Revised: March 11, 2026

Deploy Cyber Vision sensor on switches and routers

What's changed in this book

This guide applies to all Cisco Cyber Vision releases, including Release 5.4.x.

Table 1: What's new in release 5.4.0

Feature	Description	
Deploy sensors on multiple IR1101 and IR1800 routers simultaneously	Bulk host onboarding and sensor deployment in Cisco Cyber Vision lets you add multiple routers at once and deploy sensor applications to them using a guided, wizard-based workflow. It automates reachability and readiness checks, reduces manual effort, and accelerates large-scale rollouts.	

Cisco Cyber Vision Sensors

A Cisco Cyber Vision sensor is an application that:

1. Embeds as an IOx application within compatible Cisco Catalyst and Industrial Ethernet switches and routers.
2. Gathers and analyzes industrial network traffic using deep packet inspection.
3. Transmits identified assets, communication flows, and security events to the Cyber Vision Center for further analysis.

Cyber Vision sensors help you analyze industry-specific OT traffic that traditional IT security tools usually cannot interpret.

How does the Cisco Cyber Vision Sensor work?

- Cyber Vision sensors deploy as IOx applications directly on Cisco switches and routers for close integration with OT devices.

  Note

  When you install a Cyber Vision sensor on a network device, the device does not support any other IOx application.

- The sensors use traffic mirroring methods (such as SPAN, RSPAN, or ERSPAN) to receive copies of OT network traffic for analysis.
- Deep packet inspection (DPI) enables identification of industrial protocols (such as Modbus, S7, EtherNet/IP, and other similar protocols), with configurable templates for targeted protocol recognition.

Note

Cyber Vision sensors only inspect TCP and UDP traffic.

- Capture modes let you define which types of traffic to analyze to optimize performance.
- Beyond passive analysis, sensors can perform Active Discovery by probing the network for device details.
- Processed data is securely sent to Cisco Cyber Vision Center.

Specific ports are used for communication between the deployed sensor and the Cyber Vision Center.

Port	Message type
TCP 5671	AMQP (Advanced Message Queuing Protocol)
TCP 10514 **Note** From Cyber Vision Release 5.4.0, this port is not used for sensor communications. Secure syslogs are also sent using TCP 5671.	Secure syslogs

Supported switches and routers

You can deploy the Cyber Vision sensor on these switches and routers. For the supported IOS XE versions for a Cyber Vision release, see the release notes.

For futher information on platform support, see the Cyber Vision data sheet.

Switches that support the Cyber Vision sensor:

- Cisco Catalyst IE3x00 switches
  - Cisco Catalyst IE3300 Rugged Series switches (models with 4 GB RAM only).
  - Cisco Catalyst IE3400 Rugged Series switches
  - Cisco Catalyst IE3400 Heavy Duty Series switches
  - Cisco Catalyst IE3500 Rugged Series switches
  - Cisco Catalyst IE3500 Heavy Duty Series switches
- Cisco Catalyst 9x00 switches
  - Cisco Catalyst 9300 Series Switch
  - Cisco Catalyst 9300X Series Switch
  - Cisco Catalyst 9400 Series Switch
- Cisco Catalyst IE9300 Rugged Series Switch

Routers that support Cyber Vision sensor:

- Cisco IR1101 Rugged Series

- Cisco IR1800 Rugged Series
- Cisco IR8340 Rugged Series

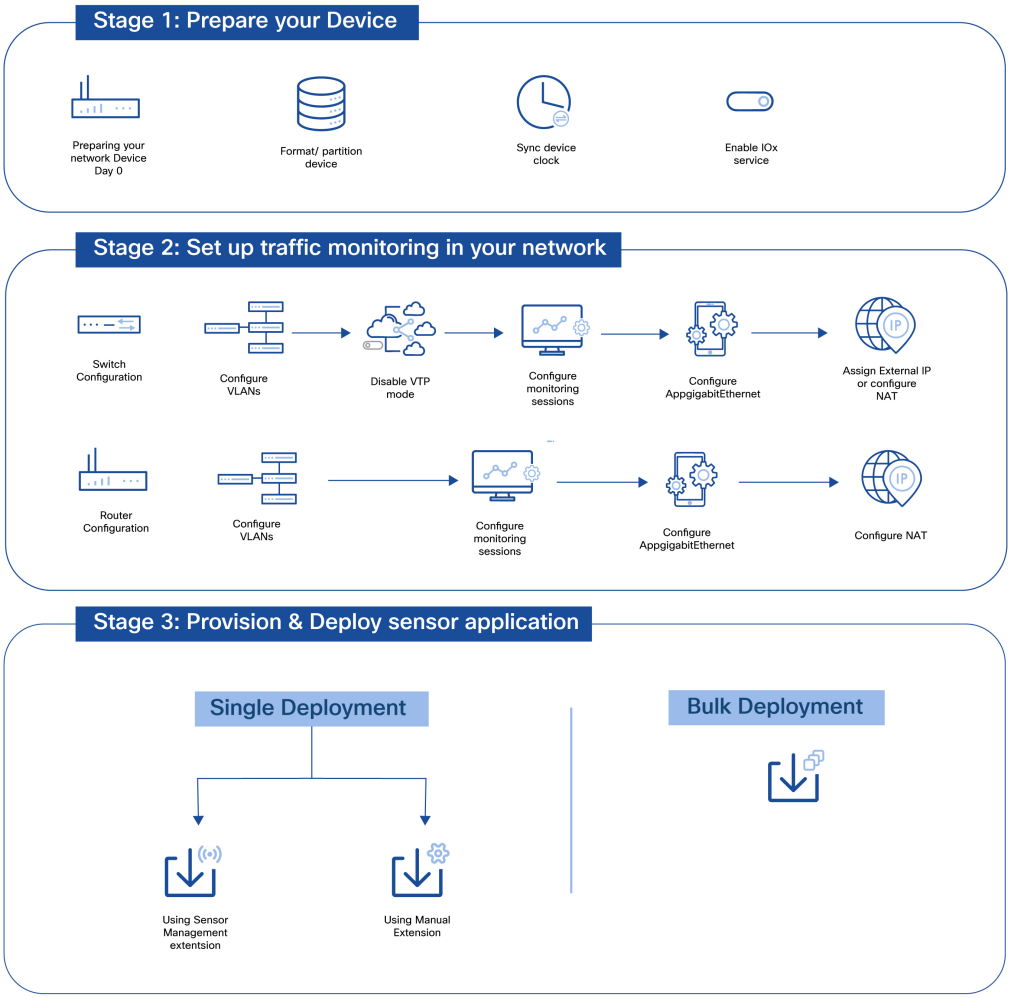
Deploying Cyber Vision sensors

Summary

Deploying Cyber Cision sensor applications on network devices is a multi-stage process that involves preparing your devices, configuring network traffic monitoring, and provisioning sensors that are capable of active discovery and packet capture.

