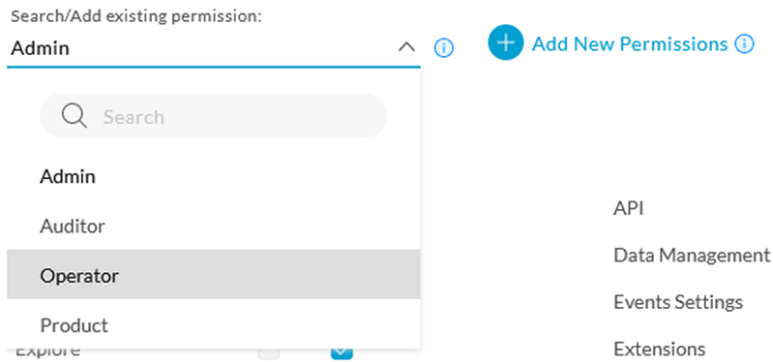
Step 5   Select/unselect permissions from the list as read or write
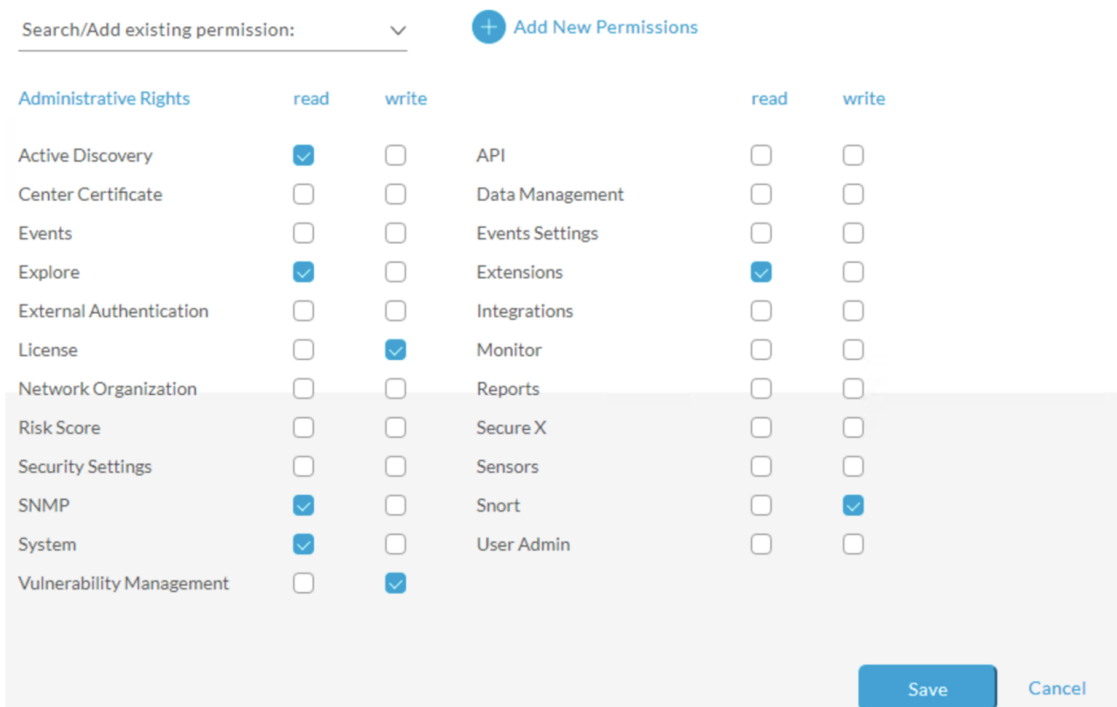
Step 6   Click save.

A message saying that the user role has been created successfully appears.

The new user role is displayed in the tab list.

You can modify or delete directly in the tab.

What to do next

Custom roles created can be mapped with an external directory's user groups in the LDAP settings page.

Security settings

From this page you can configure the security settings of users' password such as its lifetime, the number of authorized login attempts, the number of days before a password can be reused, etc.

Events

Events

The severity of events can be customized on the events administration page. By default, changes will be applied to future events only. However, you can apply new customized severities to past events by enabling Apply severity to existing events.

☞

Important	This action is irreversible and can take several minutes to complete.

You can reset the severity to default.

You can enable or disable the export of events to syslog and database storage. These two options are active by default. However, make sure Syslog configuration before the export.

CHAPTER **8**

API

Token

Cisco provides a REST API. To use it you first need to create a token through the API administration page.

A token is a random password which authenticates a request to Cisco Cyber Vision to access or even modify the data in the Center through the REST API. For instance, you can request the latest 10 components detected on Cisco Cyber Vision or create new references. Requests can be used by external applications like a SOC solution.

Note Best practice: create one token per application so you can remove or expire accesses separately.
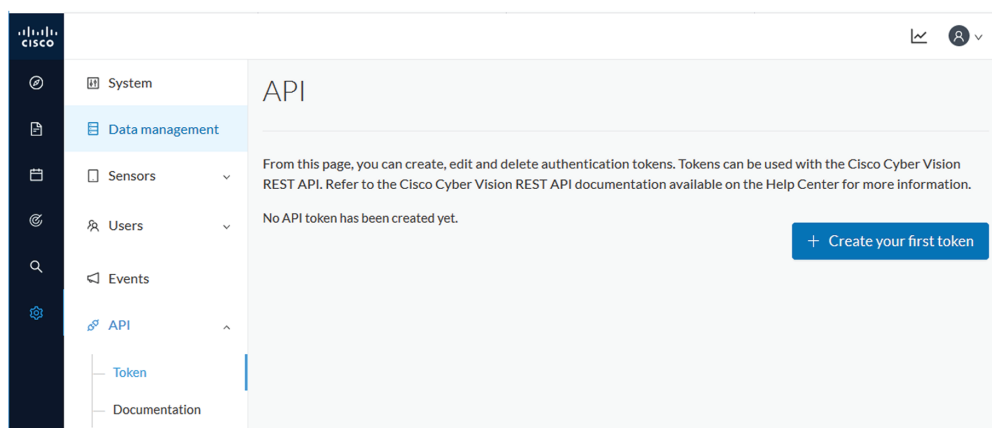
Create your first token and enter a name that will help you identifying the token. For security reasons you can also use the status toggle button to disable authorization to use the token (for example, if the token created is to be used later and you want to prevent access until then) and set an expiration time.

Once the token is created click show to see and copy the token to the clipboard.

For more information about the REST API refer to the REST API user documentation available on cisco.com.

Documentation

This page is a simplified API development feature. It contains an advanced API documentation with a list of all possible routes that can be used and, as you scroll down the page to Models, a list of possible data responses (data type, code values and meaning).

In addition to information research, this page allows you to perform basic tests and call the API by sending requests such as GET, DELETE and POST. You will get real results from the Center dataset. Specifications about routes are available such as the route's structure, and parameters and arguments that can be set. An URL is generated and curl can be used in a terminal as it is.

However, for an advanced use, you must create an application that will send requests to the API (refer to the REST API documentation).

☞

Important All routes other than GET will modify data on the Center. As some actions cannot be reversed, use DELETE, PATCH, POST, PUT with caution.

Routes are classified by Cisco Cyber Vision's elements type (activities, baselines, components, flows, groups, etc.).

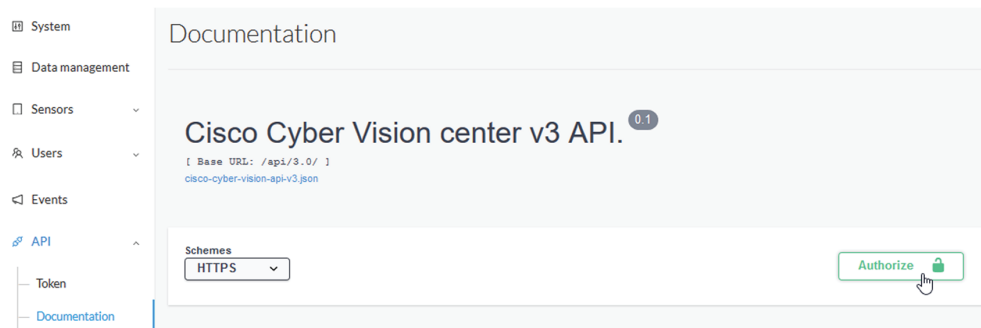*The category "Groups" containing all possible group routes:*

To authorize API communications:

Step 1   Access the API Token menu to create and/or copy a Token.

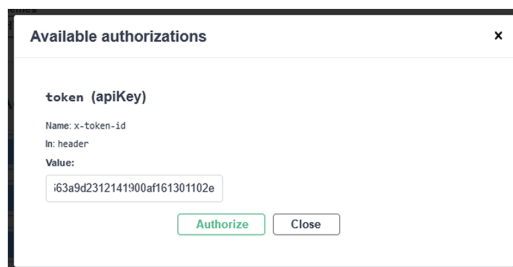Access the API Documentation page and click the Authorize button.
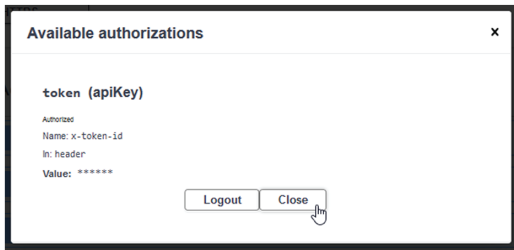

Step 2   Paste the token.

