Configure Cisco Cyber Vision

Network Organization

Network Organization 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. To access the **Network Organization** page, choose **Admin** > **Network Organization** from the main menu.

In Cisco Cyber Vision, all private IP addresses are classified as OT internal. They appear under the **IP Address / Subnet** column on the Network Organization page.

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.

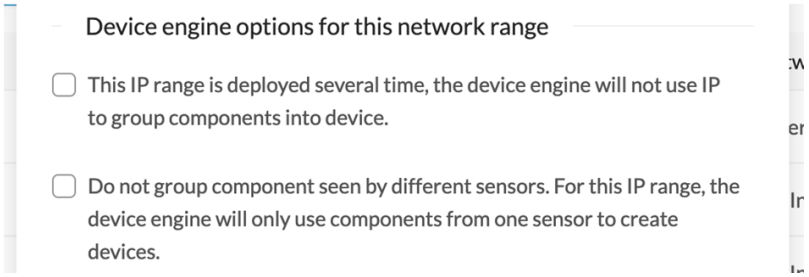
Overall, defining subnetworks in Cisco Cyber Vision is useful for several reasons:

- It allows you to choose afterwards how related flows should be stored through the Ingestion configuration page. 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.



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 specificly set in the Ingestion Configuration 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:

Procedure

Step 1 From the main menu, choose **Admin** > **Network Organization**.

Step 2 Click **Add a network**.

The **ADD A NEW NETWORK** pops-up appears.

Step 3 Enter an IP address range and its subnet in the **IP address/subnet** field.

Step 4 (Optional) Enter the **VLAN ID**.

This will allow you to create overlapping networks.

Step 5 Enter the **Network name**.

Step 6 Click the dropdown arrow of the **Network Type**.

Step 7 Select the network type from the dropdown list, such as **OT Internal**, **IT Internal**, or **External**.

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

Step 8 Check the **Use a device engine option for this network range** checkbox.

a) If applicable, select the radio button for the first option.

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

Components will not be grouped by IP.

a) If applicable, select the radio button for the second option.

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

For that particular network range, the system will not aggregate components with the same IPs detected by sensors monitoring other subnetworks. The system will aggregate the components into devices when monitored subnetworks use 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 both components are detected by the same sensor.

Step 9 Click **Add a network**.

API Token

Cisco Cyber Vision 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.

To create API token, follow these steps:

1. From the main menu, choose **Admin** > **API** > **Token**.
2. Click **+ New token**.

   The **Token** window appears.
3. Enter a name.
4. Use the **Status** toggle button to disable authorization for the token if you plan to use it later and want to prevent access until then.
5. Set an **Expiration time**.
6. Click **Create**.

   After the token creation, token appears in the list available on the **API** page.
7. Click **Show** to view the token.
8. Click copy icon to copy it.

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

API 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).

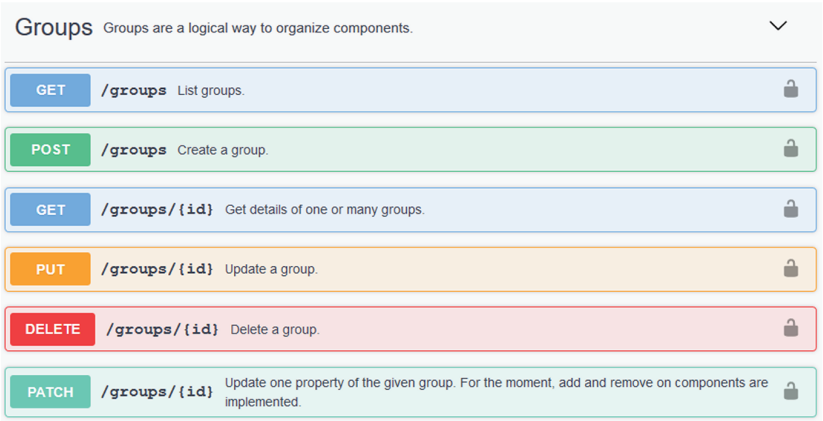
In addition to information research, this page allows you to perform basic tests and call the API by sending requests such as GET, DELETE and POST. You will get real results from the Center dataset. Specifications about routes are available such as the route's structure, and parameters and arguments 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 's elements type (activities, baselines, components, flows, groups, etc.).