Workflow

Figure 1: Overview of sensor application deployment process



1 Prepare switches and routers

1. Prepare the devices

   The following steps are crucial for successful deployment of sensors on your switches and routers:

   - (Switches only) Format or partition switch memory.
   - NTP Synchronization: Synchronize device and Center clock to ensure accurate reporting.
   - Enable IOx services on the device.

2. Set up traffic monitoring

   Configure traffic monitoring at the device level by setting up:

   - Mirroring VLANs or interfaces
   - Collection VLANs or interfaces
   - Gateways, where applicable
   - External IP address or NAT to allow connection to the Cyber Vision Center

3. Provision and deploy the sensor application

   You can provision sensors on one device at a time, or on multiple devices. The recommended provisioning and deployment method is to use the sensor management extension.

   For testing purposes or in case of connectivity issues, you can carry out a manual deployment process.

Prepare switches and routers

To deploy a Cyber Vision Sensor application in the routers and switches in your network, you must first prepare the devices.

1. Configure storage

   Note

   This step does not apply to Catalyst 9x00 switches and the IR routers. These devices support IOx applications on internal storage.

   The Cisco Cyber Vision Sensor application requires dedicated and compatible storage to install files, store configuration data, and manage logs. Format or partition storage, such as an SD card or SSD, to create a compatible file system for the Linux-based environment. The sensor application requires ext4. This preparation lets the switch's operating system (IOx) recognize, allocate, and write data to storage. Without this step, you cannot install or run the sensor application.

2. Synchronize clocks

   The sensor application obtains its time from the host device. We recommend using an NTP server so that the various devices in your network are synchronized.Using an NTP across devices enables accurate monitoring, effective security analysis, and reliable communication with the central Cyber Vision Center. It also ensures the integrity of all data collected by the Cyber Vision Sensor.

Note

Synchronize all device and IOx application clocks to UTC.

3. Enable the IOx service

   IOx is an application hosting framework. It allows applications to run directly on Cisco network devices. Enabling IOx activates a specialized environment on the device and provides the necessary runtime, resources, and isolation. This environment allows the sensor application to operate independently from the device core operating system (IOS XE). Without IOx, there is no platform or dedicated environment for the Cyber Vision Sensor application.

Before you begin

To carry out this taskflow, ensure that:

- SSH access to the device is available.
- The device is running a supported IOS XE software version.
- If you wish to use SD card on a device, the card must be 4 GB or greater.

For instructions on setting up the prerequisites, refer to the configuration guides for the specific device.

Step 1 Configure device storage.

Storage type	Commands
IE3x00 SD card	• Format the card using `format sdflash: ext4`. • Partition the card using `partition sdflash: iox`.
IE9300 SD card	Partition the card using the command `partition sdflash: iox`.
Catalyst 9x00 using SSD disk	Format the disk using the command `format usbflash1: ext4`.

Step 2 (Only for switches) Verify storage configuration. In the command response, check that the file system type is `ext4`.

Switch	Command
IE3x00 and IE9300	`show sdflash: filesys`
Catalyst 9x00	`show usbflash1: filesys`

Step 3 Use **ntp server <server-ip-address>** to add an NTP server.

Step 4 Enable IOx service:

```
configure terminal
iox
exit
```

Step 5 Use **show iox** to confirm that the IOx service is running.

If an IOx application does not have the necessary read and write permissions, the application may not initiate or function correctly.

Setting up OT traffic monitoring

Setting up traffic monitoring on switches and routers is essential for a Cisco Cyber Vision sensor to perform Deep Packet Inspection (DPI) on network traffic and securely send data to the Cyber Vision Center.

Summary

The goal of this configuration is to ensure that the Cyber Vision sensor receives a complete and accurate copy of network traffic for analysis, and can securely send the data to Cyber Vision Center. The data is then contextually organized in the Center, enabling you to effectively monitor your OT and IT assets and respond to any potential risks.

Workflow

1. Configure VLANs

   VLANs are the building blocks of any modern network. When you configure VLANs, you ensure that OT devices and relevant IT traffic are properly defined and ready for monitoring.You can then view traffic data by VLAN ID in the Cyber Vision Center, gaining visibility of your operational environment.

2. (IE3300 and IE3400 Switches Only) Disable VTP mode

   VTP can automatically propagate VLAN configurations across a network. Disabling VTP mode on the monitoring switch or relevant interfaces helps prevent unintended VLAN changes that could disrupt the monitoring setup.

3. Configure monitoring sessions

   Monitoring sessions are core mechanisms for traffic mirroring, and typically use Switched Port Analyzer (SPAN)-based methods. This step involves setting up a session to copy traffic from specific source ports or VLANs to a designated destination port where the Cyber Vision sensor is connected. This allows the sensor to passively inspect all relevant traffic without affecting network performance or operations.

Note

- If you want to mirror by port in IE3400 and IE3400 devices, you must mirror all the ports. Port mirroring only supports ingress packets, leaving egress packets unmonitored. Mirroring all ports ensures all communications are mirrored and monitored.
- In the case of VLAN mirroring, LLDP and CDP traffic may not be captured.

4. (All switches and IR8340 routers) Configure AppGigabitEthernet

   The AppGigabitEthernet interface allows switches to connect to the IOx application, Cyber Vision sensor. Proper configuration ensures that the interface is ready to receive the mirrored traffic efficiently and can handle the data throughput required for DPI.

5. Configure External Communication
   - (Switches only) Assign an external IP address

     A Switch Virtual Interface (SVI) is a virtual Layer 3 interface on a multilayer switch that serves as the default gateway for a specific VLAN, enabling communication and routing between VLANs. Setting up SVI provides an external IP for the switch. The IP address is used by the Cyber Vision Center to deploy the sensor application on a device using the sensor management extension.

   - Configure NAT

If the Cyber Vision sensor is located in a private network segment and needs to communicate with the Cyber Vision Center over a public network or a different private segment, NAT configuration is crucial. It translates the sensor's private IP address to a routable address, enabling secure and successful communication with the Cyber Vision Center for data transmission.