Step 3   Click Authorize.
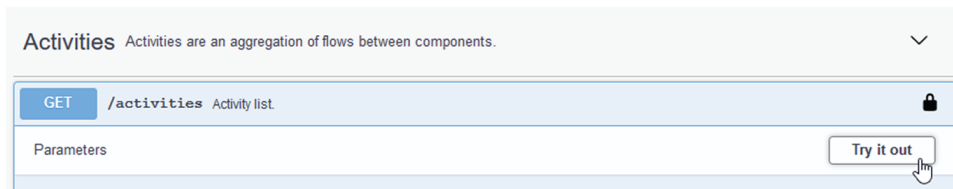

Step 4   Click Close.

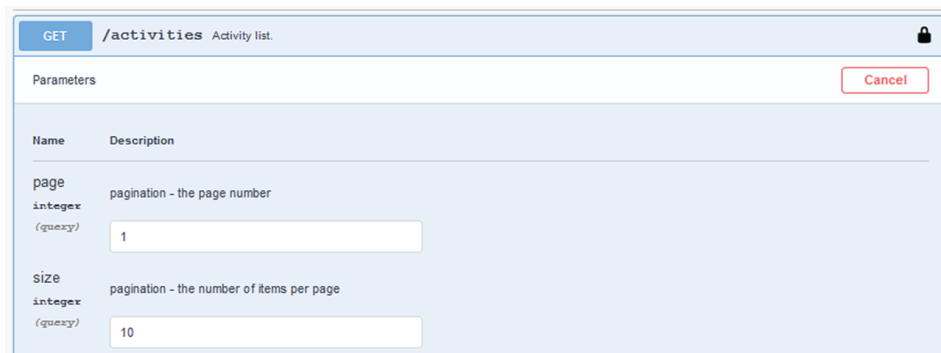Closed lockers displays. They indicate that routes are secured and authorization to use them is up.

To use a route:

Step 5   Click a route to deploy it. In the example, we choose Get activity list.

Step 6   Click Try it out.

Step 7   You can set some parameters. In the example, we set page to 1 and size to 10.

Step 8   Click Execute.

Note   You can only execute one route at a time.

A loading icon appears for a few moments. Responses display with curl, Request URL and the server response that you can copy or even download.

Step 9   When you're finished, click the Authorize button.

Step 10   Logout to clean the token variable, and click Close.

CHAPTER 9

License

- License, on page 69

License

You can install a license in Cisco Cyber Vision in the License administration panel.

Licensing is based on device count. For device count to be more accurate, it is advised to setup the subnetworks of the monitored industrial network through the Network organization page. By doing so, you will declare which subnetworks are internal, and which are external. Devices from external subnetworks will be excluded from the license count and related costs would be reduced.

For more information about how to install a license, refer to the Cisco Cyber Vision Smart Licensing User Guide available on cisco.com.

CHAPTER **10**

External Authentication

LDAP

Cisco Cyber Vision can delegate user authentication to external services using LDAP (Lightweight Directory Access Protocol), and in particular to Microsoft Active Directory services.

You can enable LDAP authentication in the LDAP Settings administration page.
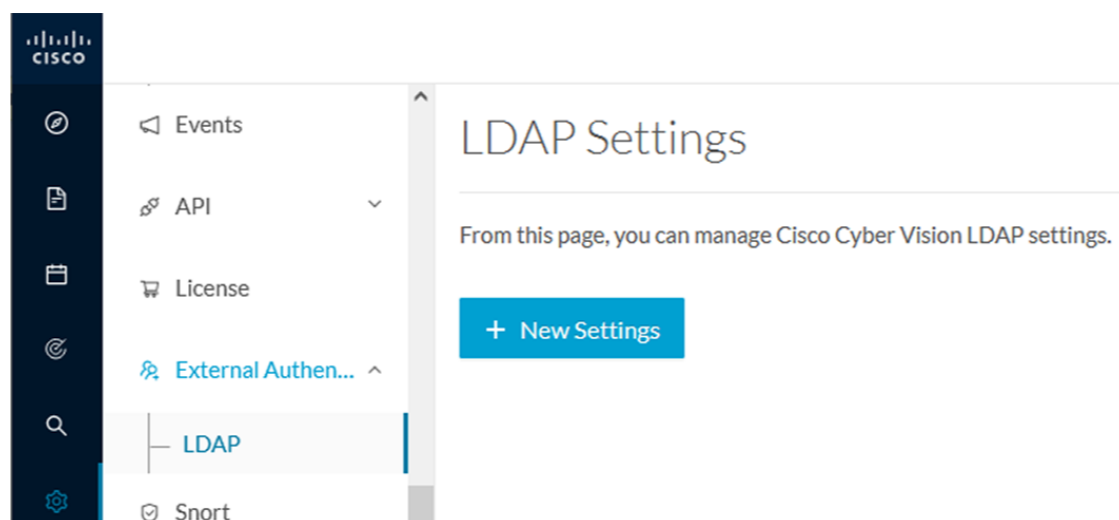
Configuring LDAP:

LDAP integration can be done through normal connection or securely by using certificates depending on the installation compatibility.

Mapping Cisco Cyber Vision roles with Microsoft Active Directory groups:

User groups available in the external directory can be mapped to Cisco Cyber Vision Product, Operator and Auditor user roles or custom roles. Refer to Role Management to create custom roles.

Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

Testing LDAP connection:

After setting up LDAP, the connection between the Cisco Cyber Vision Center and the external directory is to be tested. On the LDAP test connection window, you will use a user login and a password set in the external directory. The Center will attempt to authenticate on the directory server with these credentials. In return, you will get either a successful authentication, or a failed one with an error message.

Login in Cisco Cyber Vision:

When logging into Cisco Cyber Vision, the login format used will determine the base (i.e. internal or external) to be queried:

- If you use an email, the Cisco Cyber Vision database is queried.

- If you use the Active Directory format <domain_name>\<user_name> (e.g. cisco\john_doe), then the external directory is used to authenticate users.

Configure LDAP

This section explains how to configure LDAP in Cisco Cyber Vision using a normal connection or a secure connection.

Step 1 In Cisco Cyber Vision, navigate to Admin > External Authentication > LDAP.
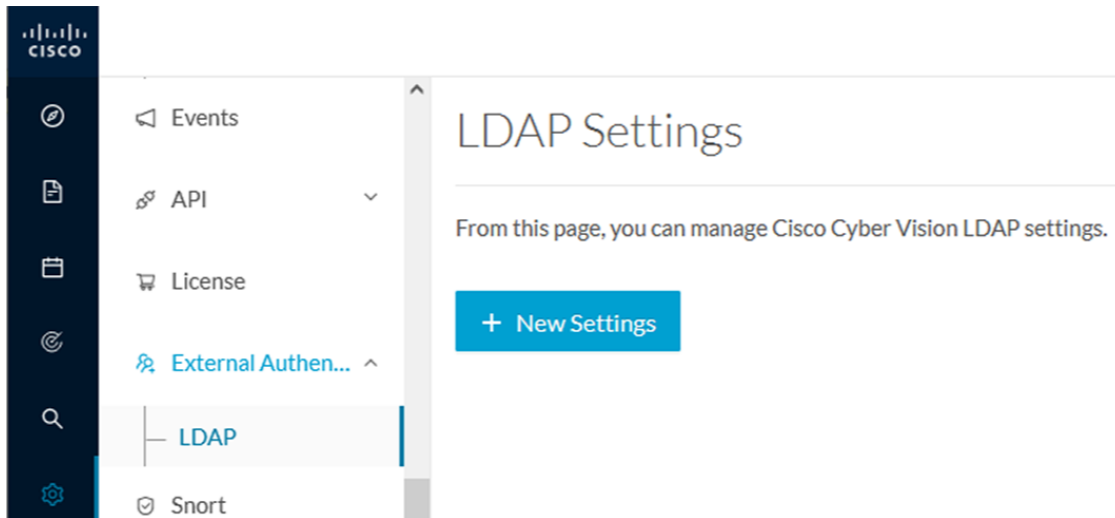
Step 2 Click New Settings.

The New LDAP Settings window pops up.

LDAP normal connection

After clicking the New Settings button, the following New LDAP Settings window pops up.

Before you begin

Step 1   Fill in the LDAP settings.

NEW LDAP SETTINGS   ✕

| Settings | Role Mapping |

☐ LDAP over TLS/SSL   ☐ Use self signed certificate

* Primary Server Address   * Primary Server Port

dc01.2019lab.local   389

Secondary Server Address   Secondary Server Port

dc01.2019lab.local   389

* Base DN ⓘ

DC=2019lab,DC=local

* Server Response Time ⓘ

10

OK   Cancel

Step 2   Click the Role Mapping tab.

Step 3   Fill in the following fields:

     a)   Map one or more Cisco Cyber Vision default roles with an Active Directory group.

        Note   At least one default role must be mapped.

        Note   Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

     b)   Map Cisco Cyber Vision custom roles with Active Directory groups.

        You must type the exact group names as configured into the remote directory so they can be retrieved and mapped to user roles.

Step 4   Click OK.

Step 5   Click the Test connection button.

The Test Connection window pops up.