The category "Groups" containing all possible group routes:



To authorize API communications:

Procedure

Step 1 From the main page, choose **Admin** > **API** .

Step 2 Click **Token** to create and/or copy a API Token.

Step 3 Click **Documentation**.

Step 4 Click **Authorize**.

The **Available authorizations** panel appear.

Step 5 Paste the token in **Value** field..

Step 6 Click **Authorize**.

Step 7 Click **Close**.

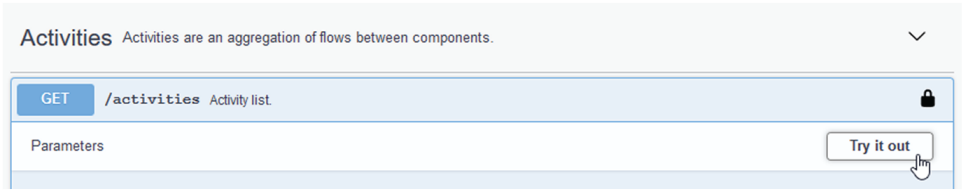
Close lockers displays. They indicate that routes are secured and authorization to use them is up.

To use a route:

Step 8 Click a route to deploy it.

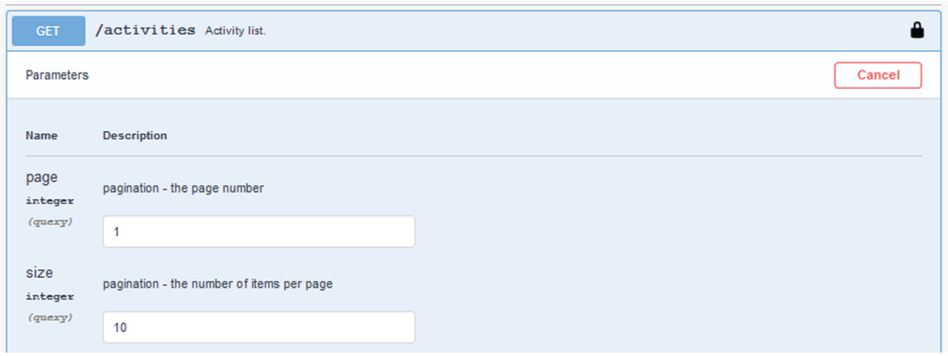
In the example, we choose Get activity list.

Step 9 Click **Try it out**.



Step 10 You can set some **Parameters**.

