Deploy Cisco Cyber Vision Sensor on Switches and Routers

Cisco Cyber Vision
Updated September 8, 2026

Topics included

1 Cisco Cyber Vision sensors....4
Cisco Cyber Vision sensor overview....5
Supported switches and routers....6
Deploying Cyber Vision sensors....7

2 Deploy Cisco Cyber Vision sensors....10
Prepare switches and routers....11
Setting up OT traffic monitoring....12
Configure traffic monitoring on the switches....13
Configure traffic monitoring on routers....17
Deploying sensor applications....19
Bulk host onboarding and sensor deployment....22
Provision sensors using sensor management extension....27
Manual Sensor Installation....30

3 Sensor deployment examples....40
Sensor deployment configuration examples....41
Center and sensor on the same network....42
Center and sensors on different networks....44
(IE3x00 only) Platform and sensors in different networks....47

1 Cisco Cyber Vision sensors

Topics:

- Cisco Cyber Vision sensor overview
- Supported switches and routers
- Deploying Cyber Vision sensors

Explains Cisco Cyber Vision sensors capabilities and features, lists compatible switches and routers, and guides users through sensor deployment procedures to optimize network monitoring and protection.

Cisco Cyber Vision sensor overview

Introduces Cisco Cyber Vision sensors by outlining their deployment on Cisco network devices, methods for analyzing OT traffic using deep packet inspection and Active Discovery, identification and transmission of industrial assets and security events, and details on communication protocols between sensors and Cyber Vision Center.

A Cisco Cyber Vision sensor is an application that:

1. Gathers and analyzes industrial network traffic using deep packet inspection.
2. 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?

- 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.
>
> For a list of supported protocols, refer the Cisco Cyber Vision Protocols Data Sheet.

- 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)

Port	Message type
TCP 10514	Secure syslogs

Note

From Cyber Vision Release 5.4.0, this port is not used for sensor communications. Secure syslogs are also sent using TCP 5671.

Supported switches and routers

Outlines the switches and routers that support Cyber Vision sensor deployment, including Cisco Catalyst, IE Rugged, and IR Rugged Series platforms, and provides references for supported IOS XE versions and platform compatibility details.

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 Switches
  - Cisco Catalyst 9300 Series Switch
  - Cisco Catalyst 9300X Series Switch
  - Cisco Catalyst 9400 Series Switch
- Heavy Duty and Rugged IE 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 IE3500 Rugged Series
  - Cisco IE3500 Heavy Duty Series
  - 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

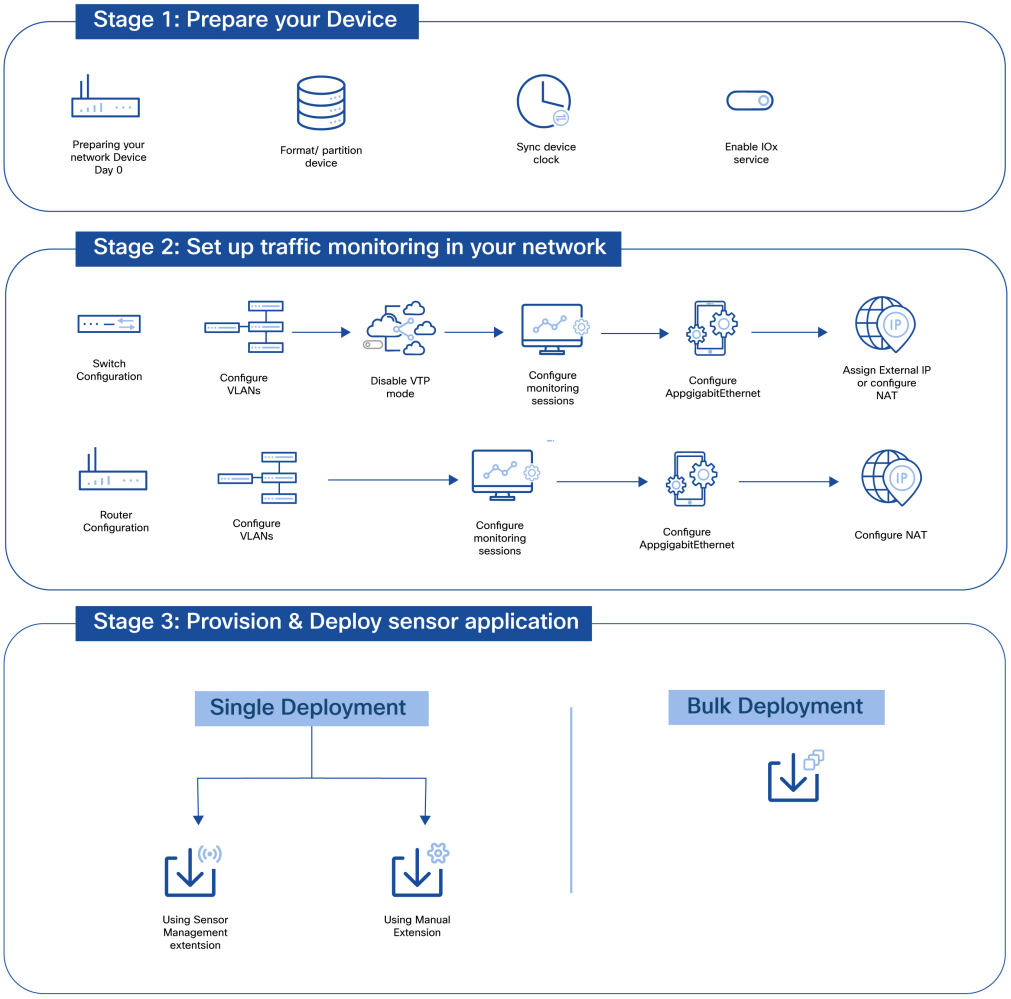
Outlines the multi-stage process for deploying Cyber Vision sensors, including preparing switches and routers, configuring traffic monitoring, and provisioning sensor applications for active discovery and packet capture on single or multiple devices.