Routers and specific switches (IE3500, IE9300, Catalyst 9x00) use classic NAT.

The IE3300 and IE3400 switches use a specially designed Layer 3 NAT (L3NAT) method. L3NAT is supported by these switches if they run IOX-XE 17.14.1 or later releases. You can only configure L3NAT for Cyber Vision use on these switches, as the NAT method is not broadly supported on the devices. L3NAT only allows supports static translation of UDP and TCP packets, and requires a Network Advantage license.

Result

The network is configured to mirror OT traffic for deep packet inspection via the Cyber Vision Sensor, with appropriate segmentation, security, and monitoring fidelity from the intended OT network segments to the Cyber Vision Center.

Configure traffic monitoring on the switches

Before you begin

This task flow provides an overview of the various steps to collect the traffic information that the Cyber Vision sensor can inspect, analyze, and send to the Cyber Vision Center. Based on the switch you use and the mirroring and monitoring techniques you want to employ, refer to these configuration guides for detailed configuration examples:

- Cisco IE3300 Rugged Series Configuration Guides
- Cisco IE3400 Rugged Series Configuration Guides
- Cisco IE3500 Series Switch Software Configuration Guide
- Cisco Catalyst IE9300 Rugged Series Configration Guides
- Cisco Catalyst 9300 Series Switches Configuration Guides
- Cisco Catalyst 9400 Series Switches Configuration Guides

In this task, the configuration examples aim to configure mirroring on VLAN 2508 and collection on VLAN 507.

Step 1 Use the `configure terminal` command to enter the global configuration mode.

Step 2 (For IE3300 and IE3400 devices) Use the `vtp mode off` command to disable VTP.

Step 3 Use the `vlan <vlan ID>` command to create a mirror VLAN (VLAN 2508) and a collection VLAN (VLAN 507).

Switch series	Configuration example

IE3300 and IE3400 (RSPAN must be enabled on the mirror VLAN as ERSPAN is not directly supported.)	`switch(config)#vlan 2508`
	`switch(config)#remote span`
	`switch(config)#exit`
	`switch(config)#vlan 507`

IE3500, IE9300, Catalyst 9x00	`switch(config)#vlan 2508` `switch(config)#vlan 507`

Step 4 Use the `monitor session` command to define monitoring sessions.

Switch series	Configuration example
IE3300 and IE3400	!To configure physical port monitoring switch#conf t switch(config)#monitor session 1 source interface Gi1/3 - 10 both switch(config)#monitor session 1 destination remote vlan 2508 switch(config)#monitor session 1 destination format-erspan <cyber-vision-sensor-capture-ip> !To configure vlan monitoring switch#conf t switch(config)#monitor session 1 source vlan 1 rx switch(config)#monitor session 1 destination remote vlan 2508 switch(config)#monitor session 1 destination format-erspan <cyber-vision-sensor-capture-ip>
IE3500, IE9300, Catalyst 9x00	!Example that defines an ERSPAN source session with header and destination parameters switch#conf t switch(config)#monitor session 1 type erspan-source switch(config)#source interface Gi1/11 both switch(config)#no shutdown switch(config)#header-type 3 switch(config)#destination erspan-id 2 ip address <erspan-destination-ip-address> switch(config)#mtu 9000 switch(config)#origin ip address <origin-ip-address> switch(config)#exit

Step 5 Configure AppGigabitEthernet port to enable communication with the IOx application, the Cyber Vision sensor.

Switch type	Configuration example
IE3300, IE3400, IE3500	switch#configure terminal switch(config)#interface AppGigabitEthernet 1/1 switch(config)#switchport mode trunk switch(config)#exit
IE9300, Catalyst 9300, Catalyst 9400	switch#configure terminal switch(config)#interface AppGigabitEthernet 1/0/1 switch(config)#switchport mode trunk switch(config)#switchport trunk native vlan <existing-vlan-ID> switch(config)#exit

Step 6 Enable external communication by configuring switchport access (external IP) for the collection VLAN, or setting up NAT, or both.

External communication method	Configuration example
L3NAT for IE3300 and IE3400 switches	!Define a private IP for the sensor application to act as its default gateway. Switch(config)#int vlan <vlan-ID> Switch(config-if)#ip address <ip-address> <subnet-mask> !Define a management SVI IP address for the switch. Switch(config)#int vlan 507

External communication method	Configuration example
	Switch(config-if)#ip address <ip-address> <subnet-mask> !Configure L3NAT-IOx. Switch(config)#l3nat-iox Switch(config-iox-nat)#app-ip <private-IP> svi-ip <svi-ip> app-name <sensor app name> server-ip <cyber-vision-center-IP>
NAT for IE3500, IE9300, and Catalyst 9x00 switches	enable switch#configure terminal switch(config)#interface port-channel <inside-interface-ID> switch(config)#ip address <ip-address> <subnet-mask> [secondary] switch(config)#ip nat inside switch(config)#exit switch(config)#interface port-channel <outside-interface-ID> switch(config)#ip address <ip-address> <subnet-mask> [secondary] switch(config)#ip nat outside switch(config)#exit end

Step 7 Use the `write mem` command to save these settings to the switch's startup configuration.

Configure traffic monitoring on routers

Of the supported routers, IR8340 is unique in hosting switched ports. If you want to monitor traffic from switched ports on IR8340, carry out step 2.

If you are configuring IR1101 or IR1800, start this task at Step 3.

Step 1 Use the **configure terminal** command to enter the global configuration mode.

Step 2 (IR8340 only) Configure a VLAN and an AppGigabitEthernet port to mirror traffic from switched ports.

The VLAN number must be between 2340 and 2349, the range reserved for internal system uses such as IOx application hosting and ERSPAN traffic.

Example:

```
#Configure VLAN
vlan 2340
exit
interface vlan 2340
ip address 169.254.2.1 255.255.255.252
no shutdown
exit

#Configure AppGigabitEthernet port
interface AppGigabitEthernet 0/1/1
switchport mode trunk
exit
```

Step 3 For routing ports, connect the application to a VirtualPortGroup and assign it an IP address to create a destination for the ERSPAN traffic.