TEST CONNECTION ✕

* Username

2019lab\user2019

* Password

••••••••• ⊘

✅ Successful LDAP bind

OK Cancel

Step 6 Enter a user credentials to test the connection between Cisco Cyber Vision and Active Directory.
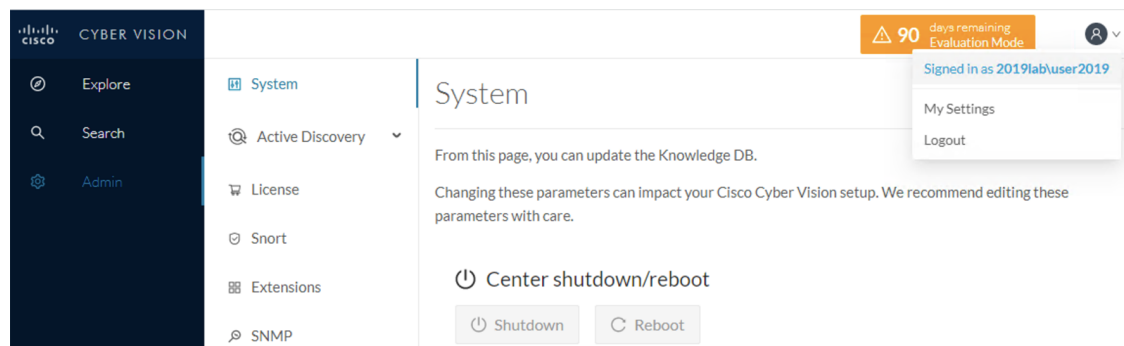
Note The Username format is domain\user.

A message Successful LDPA bind should appear.

Step 7 Click OK.

Step 8 Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

Menus are displayed according to the rights granted to the user.

What to do next

LDAP secure connection

After clicking the New Settings button, the following New LDAP Settings window pops up.

Before you begin

Step 1 Fill in the following fields:

a) Tick LDAP over TLS/SLL.

b) Fill in the LDAP settings.

c) Upload a .pem root certificate or a chain certificate, or tick Use a self-signed certificate.

If you upload a certificate, a message indicating that the certificate has been uploaded successfully appears.

The certificate appears at the bottom of the New LDAP Settings window.
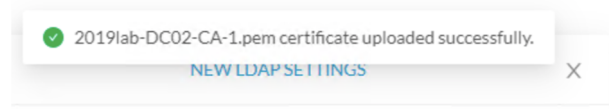
Step 2   Click OK.

Step 3   Click the Role Mapping tab.

Step 4   Fill in the following fields:

     a)   Map one or more Cisco Cyber Vision default roles with an Active Directory group.

         Note   At least one default role must be mapped.

         Note   Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

     b)   Map Cisco Cyber Vision custom roles with Active Directory groups.

         You must type the exact group names as configured into the remote directory so they can be retrieved and mapped to user roles.
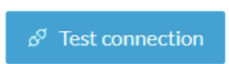
Step 5   Click OK.

Step 6   Click the Test connection button.

The Test Connection window pops up.

Step 7   Enter a user credentials to test the connection between Cisco Cyber Vision and Active Directory.

Note   The Username format is <domain_name>\<user_name> (e.g. cisco\john_doe).

A message Successful LDPA bind should appear.

Step 8   Click OK.

Step 9   Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

Menus are displayed according to the rights granted to the user.

CHAPTER **11**

Snort

Snort

Snort is a Network Intrusion Detection System (NIDS) software which detects malicious network behavior based on a rule matching engine and a set of rules characterizing malicious network activity. Cisco Cyber Vision can run the Snort engine on both the Center and some sensors. The Center stores the configuration rule files, pushes rules on compatible sensors, and intercepts Snort alerts to display them as events in the Cisco Cyber Vision's GUI.

Snort is not activated by default on sensors, so you must first Enable IDS on a sensor.

It is available on the following sensor devices:

- The Cisco IC3000 Industrial Compute Gateway

- The Cisco Catalyst 9300 Series Switches

- The Cisco IR8340 Integrated Services Router Rugged

It is also avaible on the Center DPI, and is enabled by default.

Snort Community Rules is set by default in Cisco Cyber Vision. You can enable Snort Subscriber Rules using the corresponding toggle button **(1)**. Note that this option requires the Advantage licensing and a specific IDS sensor license per enabled sensor.

Community ruleset

- The community ruleset is a Talos certified ruleset that is distributed freely. It includes rules that have been submitted by the open-source community or by Snort integrators. This ruleset is a subset of the full ruleset available to the subscriber users. It does not contain the latest Snort rules and does not ensure coverage of the latest threats.

Subscriber ruleset

- The subscriber ruleset includes all the rules released by the Talos Security Intelligence and Research Team. The ruleset ensures fast access to the latest rules and early coverage of exploits. Compared to the

Community ruleset, it contains more rules and remains in sync with the latest Talos research work on vulnerability detection.

In the Snort administration page, you can find Snort rules grouped into categories, and configure which set of rules to enable or not using the toggle status button **(2)**.

You can download each category rule file using the corresponding button **(3)**.
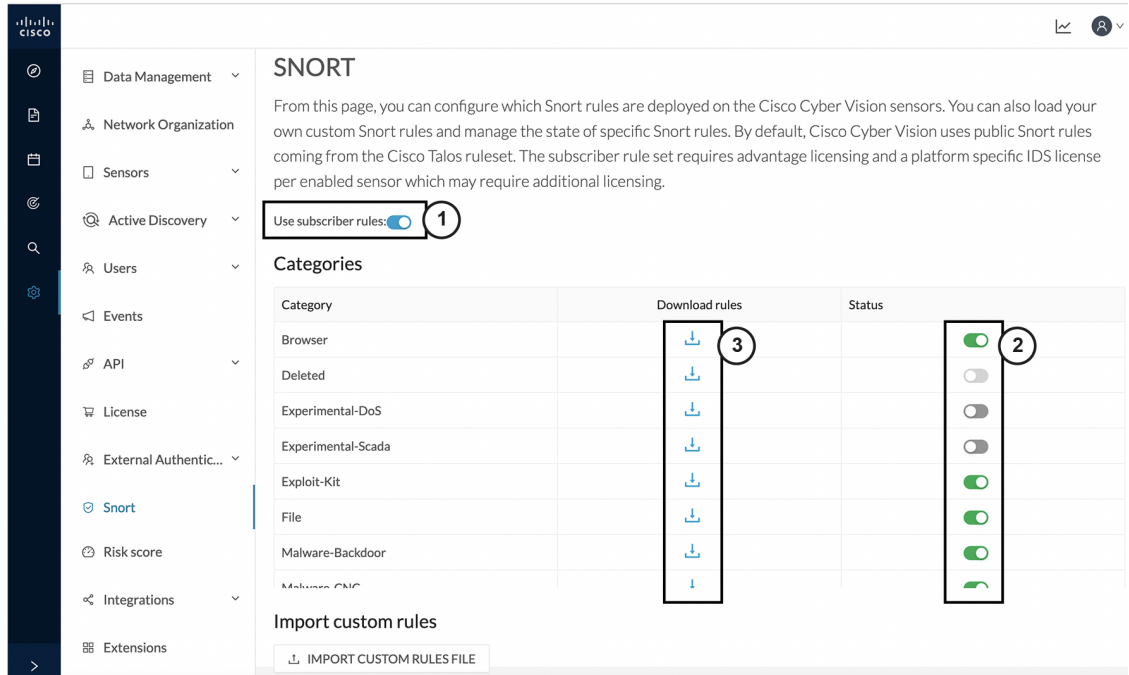
Note that some rules are **not** enabled inside these categories. So, using the toggle button on a category won't necessarily have an effect on their rules. The ones that are considered the most useful are enabled by default, others have been disabled to avoid performance issues. Consequently, if you want to enable these rules you need to use the Enable/disable a rule.

It is also possible to enable/disable a specific rule from a custom rule file.

Snort rules categories:

- Browser:

    Rules for vulnerabilities present in several browsers including, but not restricted to, Chrome, Firefox, Internet Explorer and Webkit. This category also covers vulnerabilities related to browser plugins such as Active-x.

- Deleted:

    When a rule has been deprecated or replaced it is moved to this category.

- Experimental-DoS:

    Rules developed by the Cisco CyberVision team for various kinds of DoS activities (TCP SYN flooding, DNS/HTTP flooding, LOIC, etc.).

- Experimental-Scada:

    Rules developed by the Cisco CyberVision team for attacks against industrial control system assets.

- Exploit-Kit:

Rules that are specifically tailored to detect exploit kit activity.

- File:

Rules for vulnerabilities found in numerous types of files including, but not restricted to, executable files, Microsoft Office files, flash files, image files, Java files, multimedia files and pdf files.

- Malware-Backdoor:

Rules for the detection of traffic destined to known listening backdoor command channels.

- Malware-CNC:

Known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

- Malware-Other:

Rules that deal with tools that can be considered malicious in nature as well as other malware-related rules.

- Misc:

Rules that do not fit in any other categories such as indicator rules (compromise, scan, obfuscation, etc.), protocol-related rules, policy violation rules (spam, social media, etc.), and rules for the detection of potentially unwanted applications (p2p, toolbars, etc.).

- OS-Other:

Rules that are looking for vulnerabilites in various operating systems such as Linux based OSes, Mobile based OSes, Solaris based OSes and others.

- OS-Windows

Rules that are looking for vulnerabilities in Windows based OSes.