Summary

Deploying Cyber Vision 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



rect 31, 33, 660, 187 Prepare switches and routers
rect 40, 243, 662, 332 Configure traffic monitoring on switches
rect 38, 345, 661, 450 Configure traffic monitoring on routers
rect 98, 515, 371, 743 Deploy a sensor on a device
rect 437, 509, 612, 715 Deploy sensors on multiple devices

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. For Cyber Vision Release 5.5 and earlier, 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.

   Note

   Starting with Cisco Cyber Vision Release 5.6.0, the sensor-management extension is no longer available in the classic UI for deploying sensor applications. Sensors migrated from the classic UI Sensor Management extension are fully integrated into the sensor-host model available in the new UI **Sensor Management** page. However, manual sensor deployment, Docker sensor deployment, and Sensor VM deployment remain available in classic UI.

   Use the deployment method that corresponds to your Cyber Vision version:

   - Cyber Vision 5.6 and later: Use the bulk onboarding and sensor deployment feature in the new UI (**Configuration** > **Sensor Management**).
   - Cyber Vision 5.5 and earlier: Use the Sensor Management extension in the classic UI (**Admin** > **Sensors** > **Sensor Explorer**).

2 Deploy Cisco Cyber Vision sensors

Topics:

- Prepare switches and routers
- Setting up OT traffic monitoring
- Deploying sensor applications

Guides users through the complete process of deploying Cisco Cyber Vision sensors, covering prerequisite switch and router preparation, setting up traffic monitoring for OT networks, and provisioning sensors through both automated sensor management tools and manual installations.

Prepare switches and routers

Outlines the preparation of switches and routers for Cyber Vision Sensor deployment, including storage configuration, clock synchronization, IOx service enablement, verification steps, and prerequisite requirements.

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:

- Catalyst 9x00 switches must have Cisco DNA Advantage licenses.
- 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.

Procedure

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`.

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`

3. Use **ntp server <server-ip-address>** to add an NTP server.
4. Enable IOx service:

```
configure terminal
iox
exit
```

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

Guides you through setting up OT traffic monitoring on Cisco switches and routers, including VLAN configuration, VTP management, SPAN-based traffic mirroring, AppGigabitEthernet setup, and secure communication via NAT and external IPs for integration with Cyber Vision Center.

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 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 IE3300 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

Outlines the procedures for configuring traffic monitoring on Cisco switches, including VLAN mirroring and collection, monitoring session setup, AppGigabitEthernet port configuration, external communication with NAT or switchport access, and saving settings for integration with the Cyber Vision sensor.

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.

Procedure

1. Use the `configure terminal` command to enter the global configuration mode.
2. (For IE3300 and IE3400 devices) Use the `vtp mode off` command to disable VTP.
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`

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)# interface vlan 2508 switch(config)# ip address 169.254.1.1 255.255.255.252 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)# interface vlan 2508 switch(config)# ip address 169.254.1.1 255.255.255.252 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)# interface vlan 2508 switch(config)# ip address 169.254.1.1 255.255.255.252 switch(config)#monitor session 1 type erspan-source switch(config)#source interface Gi1/11 both switch(config)#no shutdown switch(config)#header-type 3 !Use this command for Cyber Vision Sensors release 5.5.0 and later, on IE9300 and Catalyst 9x00 switches switch(config)# destination switch(config)#i erspan-id 2 switch(config)# ip address <erspan-destination-ip-address> switch(config)#mtu 9000 switch(config)#origin ip address <origin-ip-address> switch(config)#exit

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)#switchport trunk allowed vlan <collection-vlan>,<mirror-vlan>,<monitored-vlan>`
	`switch(config)#switchport trunk native vlan <approved-native-vlan>`
	`switch(config)#no shutdown`
	`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 allowed vlan <collection-vlan>,<mirror-vlan>,<monitored-vlan>`
	`switch(config)#switchport trunk native vlan <approved-native-vlan>`
	`switch(config)#no shutdown`
	`switch(config)#exit`

Note

In IE9300, Catalyst 9300 and Catalyst 9400 switches, if you want to use VLAN1 for sensor communication, assign a different VLAN to carry untagged traffic by using the command `switch(config)#switchport trunk native vlan <existing-vlan-ID>`.