Example:

```
ip routing
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
exit
```

Step 4 Configure a monitor session for the ERSPAN traffic

Option	Description

For routing ports	`monitor session 5 type erspan-source`
	`source interface Gi0/0/0`
	`no shutdown`
	`destination erspan-id 1`
	`mtu 1464`
	`ip address 169.254.1.2`
	`origin ip address 169.254.1.1`
	`end`

For switching ports	`monitor session 1 type erspan-source`
	`source interface Gi0/1/0 - 10 both`
	`no shutdown`
	`destination erspan-id 2`
	`mtu 9000`
	`ip address 169.254.2.2`
	`origin ip address 169.254.2.1`
	`exit`

Step 5 Configure NAT to enable the sensor application to reach the Cyber Vision Center.

Example:

```
Configure terminal
interface GigabitEthernet 0/0/0
ip nat outside
media-type rj45
exit
interface VirtualPortGroup 1
ip address 169.254.0.1 255.255.255.252
ip nat inside
exit
ip nat inside source list NAT_ACL interface GigabitEthernet 0/0/0 overload
ip access-list standard NAT_ACL
10 permit 169.254.0.0 0.0.0.3
exit
```

Deploying sensor applications

When deployed in your network, the Cyber Vision sensor application enables real-time threat detection. It also provides ongoing visibility into industrial network assets and traffic patterns to support security and compliance objectives.

You can deploy sensors on multiple network devices to expand coverage as needed.

There are multiple ways of deploying the sensor application on the supported switches and routers:

- (Recommended) Using the sensor management extension in the Cyber Vision Center
- Using the device CLI
- Using the device Web UI

- Bulk deployment

The sensor management extension is recommended because it offers these advantages:

- Simple deployment: Automates installation and device configuration steps, reducing complexity for IT/OT teams.
- Consistency: Sensors can be deployed in a standardized, repeatable manner.

Note

FIPS-compliant Cisco Cyber Vision does not support the sensor management extension.

Manual installation using the device's Web UI or CLI is required when the Center cannot connect to the target device because of network design or temporary issues.

This guide details the sensor extension deployment method. To deploy the sensor application using the device CLI or Web UI, see the guide for the specific device and IOS XE release:

- Deploying Cisco IOx Applications, Cisco Catalyst IE3400 Rugged, IE3400 Heavy Duty, and IE3300 Rugged Series Switches
- Chapter IOx Applications Deployment on the Switch, Cisco IE3500 Series Switch Software Configuration Guide
- Chapter IOx Application Hosting, Cisco Catalyst IR8340 Rugged Series Router Software Configuration Guide
- Chapter IOx Application Hosting, Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide
- Chapter IOx Application Hosting, Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide

Summary

After you complete initial configurations and traffic monitoring settings, you can prepare the network device and provision sensor applications for deployment. Use the sensor management extension in the Cyber Vision Center for efficient sensor deployment and management.

Workflow

The sensor provisioning process involves these stages. Each stage is executed separately when you choose manual deployment methods. With a sensor extension, all the stages are executed automatically using the configuration taskflow wizard.

1. Define sensor provisioning in the Center

   The taskflow wizard for sensor provisioning involves defining these details:

   - (If you don't use the sensor management extension) Device serial number.
   - Device address and access credentials. The user must have Level 15 privilege access, with web UI access to deploy sensors using the sensor management extension.
   - Collection and management VLANs, ports, gateway and interfaces configured on the device for Cyber Vision.
   - Define the capture mode by selecting the type of traffic you want the sensor to analyze.

2. Activate the provisioning file in the device

   If you use the sensor management extension, you can deploy the sensor provisioning from the Center.

   If you use the device Web UI or CLI, you must download the provisioning package from the Center and upload it to the device.

3. (Optional) Enable Active Discovery

   To periodically monitor a specific set of protocols on devices, enable active discovery on the sensor. Define the ports that must be monitored for each protocol for best results.

   Cisco IR1101 and IR1800 routers do not support Active Discovery.

Note

To use Active Discovery, you must download and install the Cyber Vision sensor package that includes the feature. The name of the sensor package on Cisco Software Downloads indicates if Active Discovery is available in the package. If you have already installed a sensor with a package that doesn't include Active Discovery and wish to use this feature, you must reinstall the sensor with the correct software.

4. Manage sensor application

   Deployed sensors are listed in the **Admin** > **Sensors** > **Sensor Explorer** page of the Center. You can monitor their status and manage the sensors from the Center.

Result

When the sensor application is successfully configurred and deployed, the sensor captures and analyses network traffic in real-time. The sensor extracts and forwards security and operational insights to the Cyber Vision Center, enabling alerting, troubleshooting, and security management.

Provision sensors using sensor management extension

Step 1 Install sensor management extension, on page 12.
Step 2 Add global device credentials, on page 12.
Step 3 Install sensors using sensor management extension, on page 13

Install sensor management extension

Step 1 From the Cisco Cyber Vision Center menu, choose **Admin** > **Extensions**.
Step 2 Click **Import a new extension file**.
Step 3 Choose the extension file from your local system.

What to do next

After you upload an extension file, from the **Actions** column, you can:

- Update the extension to a different release.
- Remove the extension.

Add global device credentials

Define the default credentials to be used for device access. The global credentials are used for all devices by default for sensor management workflows. When you update the credentials, the latest credentials are used to access deployed sensors as well.

The user credentials must have Level 15 access privilege, and have access to the device Web UI.

Step 1 From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Choose **Manage Cisco devices** > **Manage credentials**.

Step 3 To save the credentials, click **Update**.

Install sensors using sensor management extension

Before you begin

- Install sensor management extension, on page 12.
- Add global device credentials, on page 12.
- Define capture and collection details for network . For instructions, see Setting up OT traffic monitoring, on page 6. Capture IP and VLAN form the internal connection between the device and the sensor application. Collection IP and VLAN form the connection between the sensor application and the Cyber Vision Center.
- Device must have Web UI set up.
- A configuration template allows you to define the ports and protocols that the Cyber Vision sensor must monitor. While a default template is available for use, you can also create your own template.
- Cisco IR1101 and IR1800 routers do not support Active Discovery.
- To use Active Discovery, you must download and install the Cyber Vision sensor package that includes the feature. The name of the sensor package on Cisco Software Downloads indicates if Active Discovery is available in the package. If you have already installed a sensor with a package that doesn't include Active Discovery and wish to use this feature, you must reinstall the sensor with the correct software.

Step 1 From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Click **New sensor** > **Install via extension** to initate the installation wizard.