- Server-Other:

Rules dealing with vulnerabilities found in numerous types of servers including, but not restricted to, web servers (Apache, IIS), SQL servers (Microsoft SQL server, MySQL server, Oracle DB server), mail servers (Exchange, Courier) and Samba servers.

- Server-Webapp:

Rules pertaining to vulnerabilities in or attacks against web based applications on servers.

In case of mistake, or to revert to the default configuration, you can use the **Reset to default** button. Note that all categories status and specific rules status will be reset and any added custom rules file will be deleted.

In addition, this page allows you to import custom rules, to enable or disable rules, and reset Snort's parameters to default.

Enable IDS on a sensor

To enable the Snort engine on a sensor:

Before you begin

To use Snort you need to enable IDS on sensors.

Snort is only compatible with sensors embedded in:

- The Cisco IC3000 Industrial Compute Gateway

- The Cisco Catalyst 9300 Series Switches

- The Cisco IR8340 Integrated Services Router Rugged

Step 1   In Cisco Cyber Vision, navigate to Admin > Sensor Explorer.

Step 2   Click a compatible sensor in the list.

The sensor's right side panel opens.

Step 3   Click **Enable IDS**.

Import Snort custom rules

Custom rules are useful if you want to define and use your own rules in addition to the rules provided in the Cyber Vision rulesets. To do this, a file must be created containing syntactically well-formed Snort rules and imported into Cisco Cyber Vision. Refer to Snort documentation for more information about creating rules.

To import custom rules in the Center:

Step 1   Prepare your custom rules file.

Step 2   Click the **Import custom rules file** button.

Once a custom rules file is imported, it is stored in the Center, and a **Download** button appears to check its content.

Import custom rules

⬆ IMPORT CUSTOM RULES FILE

You already uploaded a custom file: ⬇ DOWNLOAD

✓ Custom file successfully uploaded

Specific rule

Rule sid : [   ] [DISABLE] [ENABLE]

[RESET TO DEFAULT] [⟳ SYNCHRONIZE RULES ON SENSORS]

Step 3   Click **Synchronize rules on sensors**.

What to do next

You can Enable/disable a rule.

Enable/disable a rule

You can manually enable and disable any specific rule, whether it is a default or a custom one. To do so you need the sid (i.e. signature id) that you will find in the rules file.

In the following procedure, we will disable Snort rule sid 50772 as example.

sid 50772: An unverified password change vulnerability (CVE-2018-7811) exists in the embedded web servers of Schneider Electric Quantum Modicon Ethernet modules. This vulnerability could allow an unauthenticated remote user to access the "change password" functionality of the web server. Snort rule with sid 50772 detects such attempts. It monitors and analyzes HTTP flows coming from the external network and raises an alert when the HTTP URI fields contain specific keywords (ex. "passwd=","cnfpasswd=","subhttppwd=") that indicate a password change attempt targeting the web server.

Step 1   Click the **download icon** button.

Categories

Category	Download rules	Status
Malware-Backdoor	⬇	🟢
Malware-CNC	⬇	🟢
Malware-Other	⬇	🟢
Misc	⬇	🟢
OS-Other	⬇	🟢
OS-Windows	⬇	🟢
Server-Other	⬇	🟢
Server-Webapp	⬇	🟢

Step 2   In the rule files, look for the rule you want to enable/disable.

```
📄 Server-Webapp_rules.txt
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Seowonintech
system_config.cgi local file include attempt"; flow:to_server,established; http_uri; content:"/cgi-
bin/system_config.cgi",fast_pattern,nocase; http_client_body; content:"file_name",nocase;
content:"Content-Disposition",nocase; pcre:"/name\s*=\s*[\x22\x27]?file_name((?!^--).)*?[\x2f\x5c]/
sim"; metadata:policy max-detect-ips drop; service:http; reference:cve,2016-10760;
reference:url,ethical-hacker.org/en/seowonintech-remote-root/; classtype:web-application-attack;
sid:50754; rev:1; )
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Schneider Electric quantum
modicon ethernet module unauthenticated password change attempt"; flow:to_server,established;
http_uri; content:"/unsecure/embedded/builtin",fast_pattern,nocase; content:"user=";
content:"passwd="; content:"cnfpasswd="; content:"subhttppwd="; metadata:policy balanced-ips
drop,policy max-detect-ips drop,policy security-ips drop; service:http; reference:cve,2018-7811;
classtype:attempted-admin; sid:50772; rev:1; )
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Oracle-BI convert servlet
XML external entity injection attempt"; flow:to_server,established; http_uri; content:"/xmlserver/
convert",fast_pattern,nocase; content:"xml=",nocase; content:"ENTITY",nocase; pcre:"/(\x21|%(25)?
21)ENTITY((?!\x3e|%(25)?3e).)*?(SYSTEM|PUBLIC)/i"; metadata:policy max-detect-ips drop,policy
```

Step 3   Type the rule sid and click **Disable**.

Specific rule

Rule sid :   50772   [DISABLE]   [ENABLE]

[RESET TO DEFAULT]   [⟳ SYNCHRONIZE RULES ON SENSORS]

A message indicating the rule is disabled appears.

Specific rule

Rule sid :   50772   [DISABLE]   [ENABLE]

✅ Rule successfully disabled

If you download the rules file again you will find a "#" preceding the rule. This indicates the rule is disabled.

Step 4 Click **Synchronize rules on sensors** to save and push changes on the sensors.
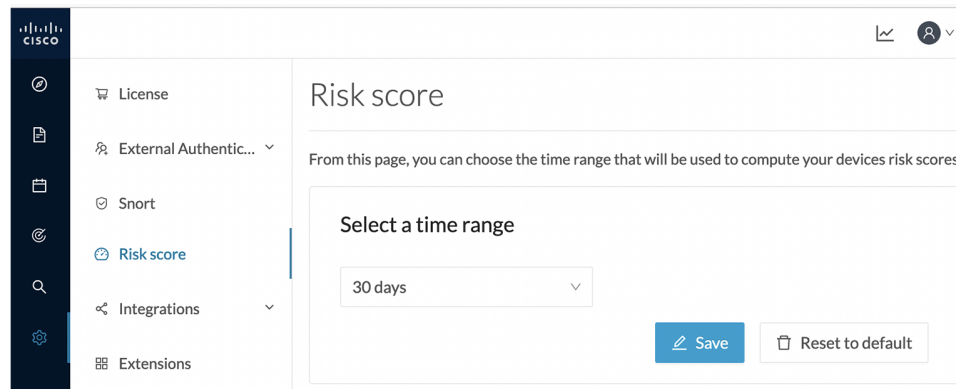
Enable/disable a rule

CHAPTER **12**

Risk score

Risk score

This page is meant to set up the time range used for risk score computation.

The computation is done every hour, but considers only the activities of the configured time period.

You can select a time range of 30 days (by default), 7 days, or set a custom one, with a minimum of one day.

For more information about risk scores, refer to the Concepts section of the User Guide..

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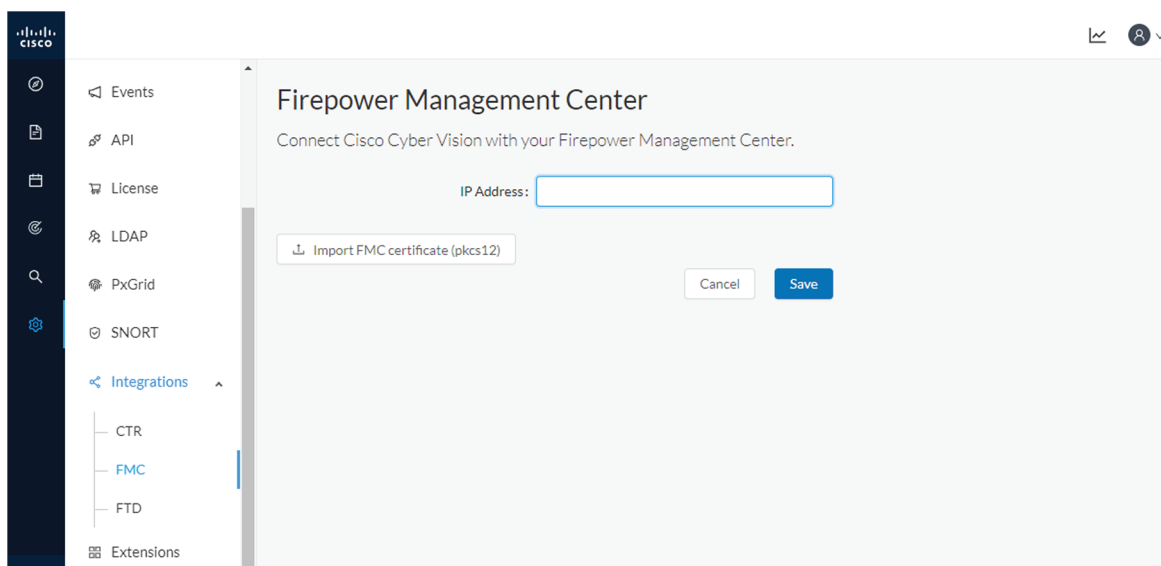
In FMC, to download the necessary certificate, please navigate to "System" then to "Integration" and open the "Host Input Client" tab. In the tab create a new Client with the button "Create Client". Add the Cisco Cyber Vision Center IP address as host name, then download the pkcs12 certificate.