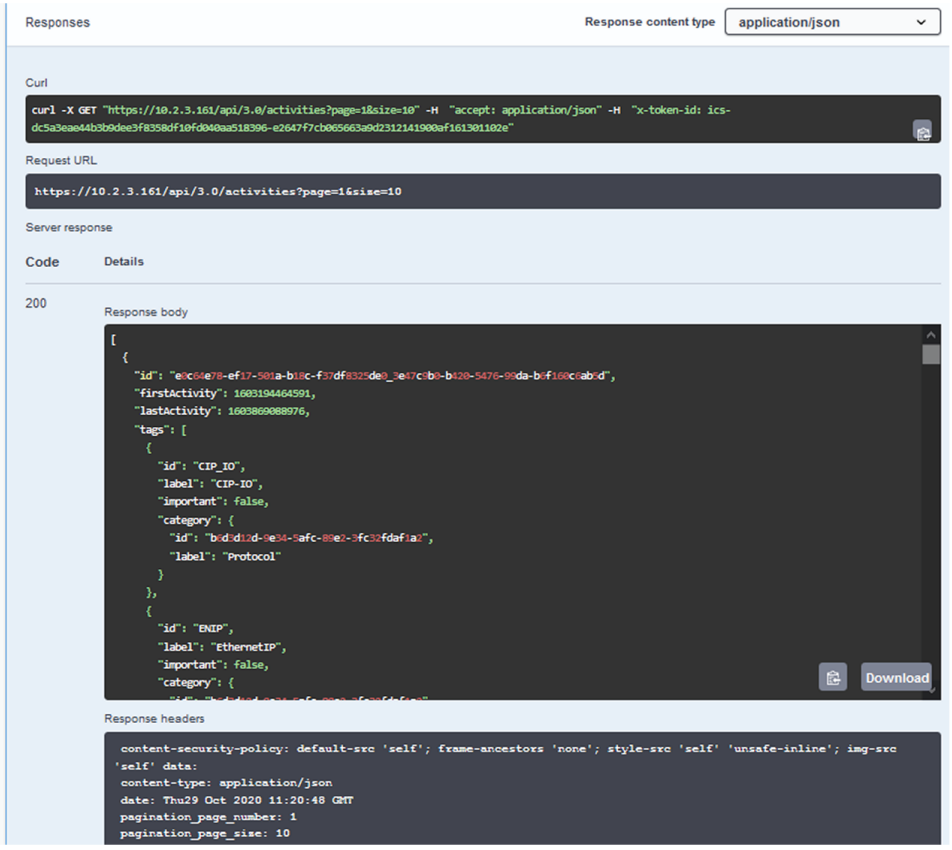
In the example, we set page to 1 and size to 10.



Step 11 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 12 When you are finished, click the **Authorize** button.

Step 13 Log out to clear the token variable, and click **Close**.

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 .

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.

To acces the **Active Discovery policies** page, choose **Admin** > **Active Discovery** > **Policies** from the main menu.

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

LDAP

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

You can enable LDAP authentication in the LDAP Settings administration page. To access **LDAP Settings** page, choose **Admin** > **External Authentication** > **LDAP**.

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.

Procedure

Step 1 From the main menu, choose **Admin** > **External Authentication** > **LDAP**.

Step 2 Click **Edit**.

The **EDIT LDAP SETTINGS** window appears.

What to do next

Configure LDAP using a LDAP Normal Connection or a LDAP Secure Connection.

LDAP Normal Connection

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

Procedure

Step 1 Fill in the LDAP settings in the **Edit ldap settings** window.

LDAP senttings are as follows:

a) Enter the **Primary Server Address**.
b) Enter the **Primary Server Port**.
c) (Optional) Enter the **Secondary Server Address**.
d) (Optional) Enter the **Secondary Server Port**.
e) Enter the **Base DN**.
f) Enter the **Server Response Time**.

Step 2 Click the **Role Mapping** tab.

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
Since the Admin user role is reserved for Cisco Cyber Vision internal usage, it cannot be mapped to external users and is not available in LDAP settings.

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

Enter the exact group names as configured in the remote directory for successful retrieval and mapping to user roles.

Step 3 Click **OK**.

Step 4 Click the **Test connection** button.

The **TEST CONNECTION** window appears.

Step 5 Enter the user credentials to test the connection between Cisco Cyber Vision and Active Directory.

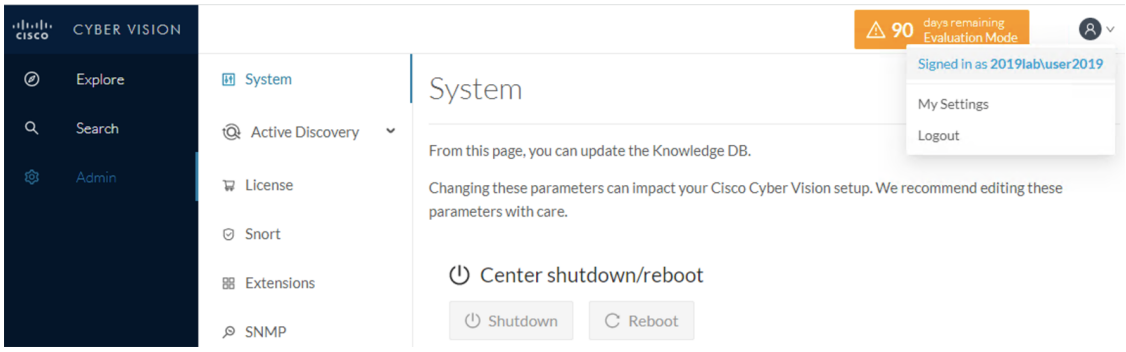
Note
The Username format is domain\user.