Step 3 In the **Reach Cisco device** page, fill out the following details to allow the Cyber Vision Center to identify and reach the device on which you want to install the sensor application:

- (Mandatory) **IP address**
- (Mandatory) **Port**: Typically, port 443 is the standard port for secure HTTPS traffic. However, you can choose to use a different port.
- **Center collection IP**: To use the Center's current collection IP, leave the field empty. To use a different collection IP, especially in case of NAT configurations, enter the reachable IP address.
- **Sensor label**: Enter a easily identifiable label for the sensor.
- **Configuration template**: From the configuration template drop-down list, choose the template to apply.
- **Credentials**: Choose to use global or custom credentials to reach the device.
- **Capture Mode**: Choose the data you want the Cyber Vision sensor to inspect.

Step 4 Click **Connect**.

Step 5 In the **Configure Cyber Vision IOx sensor app** page, define the monitor sessions on the device by providing the required details. The fields that you see in this page change based on the device have connected to.

Configuration field	Device this field applies to
• Capture (mirroring) and collection IP addresses.	All switches and routers

Configuration field	Device this field applies to
• Capture (mirroring) and collection prefix lengths. • (Optional) Collection gateway, if the Center and the sensor application are in different subnets.	RSPAN configuration on Catalyst 9300. **Note**
• Capture (mirroring) and collection VLAN numbers. • Disk size.	Swiches only.
SPAN type	Catalyst 9x00 switches only. We recommend ERSPAN sessions for optimal traffic monitoring across purdue levels.
Extra capture IP address, prefix length, and VLAN number.	IR8340 routers only. The extra capture details define the connection between sensor and the AppGig virtual interface for capturing switched traffic.

Step 6 In the **Configure Active Discovery** page, choose between:
Choose from:

- Passive only
- Passive and Active Discovery and SEA

Packages that include SEA are available for Cisco Cyber Vision Sensors Release 5.3.0 and later.

Step 7 (If you use the Active Discovery sensor package) To use active discovery, provide the following details:

a. Collection interface

b. IP address

c. Prefix length

d. VLAN number

Step 8 Click **Deploy**.

What to do next

Sensor deployment can take up to 15 minutes to complete. You can track the progress of the deployment in the **Admin** > **Sensors** > **Management jobs** page.

Create sensor configuration template

Step 1 From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Templates**.

Step 2 Click **Add sensor template** to initiate the template configuration wizard.

Step 3 In the **Basic information** step, add a name and description for the template.

Step 4 In the **Protocol configuration** step, in the displayed table:

a) Choose the protocols you want to monitor by enabling or disabling the protocol entry.

b) Where applicable, enter the port assigned for the protocol traffic.

Step 5 (Optional) In the **Select sensors** step, choose any existing sensors you want to apply the template to.

Step 6 In the **Summary** step, review your template configuration.

Step 7 To create the template, click **Confirm**.

Manual sensor deployment

To manually deploy Cyber Vision sensors on supported devices, carry out these tasks.

1. Install and activate the sensor application, on page 15.
2. Create sensor provisioning package, on page 16.
3. Import sensor provisioning package into device, on page 16.
4. If you have installed the sensor application that includes Active Discovery, Enable Active Discovery on sensors, on page 17.

Install and activate the sensor application

Before you begin

To use Active Discovery, you must download and install the Cyber Vision sensor package that includes the feature. The name of the sensor package on Cisco Software Downloads indicates if Active Discovery is available in the package.

Install and activate the sensor application on the device.

Method	Steps to follow

Using device CLI	**a.** Copy the downloaded application package to the device internal memory.
	`copy scp://<username>@<scp-server-ip>/<path-to-file>/ccvsensor.tar bootflash:`
	b. Install the application.
	`device#app-hosting install appid <sensor-name> package bootflash:ccvsensor.tar`
	c. Activate the application.
	`device#app-hosting activate appid <sensor-name>`
	d. Start the application.
	`device#app-hosting start appid <sensor-name>`
	e. Configure the resource profile for the application on the device.

Using device Web UI	**a.** Log into the device Web UI. **b.** Choose **Configuration** > **Services** > **IOx**. **c.** Log into the IOx local manager using the device credentials. **d.** In the **Applications** tab, choose **Add New**. **e.** Enter a name for the sensor application. **f.** Click **Choose File** to select and add the sensor application file. **g.** After a few minutes, the sensor application entry is visibile in the **Applications** tab. Click **Activate**.

Method	Steps to follow
	h. To activate the application, you must enter configure the resource profile for the application on the device.

When the import is successful, in the Cyber Vision Center **Sensor Explorer** page, the sensor's health status updates to **Connected**.

Create sensor provisioning package

In this task, you create a provisoning package. Here, you define the device and the sensor that you want to connect to the Center and identify the traffic you want to monitor. After you create the package, you can deploy it in the target device using the Cyber Vision Center or the device CLI.

Before you begin

- Configure traffic monitoring in the device you want to deploy the sensor on.
- Gather the device details required in step 3 to complete this task.

Step 1 In the Cyber Vision Center, go to **Admin** > **Sensor** > **Sensor Explorer**.

Step 2 Click **New sensor** > **Manual Install**.

Step 3 In the **Configure provisioning package** page, enter the following device details:

a. Serial number.

b. Center collection IP, if you wish to use a different collection IP than what is already configured on the Center.

c. Gateway address.

d. An easily identifiable sensor label.

e. Define the capture mode by choosing the type of traffic you want the sensor to analyse.

f. Choose ERSPAN or RSPAN for traffic monitoring.

Step 4 In the next page, click **Download package**.
The package is downloaded to your local system, and the sensor is added to the **Sensor Explorer** page.

What to do next

Import the provisioning package on the target device, using the device Web UI or CLI.

Import sensor provisioning package into device

Import the sensor provisioning package that you downloaded into the device.

Method	Steps to follow
Using device CLI	**a.** In the device CLI, use the **conf t** command to enter the global configuration mode. **b.** Copy the provisioning package from the USB key to the application. `app-hosting data appid <sensor-app-name> copy usbflash0:sbs-sensor-config-<serialnumber>.zip sbs-sensor-config-<serialnumber>.zip`

Method	Steps to follow
Using device Web UI	**a.** Log into the device's Web UI. **b.** Choose **Configuration** > **Services** > **IOx**. **c.** Log into the Cisco IOx Local Manager by entering your device credentials. **d.** For the sensor application, click **Manage**. **e.** Choose **App-DataDir**. **f.** Click **Upload** to select and upload the provisioning file you downloaded.