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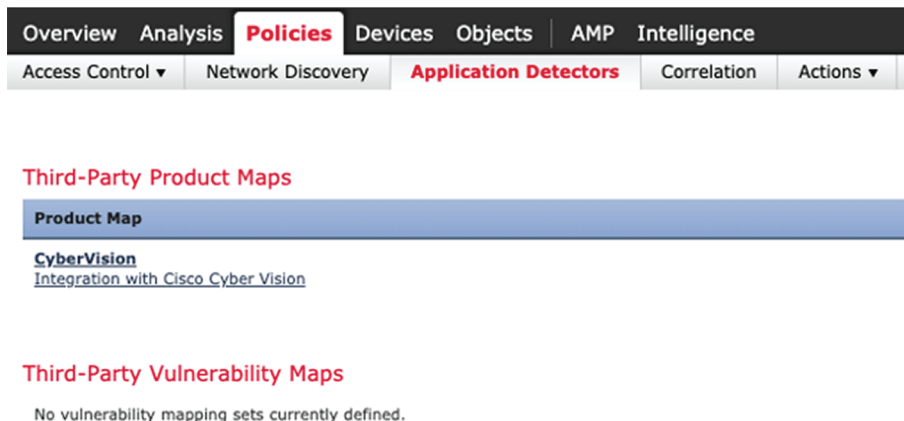
The created hosts could be consulted in FMC, menu "Analysis", tab "Hosts – Network Map":
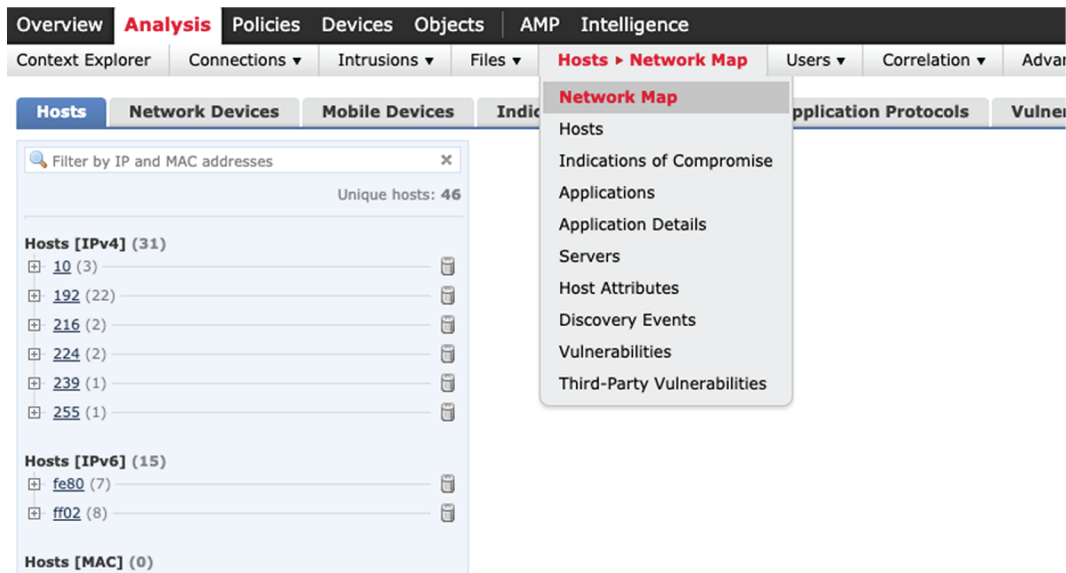
FTD

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.

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 button **Enable XDR** appears.

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

Once the link enabled, the button turns red to 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.

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

A popup appears with an authentication code.
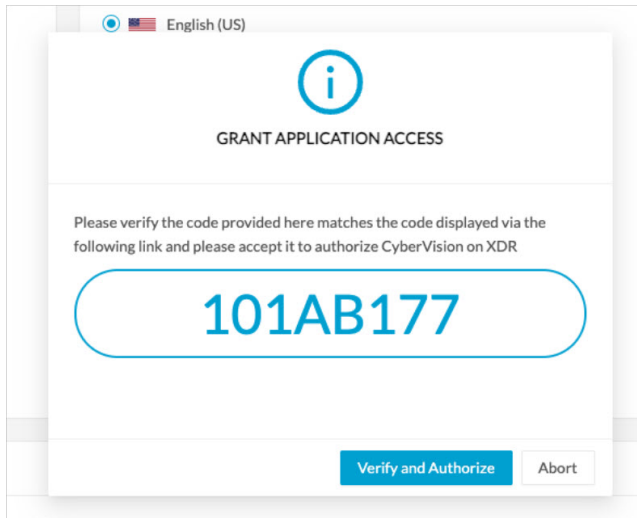
A page opens in the browser to grant Cisco Cyber Vision access to XDR. First a login is required:
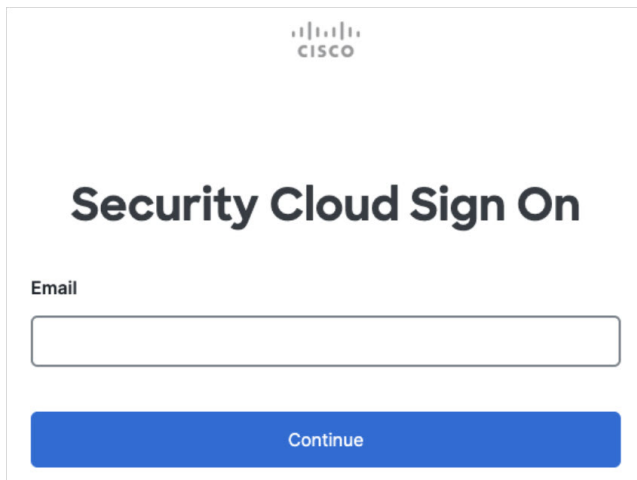
Then the authorization is required:
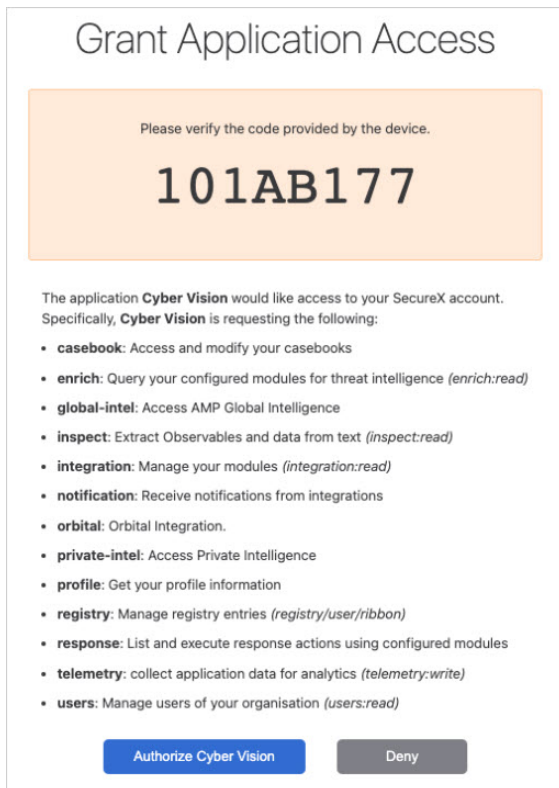
Step 6 Click **Authorize Cyber Vision**.

Step 7 A Client Access Granted popup appears.
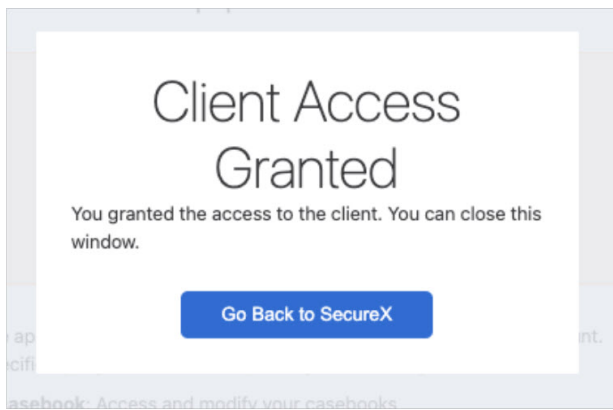
Step 8 In Cisco Cyber Vision > My Settings, the XDR menu indicates that Cisco Cyber Vision is connected to XDR. A toggle button to enable the XDR ribbon and a button to logout of XDR are displayed.
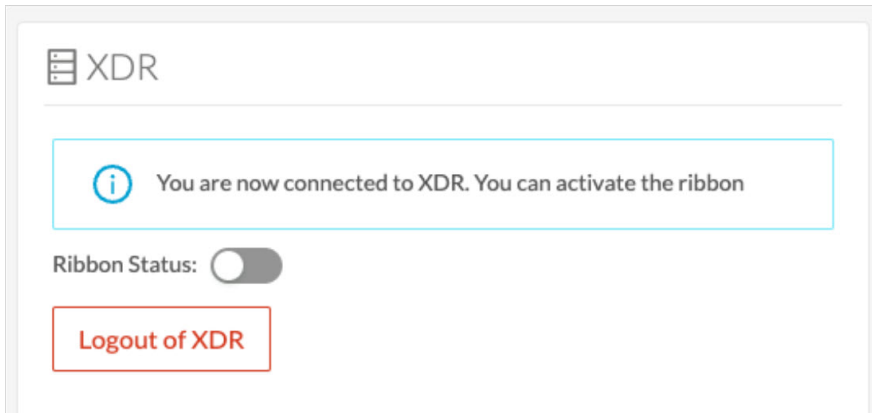
Step 9   Use the **Ribbon status** toggle button to enable the XDR ribbon.