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`
	`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	`Switch#enable`
	`Switch#configure terminal`
	`Switch(config)#ip access-list standard CCV-NAT`
	`Switch(config-std-nacl)#permit <sensor-collection-subnet> <wildcard-mask>`
	`Switch(config-std-nacl)#exit`
	`Switch(config)#interface <inside-interface>`
	`Switch(config-if)#ip address <inside-ip> <mask>`
	`Switch(config-if)#ip nat inside`
	`Switch(config-if)#exit`
	`Switch(config)#interface <outside-interface>`
	`Switch(config-if)#ip address <outside-ip> <mask>`
	`Switch(config-if)#ip nat outside`
	`Switch(config-if)#exit`
	`Switch(config)#ip nat inside source list CCV-NAT interface <outside-interface> overload`
	`Switch(config)#ip route 0.0.0.0 0.0.0.0 <outside-next-hop>`
	`Switch(config)#end`

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

Configure traffic monitoring on routers

Guides you through configuring traffic monitoring on supported routers, including setting up VLANs, mirroring switched port traffic on IR8340, ERSPAN monitor sessions for switching and routing ports, and NAT configuration for sensor application connectivity to Cyber Vision Center.

Of the supported routers, IR8340 is unique in hosting switched ports. The IR8340 supports switched-port traffic monitoring and uses three distinct application paths:

- VirtualPortGroup 0 (VPG0) is the routed ERSPAN capture path.
- VirtualPortGroup 1 (VPG1) is the collection and NAT path to the Cyber Vision Center.
- AppGigabitEthernet 0/1/1 is the switched-port capture path.

If you want to monitor traffic from switched ports on IR8340, begin with step 2.

The IR1101 and IR1800 do not support the switched-port AppGigabitEthernet path. For these routers, begin with the routed VirtualPortGroup configuration in Step 3.