When the import is successful, in the Cyber Vision Center **Sensor Explorer** page, the sensor's health status updates to **Connected**.

Enable Active Discovery on sensors

Before you begin

- Cisco IR1101 and IR1800 routers do not support Active Discovery.
- To use Active Discovery, you must download and install the Cyber Vision sensor package that includes the feature. The name of the sensor package on Cisco Software Downloads indicates if Active Discovery is available in the package. If you have already installed a sensor with a package that doesn't include Active Discovery and wish to use this feature, you must reinstall the sensor with the correct software.

Step 1 To enable Active Discovery on the sensor, go to **Admin** > **Active Discovery** > **Profiles.**.

Step 2 Click the profile you want to apply to the sensor, and click **Edit**.

Step 3 From the **Sensors** drop-down menu, choose the sensor you just enrolled to the Center.

Step 4 Click **Update**.

The profile runs on the sensor according to a configured schedule. To run the profile immediately, click the profile and click **Run Once**.

Bulk host onboarding and sensor deployment

Bulk host onboarding and sensor deployment allows you to onboard multiple routers to Cisco Cyber Vision in a single operation. It also enables you to deploy sensor applications to the onboarded routers using a streamlined, wizard-based workflow.

It offers the following advantages:

- Streamlines the onboarding of multiple routers and deployment of sensor applications.
- Minimizes manual effort for network administrators and IT operations engineers.
- Improves operational efficiency through automated checks and simultaneous deployment.

Bulk host onboarding and sensor deployment is especially useful for large-scale deployments that require simultaneous onboarding of multiple hosts and deployment of sensor applications.

This process involves two key steps:

- Onboard hosts to Cisco Cyber Vision

- Deploy sensors to the hosts that have been successfully onboarded.

Table 2: Feature History Table

Feature	Release Information	Feature Description
Bulk host onboarding and sensor deployment	Release 5.4.x	Bulk host onboarding and sensor deployment in Cisco Cyber Vision lets you add multiple routers at once and deploy sensor applications to them using a guided, wizard-based workflow. It automates reachability and readiness checks, reduces manual effort, and accelerates large-scale rollouts.

Bulk onboarding and sensor deployment capabilities

The bulk onboarding and sensor deployment feature provides these capabilities:

- Adding multiple routers simultaneously using a CSV file or manual entry.
- Instantly verifying, along with other technical checks, that each router is reachable, has IOX enabled, and possesses adequate storage for sensor deployment.
- Rapidly identifying devices that are ready for deployment, eliminating manual verification.
- Enabling sensor deployment to ready routers with a streamlined, wizard-based workflow.
- Pre-selecting default settings for typical deployment scenarios, minimizing configuration overhead.
- Offering retry options for deployment failures to maximize successful sensor rollout.

Supported devices

The bulk onboarding and sensor deployment feature currently supports the following devices:

- Cisco IR1800 routers
- Cisco IR1101 routers

Note

Other platforms will be supported in the future.

Onboard hosts to Cisco Cyber Vision

Add new hosts to Cisco Cyber Vision to enable automated sensor deployment and monitoring.

Onboarding hosts prepares network devices for sensor application deployment.

Before you begin

Ensure these requirements are met:

- IOS XE version 17.9 or higher is installed on the target hosts.

- IOx services are enabled and running on the target hosts.
- Web server is enabled on the target host.
- NAT rules are set up to access the Cisco Cyber Vision collection interface.
- Encapsulated Remote SPAN (ERSPAN) interfaces are set up for remote monitoring.
- The hosts' time is synchronized with the Center or a valid NTP server.

  For more details, review the Initial configuration.

Follow these steps to onboard hosts:

Step 1 Go to **Cyber Vision New UI > Configuration > Sensor Management**.

This section is divided into two tabs: **Hosts** and **Sensors**. The **Hosts** tab lists all onboarded platforms, while the **Sensors** tab displays your deployed sensor apps. Note that the **Sensors** view also includes apps deployed via the Sensor Management extension from the Classic UI.

Step 2 Click **Start onboarding**.

Step 3 Choose an onboarding method. To onboard multiple hosts, choose **Use CSV file (recommended)** or **Input details manually** to type them individually.

Step 4 If using a CSV file:

a) Click the **Use .CSV file (recommended)** radio button.
b) (Optional) Click the **Download sample** link to get a template for the CSV file.
c) Upload your CSV file by clicking within the **Click or drag file to this area to upload** box.

Step 5 If manually inputting host details (limited to a maximum of 10 hosts):

a) Click **Input details manually**.
b) Enter the required host details in the fields that appear.

Step 6 (Optional) Enter the global credentials that are common to all hosts in the **Global Credentials** section.

If you have not entered the credentials in the .CSV file, then the global credentials will be used.

Step 7 To complete the onboarding process, click **Onboard**.

The hosts are added to Cisco Cyber Vision and are ready for sensor deployment. If you want to add more hosts, click **Onboard host**.

What to do next

Deploy sensor apps on the ready hosts.

Deploy sensor apps on ready hosts

Install sensor applications on the hosts that have been successfully onboarded and validated.

You can deploy sensor applications only on hosts marked as "Ready" after the onboarding process. A wizard-based workflow streamlines the deployment process.

Before you begin

- Ensure that the target hosts are successfully onboarded.
- Check the "Host status" column for the routers you intend to deploy to. They should display "Ready".

- Note any hosts listed under "Wrong Credentials," "Unreachable," or "Not Ready," as these will require troubleshooting before deployment can proceed.

Follow these steps to deploy sensor apps to routers:

Step 1 Go to the **Cyber Vision New UI > Configuration > Sensor Management**.

Step 2 To deploy sensor apps on specific set of hosts, select the hosts from the table that appears, and click **Deploy**. You can filter the list of hosts by using the search criteria.

Step 3 To deploy sensor apps on all hosts whose status is "Ready", select the check box before the **Label** column and click **Deploy**.

Step 4 On the **Choose host type** screen, select "Routers" and click **Continue**.

Step 5 On the **Choose deployment mode** screen, select "Simple" and click **Continue**.

Step 6 On the **Simple deployment** screen, use the default values, or enter the required details and click **Deploy**.

When the deployment is successful, the details of the sensor applications are displayed on the **Sensors** page. To uninstall or retry sensor installation, use the **Sensor Management > Sensors** page. These operations are unavailable for sensors deployed using the Classic UI or other methods.