A message Successful LDAP bind should appear.

Step 6 Click **OK**.

Step 7 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.



LDAP Secure Connection

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

Procedure

Step 1 Fill in the LDAP settings in the **Edit ldap settings** window.

LDAP senttings are as follows:

a) Check the checkbox of **LDAP over TLS/SSL**.
b) Enter the **Primary Server Address**.
c) Enter the **Primary Server Port**.
d) (Optional) Enter the **Secondary Server Address**.
e) (Optional) Enter the **Secondary Server Port**.
f) Enter the **Base DN**.
g) Enter the **Server Response Time**.
h) Click **Choose a file** to upload a .pem root certificate or a chain certificate, or check the box of **Use self signed certificate**.

If you upload a certificate, a success message 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
Since the Admin user role is reserved for Cisco Cyber Vision internal usage, it cannot be mapped to external users and is not available in LDAP settings.

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

Enter the exact group names as configured in the remote directory for successful retrieval and mapping to user roles.

Step 5 Click **OK**.

Step 6 Click the **Test connection** button.

The **TEST CONNECTION** window appears.

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

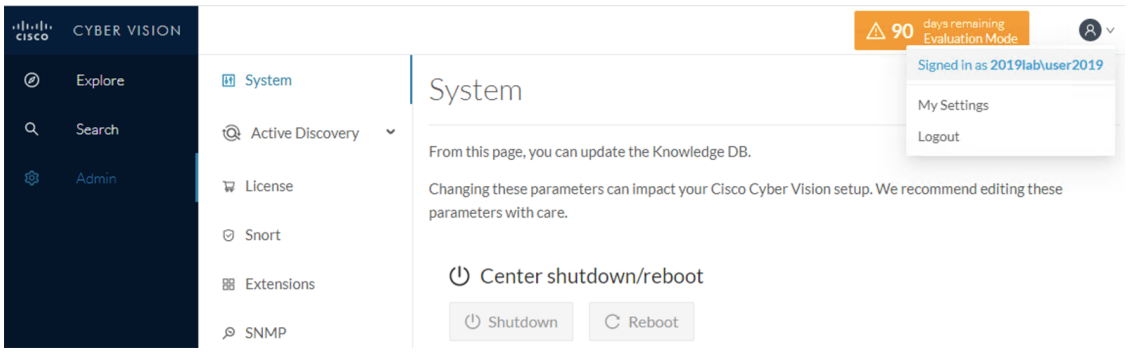
Note
The Username format is <domain_name>\<user_name> (e.g. cisco\john_doe).

A success message appears.

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.



Sensors

Sensor Explorer

The **Sensor Explorer** page allows you to install, manage, and obtain information about the sensors monitoring your industrial network. To access the **Sensor Explorer** page, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.

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

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

To filter the sensor list, follow thses steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the **Filter** icon from the top right corner of the table.
3. Type in the field or select from the drop-down menu to locate the folder(s) or sensor(s).
4. Click **Apply**.

Sorting

The sort icons next to the column titles allow you to organize sensors by label, IP address, version, location, health, and processing status in either alphabetical or ascending/descending order. The icons appear when you hover over them or apply them.

Sensors Status

To access the sensor status, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.

There are two types of sensor status:

- The **Health status**, which indicates the step of the enrollment process the sensor is at.
- The **Processing status**, which indicates the network connection state between the sensor and the Center.