Step 10   Click **Save settings**.
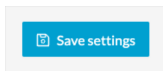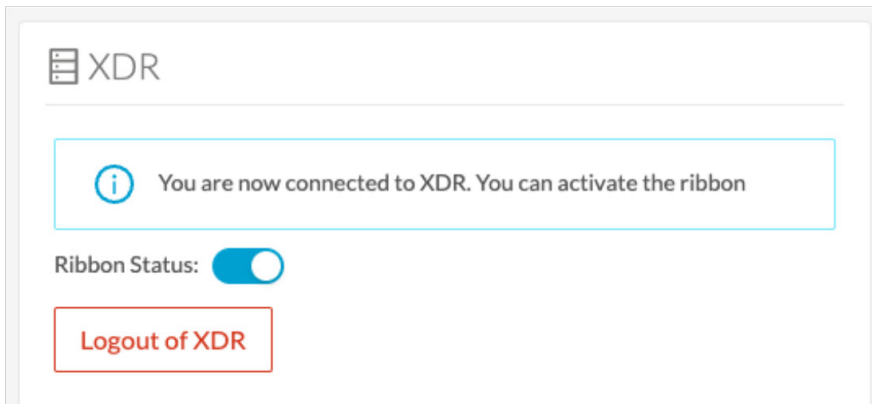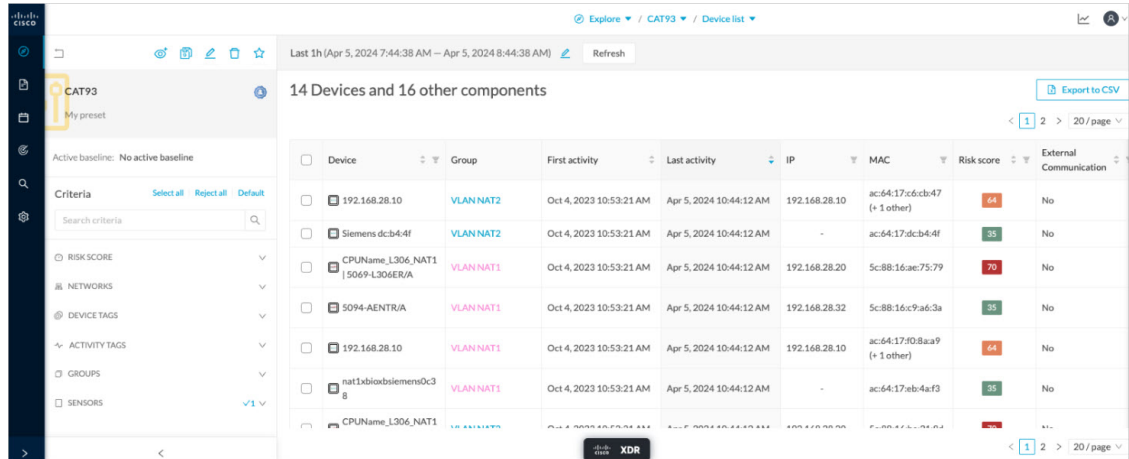
A message indicating that the XDR ribbon is enabled appears.
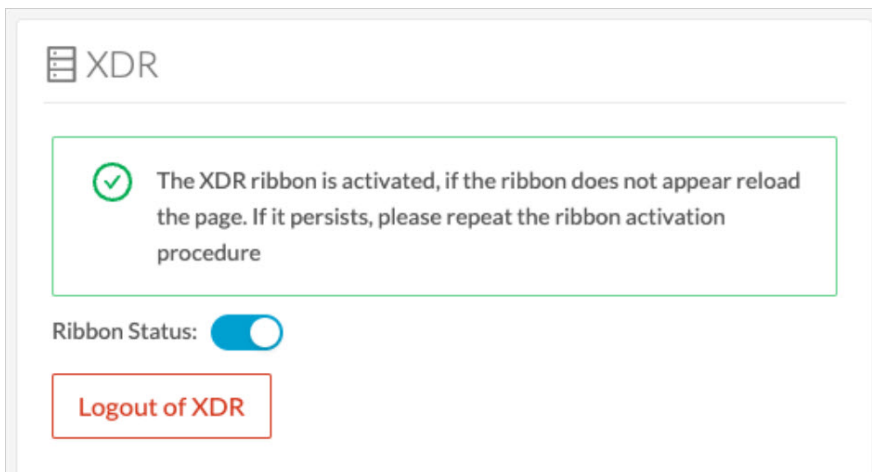
XDR ribbon

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:

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

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.
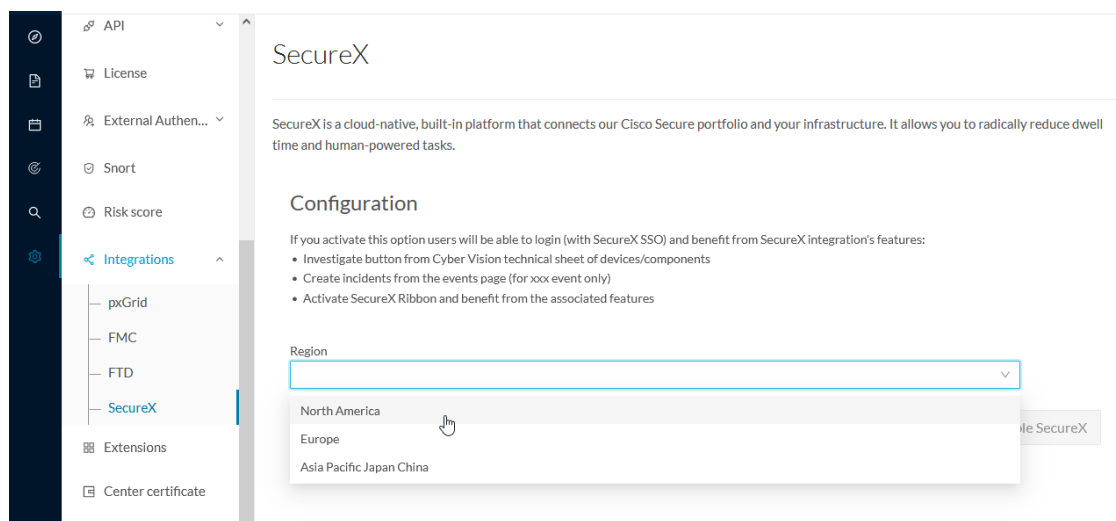
SecureX configuration

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**.
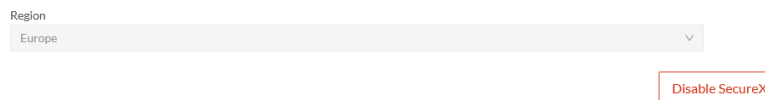**Step 2**   Select a Region.