What to do next

Review deployment status and troubleshoot any failed installations as needed. To retry the deployment, select hosts from the list and click **Retry Deployment**.

Sensor deployment configuration examples

This chapter provides examples of essential network configurations required to deploy Cisco Cyber Vision sensors on supported devices. Understanding these configurations is crucial for ensuring proper communication between the Center and the deployed sensors, as well as for effective traffic monitoring.

In these examples:

- VLAN 49 is the collection VLAN.
- VLAN 2508 is the mirroring VLAN.
- 192.168.49.40 with the subnet mask 255.255.255.0 is the SVI management address, typically configured on the collection VLAN or on the network gateway.
- 169.254.x.x IP range with the subnet mask 255.255.255.252 is used to configure ERSPAN origins and destinations.

The configuration examples provided in this guide demonstrate deploying sensors in Cisco Catalyst IE3x00, Cisco Catalyst IE9x00, and Cisco Catalyst 9x00 switches, in the following deployment scenarios:

- Center and sensors are in the same network.
- Center and sensors are in different networks.
- (IE3x00 switches only) Platform and sensors are in different networks, requiring L3NAT-IOx.

For Cisco Catalyst 9300, specific examples are provided for ERSPAN and RSPAN configurations.

There are some important differences in sensor configurations, based on the network deployment setup and the devices on which the sensor is deployed.

Switch series	Center and sensors in the same network	Center and sensors in different networks
Cisco Catalyst IE3x00	Use the `format-erspan` command to encapsulate SPAN or RSPAN traffic in ERSPAN. The encapsulated traffic can then be sent to a destination address.	• Use the `format-erspan` command to encapsulate SPAN or RSPAN traffic in ERSPAN. The encapsulated traffic can then be sent to a destination address. • Use `ip route` command to define a static route on the switch to reach the Cyber Vision Center's management network.
Cisco Catalyst IE9x00	None	Use `ip route` command to define a static route on the switch to reach the Cyber Vision Center's management network.
Cisco Catalyst 9x00	Use the `ip routing` command to enable Layer 3 routing capabilities on the switch, which is a prerequisite for ERSPAN to function.	Use the `ip routing` command to enable Layer 3 routing capabilities on the switch, which is a prerequisite for ERSPAN to function.

Center and sensor on the same network

Cisco Catalyst IE3x00 Series Switches

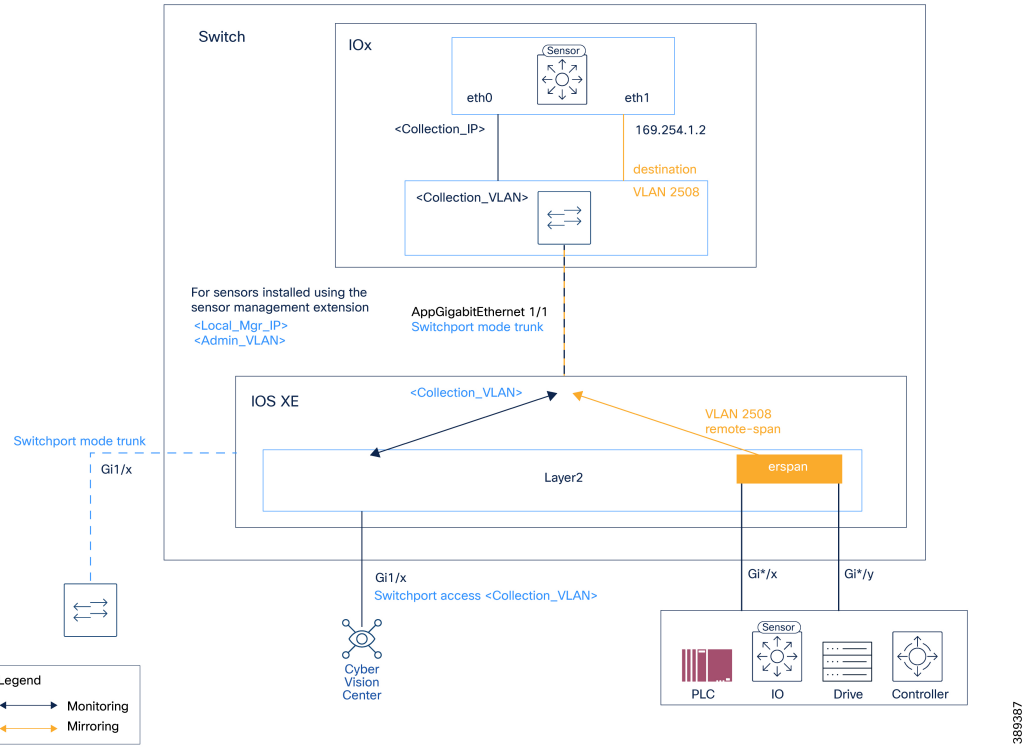
This example demonstrates deploying Cyber Vision sensors when the Center and Cisco Catalyst IE3x00 switches are in the same network:

Note

By default, trunk ports use VLAN 1 for untagged traffic. If the sensor must communicate with the Center on VLAN 1, to avoid conflicts, change the native VLAN to a different ID using the **switchport trunk native vlan xxx** command.

```
configure terminal
vtp mode off
vlan 2508
name mirror_vlan
remote-span
exit
interface AppGigabitEthernet 1/1
switchport mode trunk
monitor session 1 source interface Gi1/7-10 both
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
vlan 49
name CyberVision_Collect
exit
interface vlan49
ip address 192.168.49.40 255.255.255.0
exit
interface GigabitEthernet1/3
description To_Cybervision_center_Eth1
switchport access vlan 49
switchport mode access
end
```

Figure 2: Example architecture when the Center and IE3x00 switches are in the same network



Cisco Catalyst IE9x00 Series Switches

This example demonstrates deploying Cyber Vision sensors when the Center and Cisco Catalyst IE9x00 switches are in the same network:

```
configure terminal
ip routing
vlan 2508
exit
interface vlan2508
ip address 169.254.1.1 255.255.255.252
no shutdown
exit
interface AppGigabitEthernet 1/0/1
switchport mode trunk
exit
monitor session 1 type erspan-source
source interface Gi1/0/7 - 10 both
no shutdown
destination erspan-id 2
mtu 9000
ip address 169.254.1.2
origin ip address 169.254.1.1
exit
exit
interface GigabitEthernet1/0/3
switchport access vlan 49
no shutdown
exit
```

```
exit
write mem
```

Cisco Catalyst 9x00 Series Switches

This section provides examples of deploying Cyber Vision sensors when the Center and Catalyst IE9x00 switches are in the same network.