Procedure

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

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
   ```

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`

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

Guides you through deploying Cyber Vision sensor applications across supported switches and routers, detailing automated and manual installation methods, provisioning, optional Active Discovery, and sensor management to enable real-time threat detection and network visibility.

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.

Table 1: Feature History

Feature	Release Information	Feature Description
The Sensor Management extension removal.	Release 5.6.0	When the Cisco Cyber Vision system is updated to version 5.6.0 and rebooted, the system detects the legacy sensor-management extension data and initiates migration to the sensor-host model in new UI. The sensor management extension is removed, and the sensor identity and configuration are preserved as they transition to the sensor-host model in the new UI.

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

> **Note**
>
> Starting with release 5.6.0, use the **Sensor Management** page in the New UI to deploy sensor applications to supported switches and routers. The **Install via extension** option is removed from Classic UI. However, manual sensor deployment, Docker sensor deployment, and Sensor VM deployment remain available in Classic UI.
>
> Sensors migrated from the Classic UI Sensor Management extension appear in the New UI with a status of Deployment successful and are no longer labeled Externally managed.

- Onboarding and validating hosts, and then deploying sensors to each host.
- 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.

FIPS-compliant Cisco Cyber Vision (Release 5.6.0 and later) does not support bulk sensor deployment. To deploy sensor on a FIPS-compliant Cisco Cyber Vision Center, use the manual deployment feature in the classic UI.

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:

   - Device serial number (required if you are not using the Sensor Management Extension in release 5.5.x or the Sensor deployment option in the New UI for release 5.6.0).
   - 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.

   > **Note**
   >
   > Starting from release 5.6.0 onwards, the sensor can be deployed, managed and monitored from the new UI **Configuration** > **Sensor management**. Classic UI continues to support manual sensor deployment, Docker sensor deployment, and Sensor VM deployment.

Result

When the sensor application is successfully configured and deployed, the sensor captures and analyzes 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.

Bulk host onboarding and sensor deployment

Explains how bulk host onboarding and sensor deployment features streamline adding multiple hosts and deploying sensor applications in Cisco Cyber Vision.

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

It offers the following advantages:

- Streamlines the onboarding of multiple hosts 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
The Sensor Management extension removal.	Release 5.6.0	The system detects the legacy sensor-management extension data and initiates migration to the sensor-host model in new UI. The sensor management extension is removed, and the sensor identity and configuration are preserved as they transition to the sensor-host model in the new UI.
Bulk host onboarding and sensor deployment on switches	Release 5.5.x	Enables you to onboard multiple switches and deploy sensor applications using a guided, wizard-based workflow. Supported switches: • Cisco Catalyst IE3x00 switches • Cisco Catalyst 9x00 switches • Cisco Catalyst IE9300 Rugged Series Switches
Bulk host onboarding and sensor deployment on routers	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 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

Outlines bulk onboarding and sensor deployment capabilities, including adding multiple hosts, automated readiness checks, streamlined deployment workflows, default configurations, retry options, and supported Cisco routers and switches.

The bulk onboarding and sensor deployment feature provides these capabilities:

- Adding multiple hosts simultaneously using a CSV file or manual entry.
- Instantly verifying, along with other technical checks, that each host 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 hosts 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
- Cisco Catalyst IE3x00 switches
- Cisco Catalyst 9x00 switches
- Cisco Catalyst IE9300 Rugged Series Switches

> **Note**
>
> Other platforms will be supported in the future.

Onboard hosts to Cisco Cyber Vision

Provides instructions for onboarding network hosts to Cisco Cyber Vision, including prerequisites, CSV and manual entry options, credential management, UI navigation, readiness checks, and preparing hosts for automated sensor deployment and monitoring.

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

Onboarding hosts prepares network devices for sensor application deployment. The CSV file can include both switch and router IP addresses and credentials.

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.

  Cisco Cyber Vision runs readiness checks to determine whether each host is ready for sensor deployment. If a host is not yet ready, you can use the **More Actions > Verify readiness** menu for that host to run the checks again after correcting any issues.

Follow these steps to onboard hosts:

Procedure

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. The **Sensors** view also includes apps deployed via the **Sensor Management extension** from the Classic UI.

2. Click **Onboard host**.

3. Choose an onboarding method. To onboard multiple hosts, choose **Use CSV file (recommended)** or **Input details manually** to type them individually.
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.
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.
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.
7. To complete the onboarding process, click **Onboard**.

The hosts are added to Cisco Cyber Vision. If you want to add more hosts, click **Onboard host**.

What to do next

Deploy sensor apps on the ready hosts.

Deploy sensor apps to hosts

Provides instructions for deploying and configuring sensor applications on onboarded, ready hosts—including routers and switches—using simple or advanced deployment modes, and outlines prerequisites, step-by-step procedures, deployment options, and post-deployment management tasks.

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

You can deploy sensor applications only on hosts marked **Ready** after onboarding. For switches, choose between two configuration types:

- **Simple**: Uses the default deployment values displayed by the New UI for the selected host type.
- **Advanced**: Uses the host list and collection-interface values from the CSV file. If supported parameters are omitted from the CSV file, the New UI uses the default deployment values for the selected host type.

Before you begin

- Ensure that the target hosts are successfully onboarded.
- Ensure that the host can reach Cisco Cyber Vision Center through the interface configuration used for sensor deployment. In particular, the collection interface, and any other interface specified in the deployment configuration, must be connected to the correct network and have valid addressing and routing. If an interface is configured on the wrong network or with incorrect parameters, the sensor will not be able to connect to the Center.
- If you plan to use the advanced workflow for switches, ensure your CSV file is ready. The file must include the host list and collection interface parameters. Capture interface parameters are optional; if they are omitted, the default values displayed by the New UI for the selected host type are used.
- Ensure that you deploy sensor apps to only one host type—routers or switches—at a time.