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.
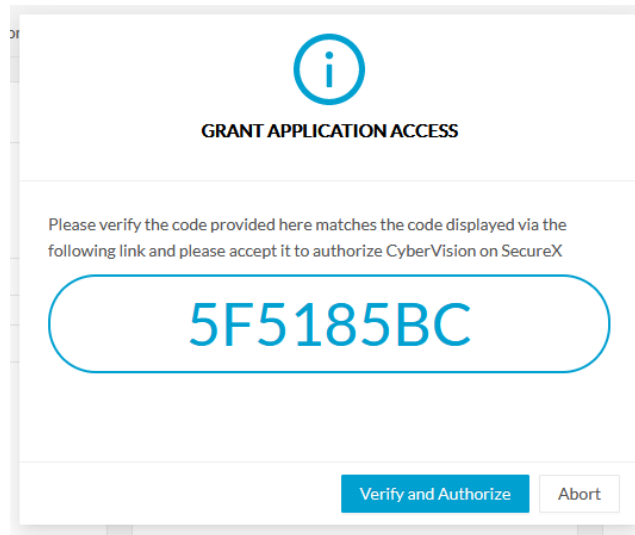
Step 4   Navigate to the user menu on the top right corner of the GUI and click **My Settings**.
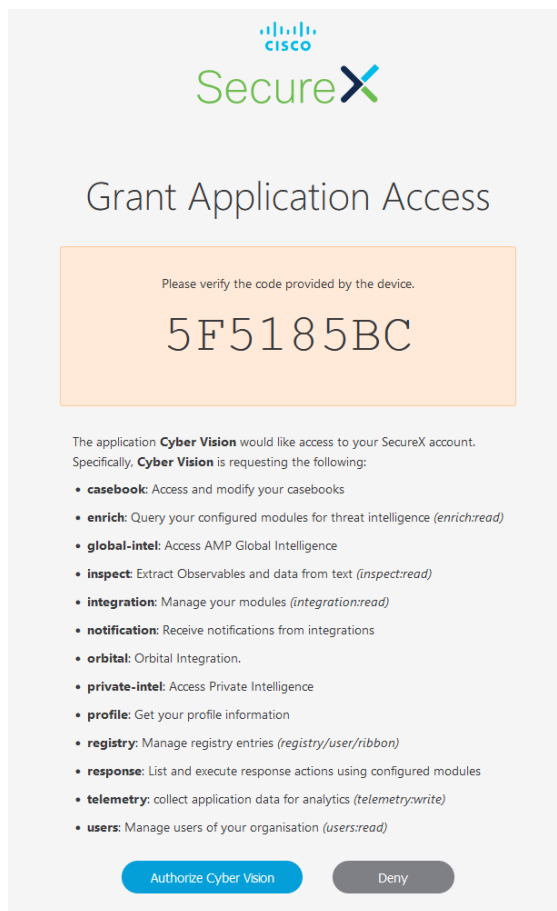
A new SecureX menu appears on the right.
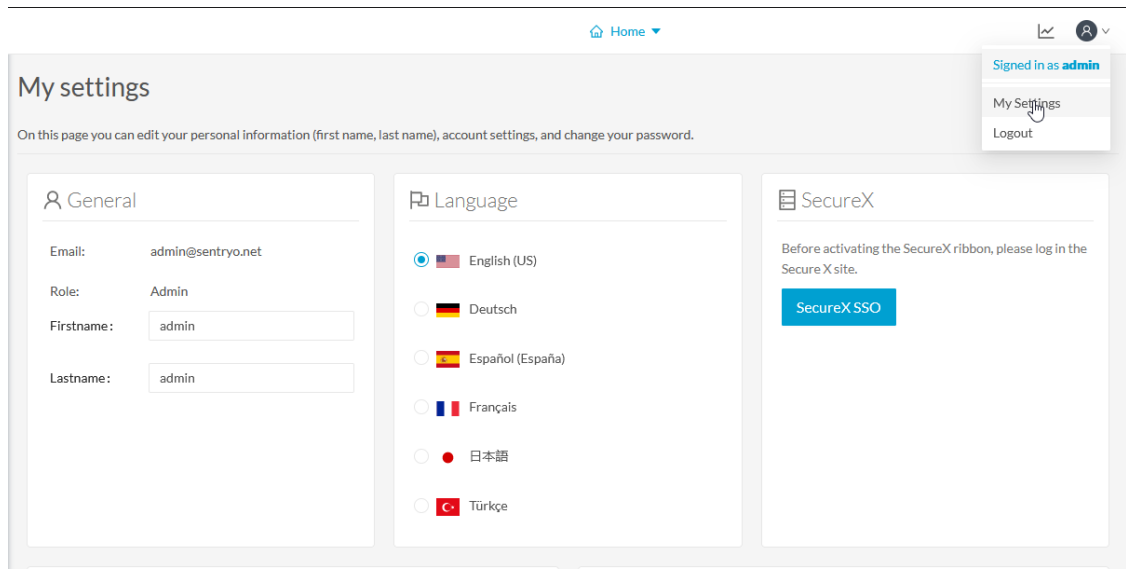
Step 5 Click the **SecureX SSO** button.

A popup appears with an authentication code.

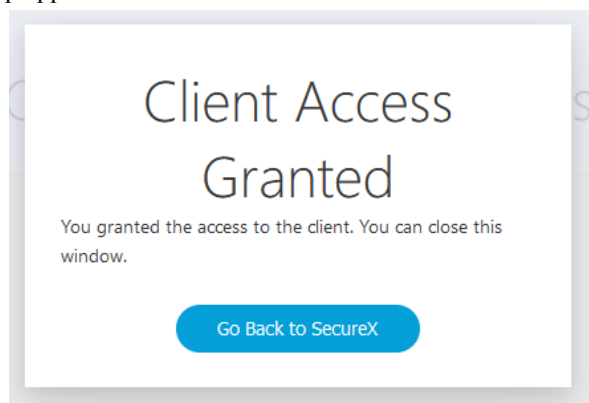

A page opens in the browser to grant Cisco Cyber Vision access to SecureX.

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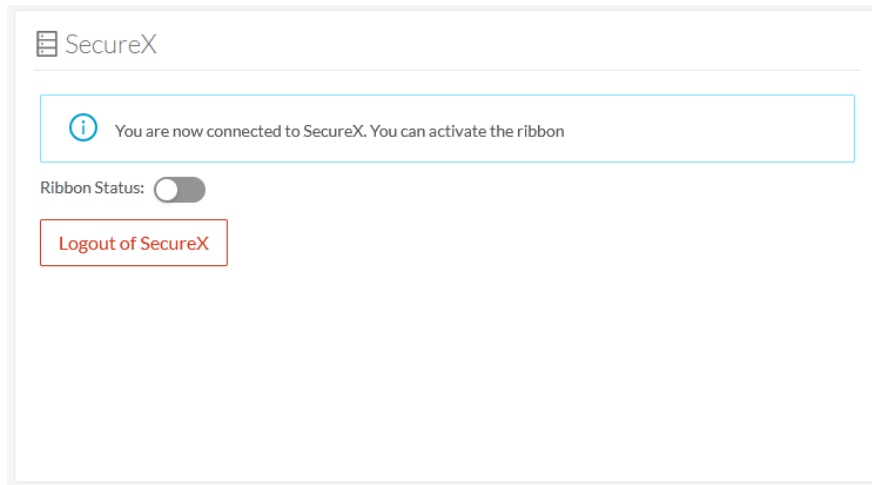
Step 9   Use the **Ribbon status** toggle button to enable the SecureX ribbon.

Step 10   Click **Save settings**.

A message indicating that the SecureX ribbon is enabled appears.
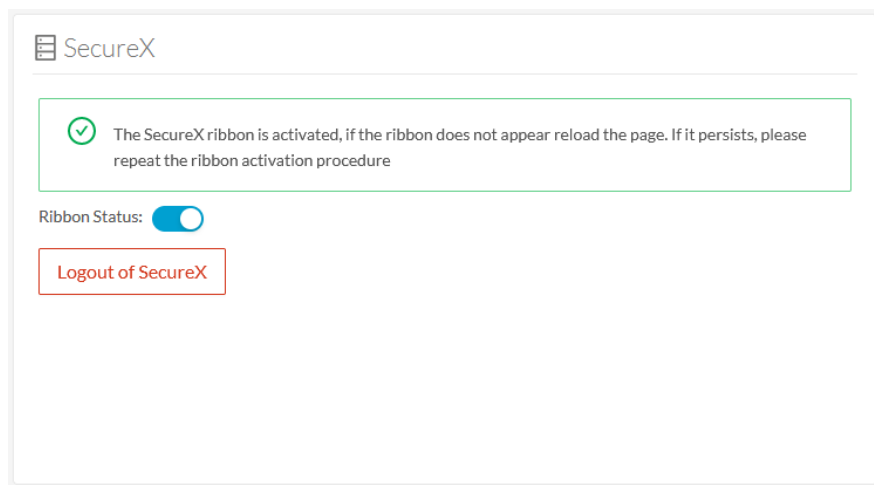
SecureX ribbon

Once configured and activated, the SecureX ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.
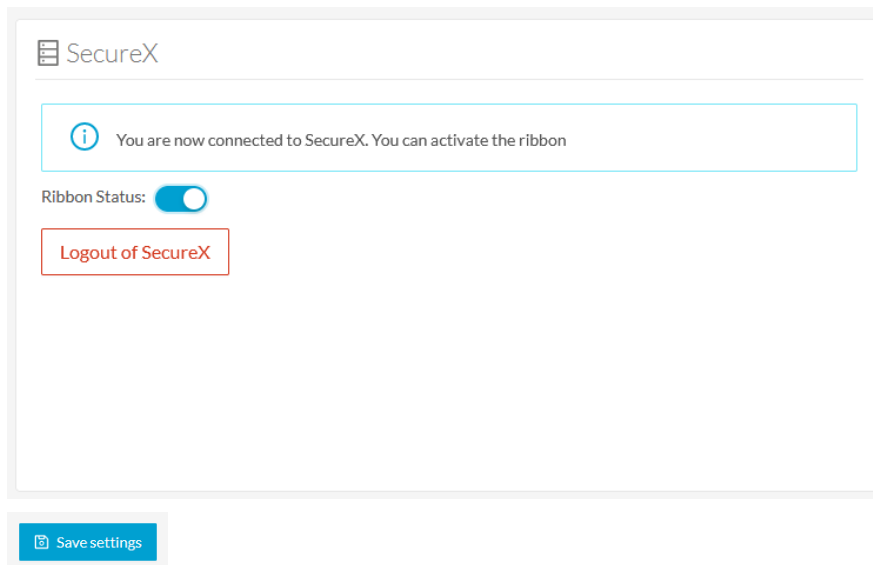
The SecureX ribbon in the Device List view:

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

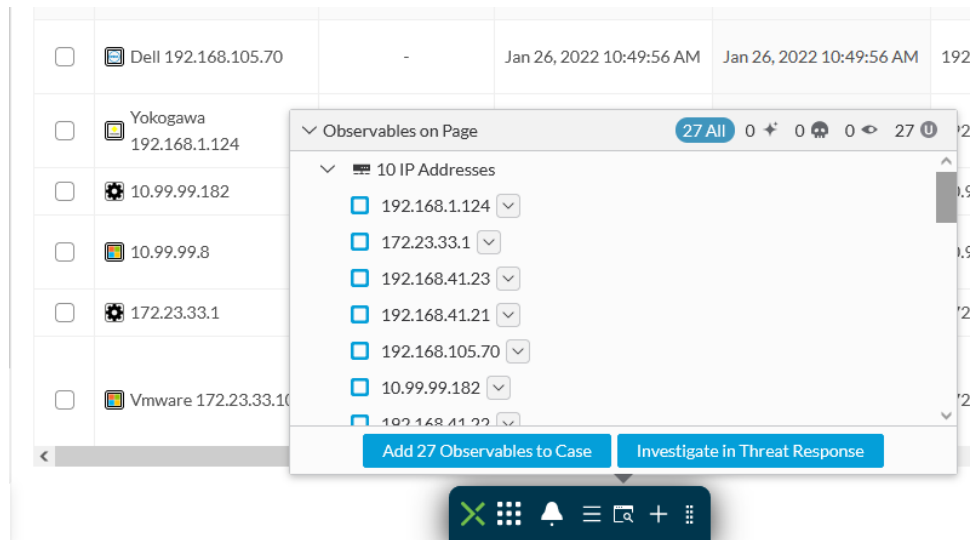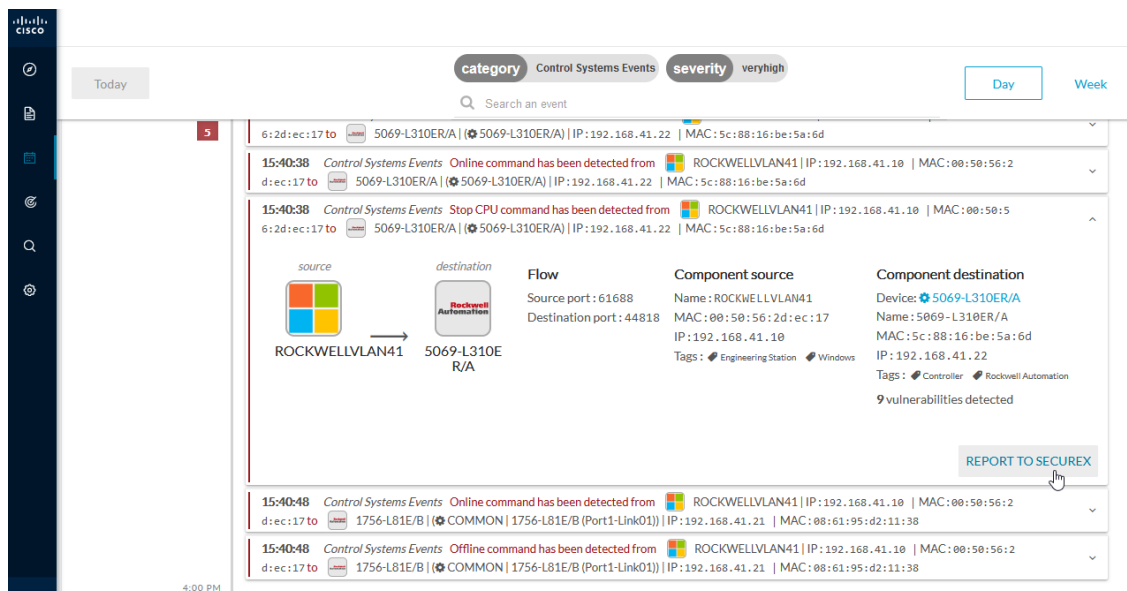Once SecureX has been configured in Cisco Cyber Vision, a **Report to SecureX** button appears on some events of the event calendar page. Using this button will push the event to SecureX and create an incident.

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.
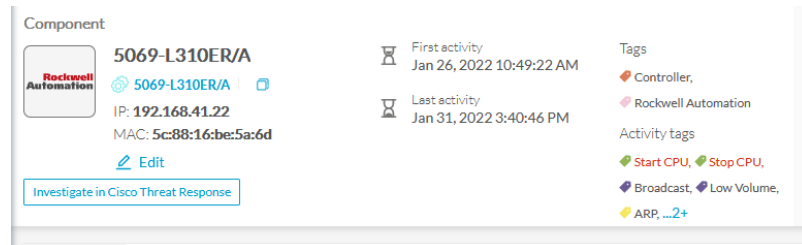
External resources for SecureX integration

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

CHAPTER 14

Extensions

- Extensions, on page 111

Extensions

From this page, you can manage Cisco Cyber Vision extensions. Extensions are optional add-ons to the Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services.

Currently, there are two extensions available:

- Sensor management extension

  For more information about this extension and how to use it, refer to the corresponding Cisco Cyber Vision Sensor Installation Guide available on cisco.com.

- Reports management extension

  For more information about this extension and how to use it, refer to the Cisco Cyber Vision GUI User Guide available on cisco.com.

To install an extension, retrieve the extension file on cisco.com and import it with the **Import a new extension file** button.

C H A P T E R 15

Web Server Certificate

- Center web server certificate, on page 113

Center web server certificate

The Center web server certificate page is to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

For more information, refer to the corresponding Center Installation Guide.

SNMP

SNMP Protocol in CyberVision is used for remote monitoring purposes.
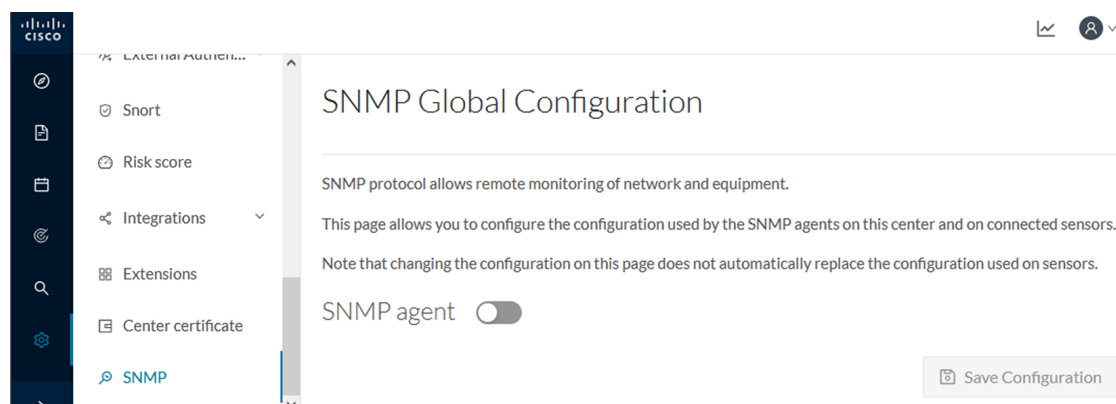
Supported versions are:

- SNMP V2C
- SNMP V3

Older versions are not supported.

☞

| Important | It is highly recommended to use version 3 of the SNMP protocol. Version 2c is available due to a large number of infrastructures still using it. However, take into account that risks in terms of security are higher. |

Snmp information:

- CPU % per core
- Load 0 to 100 (combination of CPU and I/O loads)
- RAM kilobytes
- Swap kilobytes
- Traffic for all physical interfaces (nb bytes in and out/interface (since the snmp service startup))
- Data storage (% - 250G)

  • Packets stats (packets/sec/int)

Configure SNMP

This section explains how to configure SNMP on a CyberVision Center.

Step 1   In Cisco Cyber Vision, navigate to Admin > SNMP.

Step 2   Toggle the SNMP agent button.

A configuration menu appears.

SNMP Global Configuration

SNMP protocol allows remote monitoring of network and equipment.

This page allows you to configure the configuration used by the SNMP agents on this center and on connected sensors.

Note that changing the configuration on this page does not automatically replace the configuration used on sensors.

SNMP agent

Configuration

Monitoring hosts (IPv4):

Version: ● 3   ○ 2c

Security type: NoAuth

Username: ics

Step 3   In the Monitoring hosts (IPv4) field, fill in the IP address of the Monitoring host.

Step 4   Select a version:

  • Version 3
  • Version 2c

Note For security reasons, it is recommended to use SNMP version 3.

a) **Version 3**

Select a security type:

- NoAuth: Only a username is required. No authentication password required.

Add the username that will be used for the SNMP authentication. "ics" is used by default.

- Auth with NoPriv : A username and an encrypted password are required.

Add the username that will be used for the SNMP authentication. "ics" is used by default.

Add the Hash algorithm needed and its password. It must be at least 8 characters long.

- Auth with Priv: Only the AES encryption is available. A username, an encrypted password, and an AES encryption are required.

Add the username that will be used for the SNMP authentication. "ics" is used by default.

Add the Hash algorithm needed and its password. It must be at least 8 characters long.

Add the AES password. It must be at least 8 characters long.

b) **Version 2c**

Add the community string for the Center to communicate with the monitoring host.

Step 5   Toggle the Trap button.

The following configuration menu appears:

Step 6   Setup traps to be delivered.

a) If SNMP v3 has been selected, the Engine ID field (i.e. the Center id) is displayed so you can customize it.

b) Select and set the CPU and memory rate limit and threshold according to your needs.

Step 7   Click Save Configuration.

SNMP MIB

Table 2:

MIB	OID prefix	Description
MIB-2	.1.3.6.1.2.1.1	System

MIB	OID prefix	Description
IF-MIB	.1.3.6.1.2.1.2.2.1.1	All physical interfaces
IF-MIB	.1.3.6.1.2.1.31.1.1	All physical interfaces
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.1	System
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.2.3	Storage
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.3.3	CPU
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4	Memory
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9	Disk
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10	Load
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11	CPU
UCD-DISKIO-MIB	.1.3.6.1.4.1.2021.13.15.1	Disk IO