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

The Sensor Explorer page provides several features to manage and use your sensors. Some buttons are accessible directly from the Sensor Explorer page to manage one or more sensors, while other buttons become available when clicking a sensor in the list. To access the sensor features, follow these steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the sensor name from the **Label** column.

   A right-side panel appears with all the features.

The features of sensors are as follows:

- The **Start recording** button records a traffic capture on the sensor. Records can be used for traffic analysis and may be requested by 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 15.
- 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. To access the **Sensor Explorer** page, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu. There are three ways to install a sensor, as follows:

- 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, you receive an alert to update the sensor. When this occurs, the latest version number appears in red, and a blue arrow with a tooltip indicates the sensor is upgradeable.

To update the senosr, follow thses steps:

- From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
- Click the sensor that is upgradeble from the **Label** column.
- The right side panel appears with sensor details.
- Click **Update**.

Update Procedure

Procedure

Step 1 From the main menu, choose **Admin** > **Senors** > **Sensor Explorer**.

Step 2 Check the checkboxes to select multiple sensors.

Step 3 Click the drop-down arrow of the **More Actions** button.

Step 4 Click **Update sensors** from the drop-down list.

The **UPDATE SENSORS** pop-up appears.

Step 5 Click **OK**.

During the update, a blue circle appears in the **Update status** column. After the update is complete, the version number turns black, and a green symbol appears in the same column.

Update Failure

If the update is unsuccessful, the **Update Status** column displays a red cross and a detailed message. To view the failure message, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu. Hover over the red cross in the **Update Status** column to see the details of the update failure.

Manage Credentials

You can use the **Manage credentials** button 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, follow these steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click **Manage Cisco devices**.
3. Click **Manage credentials** from the drop-down list.

   The **SET GLOBAL CREDENTIALS** window appears.
4. Enter the **Login** and **Password**.
5. Click **Update**.
6. After you register the global credentials, the feature is enabled in the **Install via extension** procedure. Check the **Use global credentials** checkbox to use your global credentials.

Organize Sensors

You can create folders to organize your sensors more clearly. Folders can be categorized by location, person in charge, or type of sensor, such as disconnected sensors.

To create a folder and move a sensor into it, follow these steps:

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Click **Organize**.

Step 3 Click **+ Create folder** from the dropdown list.

Step 4 Enter the **folder name**.

Step 5 (Optional) Enter **Location** and **Description**.

Step 6 Click **Ok**.

A success message appears, and the system displays the new folder in the sensor list.

Step 7 Check the checkbox of the sensor that you want to move.

Step 8 Click **Move selection to**.

The **Move selection to** pop-up appears.

Step 9 Click the drop-down arrow of the **Destination** field.

The three options are as follows:

a) Select the required folder to move the sensor.
b) Click **+New folder** to create a new folder and move the sensor.
c) Click **Root** to move sensors back into the primary list.

Step 10 Click **Ok**.

After you move the sensor into the folder, the sensor version, health status, and processing status display in the folder line.

If you move a sensor in a disconnected state into this folder, its information displays in the folder line instead of the connected sensor's information. Less secure sensor statuses are prioritized to draw your attention.

Set a Capture Mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. To access the **Capture mode** feature, follow these steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the name of the sensor from the label column.

   The side panel appears with the sensor details.
3. Click **Capture mode**.

   The **CAPTURE MODE** window appears.
4. Click the radio button to select **Capture Mode**.

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.

By 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).

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 Cyber Vision 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.

To access the Deployment Tokens page, choose **Admin** > **Sensors** > **Deployment Tokens** from the main menu.

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 starts after the sensors present the PSK to the Center and the Center delivers all necessary information for enrollment.

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 Deployment Tokens

To create tokens, follow these steps:

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Deployment Tokens**.

The **Deployment Tokens** page appears.

Step 2 Click **Add Tokens**.

The **Add new deployment tokens** panel appears.