Follow these steps to deploy sensor apps:

Procedure

---

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

2. Select the target hosts for sensor application installation, then click **Deploy sensor**.
3. For routers:
   a) Select **Simple** on the **Choose deployment mode** screen, and then click **Continue**.
   b) On the **Simple Deployment** screen, either keep the default values or enter the required details.
4. For switches, do one of the following:
   - To use the default configuration settings, select **Simple** on the **Choose deployment mode** screen, and then click **Continue**. On the **Simple Deployment** screen, enter the required details.

     Table 3: Simple Deployment fields

Field	Description
Use default values	When checked, the system automatically applies standard network configurations and bypasses the need for manual entry.
Collection Interface	Specifies the network parameters for the collection interface, including **IP address**, **Prefix**, **Gateway**, and **virtual port group number**.
Capture Interface	Specifies the network parameters for the capture interface, including **IP address**, **Prefix**, and **virtual port group number**.
Sensor Template	Selects the configuration profile to be applied to the sensor.
Capture Mode	Sets the performance profile (e.g., Optimal) for data traffic capture.

   - To provide host and collection-interface parameters through a CSV file, select **Advanced** on the **Choose deployment mode** screen and upload your CSV file. Any supported parameters omitted from the CSV file use the default values displayed by the New UI for the selected host type.
5. Click **Deploy**.

When the deployment is successful, the details of the sensor applications are displayed on the **Sensor Management > Sensors** page. To uninstall or retry sensor installation, use the **Sensors** page. Starting with Release 5.6.0, you can manage and monitor sensors apps migrated from the Classic UI Sensor Management extension to the sensor-host model from this page.

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**.

After deploying the sensor application, configure the sensor settings as needed:

- Configure the sensor capture mode in the classic UI **Sensor Explorer** page. Refer **Set a Capture Mode** in the *Cisco Cyber Vision Classic UI Administration Guide, Release 5.6.0*
- Configure Snort to enable or disable intrusion detection.
- Configure Active Discovery and specify the collection interface or additional network interfaces as required.
- Before configuring Secure Remote Access (SRA), ensure that Active Discovery is enabled on the sensor. You can then enable or disable SRA and select the required connection method.

For detailed instructions on configuring Snort, Active Discovery, and Secure Remote Access on a sensor, refer the *Cisco Cyber Vision New UI Administration Guide, Release 5.6.0*.

Provision sensors using sensor management extension

Outlines installing the sensor management extension, adding device credentials, and provisioning sensors using the extension.

> **Note**
>
> These steps apply to Cisco Cyber Vision release 5.5.x and earlier, where the sensor management extension is used for sensor installation and management.
>
> Starting with Release 5.6.0, the **Install via extension** option is no longer available in Classic UI. Sensor deployment and management for switches and routers have transitioned to the New UI **Sensor Management** page. Sensors apps migrated from the Classic UI Sensor Management extension appear in the New UI with a status of Deployment successful. They are integrated into the New UI sensor-host model, where you can manage and monitor them.

Procedure

1. Install sensor management extension on page 27.
2. Add global device credentials on page 27.
3. Install sensors using sensor management extension on page 28

Install sensor management extension

Provides instructions for installing the sensor management extension in Cisco Cyber Vision Center, including importing, updating, and removing extension files.

Procedure

1. From the Cisco Cyber Vision Center menu, choose **Admin** > **Extensions**.
2. Click **Import a new extension file**.
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

Guides you through defining and updating global device credentials with Level 15 access for sensor management workflows in Cisco Cyber Vision Center, ensuring appropriate access to deployed sensors and the device Web UI.

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.

Procedure

1. From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Choose **Manage Cisco devices** > **Manage credentials**.
3. To save the credentials, click **Update**.

Install sensors using sensor management extension

Guides you through installing sensors with the sensor management extension in Cyber Vision Center, including prerequisites, device configuration, capture and collection settings, configuration templates, Active Discovery options, deployment steps, and monitoring sensor installation progress.

Before you begin

- Install sensor management extension on page 27.
- Add global device credentials on page 27.
- Define capture and collection details for network . For instructions, see Setting up OT traffic monitoring on page 12. 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.

Procedure

1. From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click **New sensor** > **Install via extension** to initate the installation wizard.
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.
4. Click **Connect**.

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.** • **Capture (mirroring) and collection prefix lengths.** • **(Optional) Collection gateway, if the Center and the sensor application are in different subnets.**	All switches and routers **Note** RSPAN configuration on Catalyst 9300.
• **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.

6. In the **Configure Active Discovery** page, choose between:
   - 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.
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
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

Guides you through creating a sensor configuration template in Cisco Cyber Vision Center, including specifying basic details, protocol settings, applying templates to sensors, and confirming the template setup.

Procedure

1. From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Templates**.
2. Click **Add sensor template** to initiate the template configuration wizard.
3. In the **Basic information** step, add a name and description for the template.
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.
5. (Optional) In the **Select sensors** step, choose any existing sensors you want to apply the template to.
6. In the **Summary** step, review your template configuration.
7. To create the template, click **Confirm**.

Manual Sensor Installation

Manual sensor installation deploys the Cisco Cyber Vision sensor application directly on a supported switch or router by using IOx Local Manager or the device CLI.

Manual sensor installation deploys the Cisco Cyber Vision sensor application directly on a supported IOS XE switch or router by using the device CLI or IOx Local Manager.

Use manual installation when the Cisco Cyber Vision Center cannot deploy the application through the sensor management extension, such as when the Center cannot reach the device management interface, when network policy blocks extension-based deployment, or when you need to test a single device before a larger rollout.

Manual installation does not replace device preparation. Before you manually install the sensor application, configure the device storage when required, synchronize the device clock, enable IOx, and configure OT traffic monitoring. The sensor must receive mirrored traffic and must be able to communicate with the Cisco Cyber Vision Center collection interface.

> **Note**
>
> If you install a sensor package that does not include Active Discovery and later decide to use Active Discovery, reinstall the sensor with the correct package.