This example demonstrates ERSPAN configuration:

```
configure terminal
ip routing
vlan 2508
exit
interface vlan2508
ip address 169.254.1.1 255.255.255.252
no shutdown
exit
interface AppGigabitEthernet 1/0/1
switchport mode trunk
exit
monitor session 1 type erspan-source
source interface Gi1/0/7 - 10 both
no shutdown
destination erspan-id 2
mtu 9000
ip address 169.254.1.2
origin ip address 169.254.1.1
exit
exit
interface GigabitEthernet1/0/3
switchport access vlan 49
no shutdown
exit
exit
write mem
```

This example demonstrates RSPAN configuration:

```
configure terminal
vlan 2508
name mirror_vlan remote-span
exit
interface AppGigabitEthernet 1/1
switchport mode trunk
monitor session 1 source interface Gi1/0/7 - 10 both
monitor session 1 destination remote vlan 2508
vlan 49
name CyberVision_Collect
exit
interface vlan49
ip address 192.168.49.40 255.255.255.0
exit
interface GigabitEthernet1/3
description To_Cybervision_center_Eth1
switchport access vlan 49
switchport mode access
end
```

Center and sensors on different networks

Catalyst IE3x00 Series Switches

This example demonstrates deploying Cyber Vision sensors when the Center and Cisco Catalyst IE3x00 switches are in different networks:

Note

By default, trunk ports use VLAN 1 for untagged traffic. If the sensor must communicate with the Center on VLAN 1, to avoid conflicts, change the native VLAN to a different ID using the **switchport trunk native vlan xxx** command.

```
configure terminal
vtp mode off
vlan 2508
name mirror_vlan remote-span
exit
interface AppGigabitEthernet 1/1
switchport mode trunk
monitor session 1 source interface Gi1/7-10 both
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
Vlan 10
name Management_Vlan
!
Vlan 49
name CyberVision_Collect
!
interface Vlan49
ip address 192.168.49.40 255.255.255.0
!
interface Vlan10
ip address 172.16.1.250 255.255.255.0
!
interface GigabitEthernet1/3
description To_Router
switchport mode Trunk
switchport trunk allowed vlan 49,10
!
ip route 10.2.1.0 255.255.255.0 172.16.1.254
```

Catalyst IE9x00 Series Switches

This example demonstrates deploying Cyber Vision sensors when the Center and Cisco Catalyst IE9x00 switches are in different networks:

```
configure terminal
ip routing
vlan 2508
exit
interface Vlan2508
ip address 169.254.1.1 255.255.255.252
no shutdown
exit
interface AppGigabitEthernet 1/0/1
switchport mode trunk
exit
monitor session 1 type erspan-source
source interface Gi1/0/7 - 10 both
no shutdown
destination erspan-id 2 mtu 9000 ip address 169.254.1.2 origin ip address 169.254.1.1
exit
exit
Vlan 10
name Management_Vlan
!
Vlan 49
```

```
name Collection_Vlan
!
interface Vlan10
ip address 172.16.1.250 255.255.255.0
!
interface Vlan49
ip address 192.168.49.40 255.255.255.0
!
interface GigabitEthernet1/0/3
description To_Router_center_Eth1
exit
ip route 10.2.1.0 255.255.255.0 172.16.1.254
exit
write mem
```

Catalyst 9x00 Series Switches

This section provides examples of deploying Cyber Vision sensors when the Center and Catalyst 9x00 switches are in different networks.

This example demonstrates ERSPAN configuration:

```
configure terminal
ip routing
vlan 2508
exit
interface Vlan2508
ip address 169.254.1.1 255.255.255.252
no shutdown
!
interface AppGigabitEthernet 1/0/1
switchport mode trunk
!
monitor session 1 type erspan-source
source interface Gi1/0/7 - 10 both
no shutdown
destination erspan-id 2 mtu 9000 ip address 169.254.1.2 origin ip address 169.254.1.1
!
!
Vlan 10
name Switch_Management_Vlan
!
Vlan 49
name NATed_CyberVision_Collect
interface Vlan49
ip address 192.168.49.40 255.255.255.0
!
interface Vlan10
ip address 172.16.1.250 255.255.255.0
!
interface GigabitEthernet1/0/3
description To_Router_center_Eth1
switchport mode trunk
switchport trunk allowed vlan 49,10
```

This example demonstrates RSPAN configuration:

```
configure terminal
vlan 2508
name mirror_vlan remote-span
!
interface AppGigabitEthernet 1/1
switchport mode trunk
!
monitor session 1 source interface Gi1/0/7 - 10 both
```

```
monitor session 1 destination remote vlan 2508
!
Vlan 10
name Switch_Management_Vlan
!
Vlan 49
name NATed_CyberVision_Collect
interface Vlan49
ip address 192.168.49.40 255.255.255.0
!
interface Vlan10
ip address 172.16.1.250 255.255.255.0
!
interface GigabitEthernet1/3
description To_Router_center_Eth1
switchport mode trunk
switchport trunk allowed vlan 49,10
```

(IE3x00 only) Platform and sensors in different networks

This example demonstrates deploying Cyber Vision sensors when Cisco Catalyst IE3x00 switches are in multiple networks.

Note

By default, trunk ports use VLAN 1 for untagged traffic. If the sensor must communicate with the Center on VLAN 1, to avoid conflicts, change the native VLAN to a different ID using the **switchport trunk native vlan xxx** command.

```
configure terminal
vtp mode off
vlan 2508
name mirror_vlan remote-span
exit
Vlan 49
name NATed_CyberVision_Collect
interface Vlan49
ip address 192.168.49.40 255.255.255.0
Vlan 2507
name CyberVision_Collect
interface Vlan2507
ip address 169.254.0.1 255.255.255.252
interface AppGigabitEthernet 1/1
switchport mode trunk
monitor session 1 source interface Gi1/7-10 both
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
interface GigabitEthernet1/3
description To_Router_center_Eth1
switchport mode access
switchport access vlan 49
!
l3nat-iox
app-ip 169.254.0.2
svi-ip 192.168.49.40
app-name CCV-ONPREM
server-ip 10.2.1.100
```