Step 3 Fill in the following details in **Add new deployment tokens** panel:

a) Enter a name for the deployment phase.
b) Add the **Number of uses** for the number of devices to be deployed.
c) Set the token's **Expiration time**.
d) Use the **Enabled** toggle button to enable the token to continue the deployment process.

Step 4 Click **Create**.

The deployment phase with tokens per device type appears.

Note
You can view, copy, edit, disable, and delete the token.

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 , 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

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Templates**.

Step 2 Click the **Add sensor template** button.

The **CREATE SENSOR TEMPLATE** window appears.

Step 3 Add a name to the template.

(Optional) You can 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.

Step 6 To edit its settings, click the **pen** icon under the **Port Mapping** column, .

The protocol's port mapping window appears.

Step 7 Enter the port numbers you want to add.

Note
If you have continuous port numbers, you can enter a port range. For example, type 15000-15003 for ports 15000, 15001, 15002, and 15003.

Step 8 Click **OK**.

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

Step 9 Enable the toggle button **Displayed modified only** to quickly find the protocol.

Step 10 Click **Next**.

Step 11 Select the checkboxes for the sensors to which you want to apply the template.

Step 12 Click **Next**.

Step 13 Check the template configurations and click **Confirm**.

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.

Export Templates

You can use this feature to define the template at one center and then migrate it to another. To export the template, follow these steps:

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Templates**.

Step 2 Locate the template and hover over the ellipsis (…) in the **Actions** column.

Step 3 Click **Export** from the drop-down list.

Your system downloads the template to its local location.

Import Templates

To import the template, follow these steps:

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Templates**.

Step 2 Click **Import sensor template**.

The system's local folder will opens.

Step 3 Select the template and click **Open**.

The system displays the imported template on the **Configuration Template** page.

Step 4 Locate the template and hover over the ellipsis (…) in the **Actions** column.

Step 5 Click **Edit** from the dropdown list.

Step 6 From the **Select sensors** tab, check the checkboxes of the sensors to which you want to apply the template.

Step 7 Click **Next**.

Step 8 Check the details and click **Update**.

The template recovers all the changes made in the previous center, and will be applied to the selected sensors.

Management Jobs

Since some deployment tasks on sensors can take several minutes, this page displays the execution status and progress for each sensor deployed with the Sensor Management Extension. The page is visible only when the Sensor Management Extension is installed in the Cisco Cyber Vision Center.

To access the **Management jobs** page, choose **Admin** > **Sensors** > **Management jobs** from the main menu.

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

The PCAP Upload page allows you to upload PCAPs to view their data in Cisco Cyber Vision Center.

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **PCAP Upload**.

Step 2 Click **Upload a new file**.

The **UPLOAD A NEW FILE** window appears.

Step 3 Click **Choose a file or drag and drop to upload** and add the file in the box.

Step 4 Click **Upload**.

Note
During the upload, the status for DPI and Snort is displayed.

If uploading a large file, you can pause it. To resume the upload, select the same PCAP again with the browse button and click **Resume**.

SNMP

SNMP Protocol in Cisco CyberVision is used for remote monitoring purposes. To access the **SNMP Global Configuration** page, choose **Admin** > **SNMP** from the main menu.

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.

Procedure

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

Step 2 Enable the **SNMP agent** toggle button.

A configuration menu appears.

Step 3 Enter the IP address of the monitoring host in the **Monitoring hosts (IPv4)** field.

Step 4 Click the radio buttons to select a version. Version options are as follows:

- Version 3
- Version 2c

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

a) **Version 3**

- **Security type**: When the security type is **NoAuth**, only a username is required. No authentication password required.

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

- **Security type**: When the security type is **Auth** with **NoPriv**, a username and an encrypted password are required.

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

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

- **Security type**: When the security type is **Auth** with **Priv**, only AES encryption is available. A username, an encrypted password, and AES encryption are required.

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

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

  Privacy: 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 Enable the **Trap** toggle button.

The configuration menu appears:

Step 6 Set up 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
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