Table 4: Manual Installation Methods

Method	Use this method when	What you do
IOx Local Manager	You can reach the device Web UI and prefer a guided interface for resource and interface configuration.	Upload the sensor application archive, configure the resource profile and network interfaces, start the application, create a provisioning package in Cisco Cyber Vision, and upload the provisioning package to the application data directory.

Method	Use this method when	What you do
Device CLI	You need repeatable commands, remote terminal access, or cannot use the device Web UI.	Configure the hosted application, install the sensor archive from device storage, activate and start the application, create a provisioning package in Cisco Cyber Vision, and copy the provisioning package into the hosted application.

Table 5: Manual Installation Packages

Device family	Standard sensor package	Active Discovery package
Cisco IR1101 and Cisco IR1800 routers	CiscoCyberVision-IOx-aarch64-<version>.tar	Not supported on Cisco IR1101 and Cisco IR1800.
Cisco IR8340 routers	CiscoCyberVision-IOx-x86-64-<version>.tar	CiscoCyberVision-IOx-Active-Discovery-x86-64-<version>.tar
Cisco IE3300 10G, IE3400, IE9300, and IE3500 switches	CiscoCyberVision-IOx-aarch64-<version>.tar	CiscoCyberVision-IOx-Active-Discovery-aarch64-<version>.tar
Cisco Catalyst 9x00 switches	CiscoCyberVision-IOx-x86-64-<version>.tar	CiscoCyberVision-IOx-Active-Discovery-x86-64-<version>.tar

Manual Sensor Installation Workflow

The manual sensor installation workflow describes how to install, provision, validate, and optionally enable Active Discovery for a Cisco Cyber Vision sensor application.

Manual sensor installation separates application deployment from Center-side provisioning.

You install the IOx application on the device first, then use Cisco Cyber Vision to create a provisioning package that enrolls the sensor with the Center.

Summary

The workflow starts with device preparation and ends when the sensor is connected in Cisco Cyber Vision.

Workflow

The manual sensor installation workflow has these stages.

1. Prepare the device.

   Configure storage if the platform requires external storage, synchronize the device clock, enable IOx, and configure traffic mirroring and collection connectivity. For traffic monitoring commands, use Setting up OT traffic monitoring and the examples in Sensor deployment examples.

2. Select the sensor package.

   Download the package that matches the device architecture and the required feature set. Use an Active Discovery package only on platforms that support Active Discovery.

3. Install and activate the sensor application.

4. Create the provisioning package.

   In Cisco Cyber Vision, create a manual Cisco IOx sensor entry. The Center generates sbs-sensor-config-<serialnumber>.zip.

5. Import the provisioning package into the device.

   Upload the package through IOx Local Manager or copy it into the hosted application with the device CLI.

6. Verify sensor connectivity.

   Confirm that the sensor appears as **Connected** in **Admin** > **Sensors** > **Sensor Explorer**. Save the device configuration.

7. Enable Active Discovery if required.

   If you installed an Active Discovery package and the platform supports Active Discovery, assign the sensor to an Active Discovery profile.

Install the Sensor Application with IOx Local Manager

Use IOx Local Manager to manually install and start the Cisco Cyber Vision sensor application from the device Web UI.

Install the Cisco Cyber Vision sensor application by using the device Web UI and IOx Local Manager.

Use IOx Local Manager when you can reach the device Web UI and want to configure the hosted application through a graphical interface.

Before you begin

Complete the device preparation and OT traffic monitoring tasks.

Download the Cisco Cyber Vision sensor package for the device platform.

Verify that you can sign in to the device Web UI with a user account that can manage IOx applications.

Have the collection, capture, VLAN, gateway, and resource values that match the traffic monitoring configuration on the device.

Procedure

1. Open the device Web UI in the browser, and sign in with the device credentials..
2. Choose **Configuration** > **Services** > **IOx**.
3. Sign in to IOx Local Manager.
4. In the **Applications** tab, click **Add New**.
   a) Enter an application ID, such as CCVSensor.
   b) Upload the Cisco Cyber Vision sensor application archive.
   c) Wait until the application appears in the application list.
5. Click **Activate**.
   a) Configure the resource profile.

      Use the platform guidance in the resource settings table.

   b) Configure the network interface bindings for the hosted application.

      Use the IP addresses, prefix lengths, VLAN IDs, and gateway values that match the traffic monitoring and collection settings configured on the device.

   c) Click **Activate App**.
6. Return to the **Applications** tab and click **Start**.
7. Confirm that the application state changes to **RUNNING**.

The sensor application is installed and running on the device. The sensor does not connect to Cisco Cyber Vision until you create and import the provisioning package.

Resource settings

Table 6: IOx Local Manager resource settings

Platform	Resource settings
Cisco IR1101, IR1800, and IR8340 with SSD	Set the disk size to at least 4 GB.
Cisco IR1101, IR1800, and IR8340 without SSD	Set the disk size to 384 MB and add Docker option --tmpfs /tmp:rw,size=128m.
Cisco IE3300 10G, IE3400, IE9300, and IE3500	Set the disk size to 1248 MB. Do not set a larger value.
Cisco Catalyst 9x00 with SSD	Set the disk size to at least 15 GB and add Docker option --rm.
Cisco Catalyst 9x00 without SSD	Set the disk size to 384 MB and add Docker option --rm --tmpfs /tmp:rw,size=128m.

Interface bindings

Table 7: IOx Local Manager interface bindings

Platform	Interface bindings
Cisco IR1101 and Cisco IR1800	Bind eth0 to VPG1 for collection/NAT traffic. Bind eth1 to VPG0 for routed ERSPAN capture traffic. Disable IPv6 on both interfaces.
Cisco IR8340	Bind eth0 to VPG1 for collection/NAT traffic. Bind eth1 to mgmt-bridge300 for switched-port mirrored traffic. Bind eth3 to VPG0 for routed ERSPAN capture traffic. If you use Active Discovery, bind eth2 to mgmt-bridge300. Disable IPv6 on all interfaces.
Cisco IE3300 10G, IE3400, IE9300, and IE3500	Bind eth0 to mgmt-bridge300 and set the collection vlan id. Bind eth1 to mgmt-bridge300 and set the mirror vlan id. Disable IPv6 on both interfaces. If you use Active Discovery, add eth2 without an IP address and disable IPv4 and IPv6.
Cisco Catalyst 9x00	Bind eth0 to mgmt-bridge300 and set the collection vlan id. Bind eth1 to mgmt-bridge300, set the mirror vlan id and enable mirror mode. Disable IPv6 on both interfaces. If you use Active Discovery, add eth2 without an IP address and disable IPv4 and IPv6.

Install the Sensor Application with the Device CLI

Use IOS XE CLI commands to manually configure, install, activate, and start the Cisco Cyber Vision sensor application.

Install the Cisco Cyber Vision sensor application by using IOS XE CLI commands.

Use the device CLI when you need command-based installation or cannot use IOx Local Manager.

Before you begin

Complete the device preparation and OT traffic monitoring tasks.

Download the Cisco Cyber Vision sensor package for the device platform.

Copy the package to a location that the device can access, such as bootflash:, flash:, or usbflash0:.

Decide the application ID. The examples use CCVSensor.

Have the collection, capture, VLAN, gateway, and resource values that match the device traffic monitoring configuration.

Procedure

1. Connect to the device through SSH or console.
2. Configure the hosted application interfaces and resources.

   The following examples show common patterns. Replace the example addresses, VLAN IDs, and resource values with values for your deployment.

   Example

```
Cisco IR1101 and Cisco IR1800 without SSD:
enable
configure terminal
app-hosting appid CCVSensor
app-vnic gateway0 virtualportgroup 1 guest-interface 0
guest-ipaddress 169.254.0.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 0 guest-interface 1
guest-ipaddress 169.254.1.2 netmask 255.255.255.252
app-default-gateway 169.254.0.1 guest-interface 0
app-resource docker
run-opts 1 "--tmpfs /tmp:rw,size=128m"
end

Cisco IR8340 without SSD:
enable
configure terminal
app-hosting appid CCVSensor
app-vnic gateway0 virtualportgroup 1 guest-interface 0
guest-ipaddress 169.254.0.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 0 guest-interface 3
guest-ipaddress 169.254.1.2 netmask 255.255.255.252
app-vnic AppGigabitEthernet trunk
vlan 2340 guest-interface 1
guest-ipaddress 169.254.2.2 netmask 255.255.255.252
app-default-gateway 169.254.0.1 guest-interface 0
app-resource docker
run-opts 1 "--tmpfs /tmp:rw,size=128m"
end

Cisco IE3300 10G or Cisco IE3400:
enable
configure terminal
app-hosting appid CCVSensor
app-vnic AppGigabitEthernet trunk
guest-interface 2
vlan <collection-vlan-id> guest-interface 0
guest-ipaddress <sensor-collection-ip> netmask <collection-netmask>
vlan <mirror-vlan-id> guest-interface 1
guest-ipaddress 169.254.1.2 netmask 255.255.255.0
app-default-gateway <collection-gateway-ip> guest-interface 0
app-resource profile custom
persist-disk 2048
cpu 1400
```

```
memory 1248
vcpu 2
end

Cisco Catalyst 9x00:
enable
configure terminal
app-hosting appid CCVSensor
app-vnic AppGigabitEthernet trunk
guest-interface 2
vlan <collection-vlan-id> guest-interface 0
guest-ipaddress <sensor-collection-ip> netmask <collection-netmask>
vlan <mirror-vlan-id> guest-interface 1
mirroring
guest-ipaddress <sensor-capture-ip> netmask <capture-netmask>
app-default-gateway <collection-gateway-ip> guest-interface 0
app-resource profile custom
cpu 7400
memory 2048
vcpu 2
end

Cisco Catalyst 9x00 without SSD:
app-resource docker
run-opts 1 --rm --tmpfs /tmp:rw,size=128m
```

3. Install the application package.

   Example

   ```
   app-hosting install appid CCVSensor package
   <storage-location>:<sensor-package-file>.tar

   Example:
   app-hosting install appid CCVSensor package
   usbflash0:CiscoCyberVision-IOx-aarch64-<version>.tar
   ```

4. Verify that the application is deployed.

   Example

   ```
   show app-hosting list
   ```

5. Activate the application.

   Example

   ```
   app-hosting activate appid CCVSensor
   ```

6. Start the application.

   Example

   ```
   app-hosting start appid CCVSensor
   ```

7. Verify that the application state is **RUNNING**.

Example

```
show app-hosting list
```

The sensor application is installed and running on the device. The sensor does not connect to Cisco Cyber Vision until you create and import the provisioning package.

Create a Sensor Provisioning Package

Create the Cisco Cyber Vision provisioning package that enrolls a manually installed Cisco IOx sensor with the Center.

Create the Cisco Cyber Vision provisioning package that enrolls a manually installed Cisco IOx sensor with the Center.

Create the provisioning package after the sensor application is installed and running on the target device.

Before you begin

Configure traffic monitoring on the target device.

Install and start the sensor application on the target device.

Collect the hardware serial number.

Know whether the device uses ERSPAN or RSPAN for traffic monitoring.

Procedure

---

1. From the Cisco Cyber Vision Center menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Select **New sensor**, then select **Manual install**.
3. In the Cisco IOx manual installation page, enter the device and sensor details.

   Use the field descriptions table to complete the manual installation page.
4. Select **Create sensor**.
5. Select **Download package**.
6. Save the provisioning package.

Cisco Cyber Vision creates a sensor entry in Sensor Explorer and downloads a provisioning package named sbs-sensor-config-<serialnumber>.zip.

Manual installation fields

Table 8: Cisco IOx manual installation fields

Field	Description
Serial number	Hardware serial number of the switch or router.
Center collection IP	Leave blank to use the Center collection IP already configured on the Center. Enter a different reachable collection IP when the deployment uses NAT or a different collection address.
Gateway	Gateway used by the sensor application, if required by the network design.
Sensor label	A label that helps you identify the sensor in Sensor Explorer.

Field	Description
Capture mode	The type of traffic the sensor analyzes.
Monitor session type	Use ERSPAN, or use RSPAN only when ERSPAN is not possible and the platform supports RSPAN.

What to do next

Import the provisioning package into the device through IOx Local Manager or the device CLI.

Import the Provisioning Package with IOx Local Manager

Import the Cisco Cyber Vision provisioning package into a manually installed sensor application through IOx Local Manager.

Import the Cisco Cyber Vision provisioning package into a manually installed sensor application through IOx Local Manager.

Before you begin

Create and download the provisioning package from Cisco Cyber Vision.

Confirm that the sensor application is running in IOx Local Manager.

Procedure

1. Open the device Web UI.
2. Choose **Configuration** > **Services** > **IOx**.
3. Sign in to IOx Local Manager.
4. In the **Applications** tab, locate the sensor application.
5. Select **Manage**.
6. Select **App-DataDir** and click **Upload**.
7. Select the provisioning package, such as sbs-sensor-config-<serialnumber>.zip.
8. In the path field, enter the exact file name, including the .zip extension and click **OK**.

The provisioning package is imported into the sensor application. After the sensor completes enrollment, its health status changes to Connected in Cisco Cyber Vision Sensor Explorer.

Import the Provisioning Package with the Device CLI

Use the device CLI to copy the Cisco Cyber Vision provisioning package into a manually installed sensor application.

Import the Cisco Cyber Vision provisioning package into a manually installed sensor application by using the device CLI.

Before you begin

Create and download the provisioning package from Cisco Cyber Vision.

Copy the provisioning package to a location that the device can access, such as usbflash0:.

Confirm that the sensor application is running.

Procedure

1. Connect to the device through SSH or console.
2. Copy the provisioning package into the application data directory.

Example

```
app-hosting data appid <sensor-app-name> copy
<storage-location>:sbs-sensor-config-<serialnumber>.zip
sbs-sensor-config-<serialnumber>.zip

Example:
app-hosting data appid CCVSensor copy
usbflash0:sbs-sensor-config-<serialnumber>.zip
sbs-sensor-config-<serialnumber>.zip
```

3. Wait for the sensor to enroll with the Center.

The provisioning package is imported into the sensor application. After the sensor completes enrollment, its health status changes to Connected in Cisco Cyber Vision Sensor Explorer.

Verify a Manually Installed Sensor

Verify that a manually installed Cisco Cyber Vision sensor is connected and processing data.

Validate that a manually installed Cisco Cyber Vision sensor is connected and processing data.

Procedure

---

1. In Cisco Cyber Vision Center, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Locate the sensor that you manually installed.
3. Confirm that the sensor health status is **Connected**.
4. Confirm that the sensor processing status indicates normal processing.
5. If the sensor is not connected, check the deployment prerequisites.

   Use the verification table to check the sensor application state, provisioning package, collection connectivity, time synchronization, and traffic monitoring configuration.
6. Save the device configuration.

Example

```
write mem
```

The sensor is connected to Cisco Cyber Vision and the device configuration is saved.

Verification checks

Table 9: Manual sensor verification checks

Check	What to verify
Sensor application state	In IOx Local Manager or with show app-hosting list, confirm that the application is running.
Provisioning package	Confirm that the package was imported into the correct application ID and that the file name is exact.
Collection connectivity	Confirm that the sensor collection interface can reach the Cisco Cyber Vision Center collection interface.

Check	What to verify
Time synchronization	Confirm that the device clock is synchronized with the Center or an NTP source.
Traffic monitoring	Confirm that SPAN, RSPAN, or ERSPAN configuration matches the sensor capture interface values.

Enable Active Discovery on a Manually Installed Sensor

Enable Active Discovery on a manually installed sensor when the platform and installed package support the feature.

Enable Active Discovery on a manually installed sensor when the platform and installed package support the feature.

Cisco IR1101 and Cisco IR1800 routers do not support Active Discovery. To use Active Discovery on a supported platform, install a sensor package that includes Active Discovery.

Before you begin

Install and provision the sensor.

Confirm that the sensor health status is Connected.

Confirm that the installed package includes Active Discovery.

Procedure

1. From the Cisco Cyber Vision Center menu, choose **Admin** > **Active Discovery** > **Profiles**.
2. Select the profile that you want to apply to the sensor.
3. Select **Edit**.
4. From the **Sensors** list, select the sensor.
5. Select **Update**.
6. To run the profile immediately, select the profile and select **Run Once**.

The Active Discovery profile runs on the sensor according to the configured schedule, or immediately if you selected Run Once.

3 Sensor deployment examples

Topics:

- Sensor deployment configuration examples

Details sensor deployment setup, featuring configuration examples and guidance for deploying sensors in different scenarios such as same network, separate networks, and platform-specific cases for IE3x00 devices.

Sensor deployment configuration examples

Outlines essential network configuration examples for deploying Cisco Cyber Vision sensors, detailing VLAN settings, IP addressing, ERSPAN/RSPAN configurations, and deployment scenarios across various Cisco Catalyst switch series to ensure proper sensor communication and traffic monitoring.

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

Outlines deployment and configuration procedures for Cyber Vision sensors on Cisco Catalyst IE3x00, IE9x00, and 9x00 Series switches when the Center and sensors are on the same network, including VLAN, ERSPAN, and RSPAN setup examples.

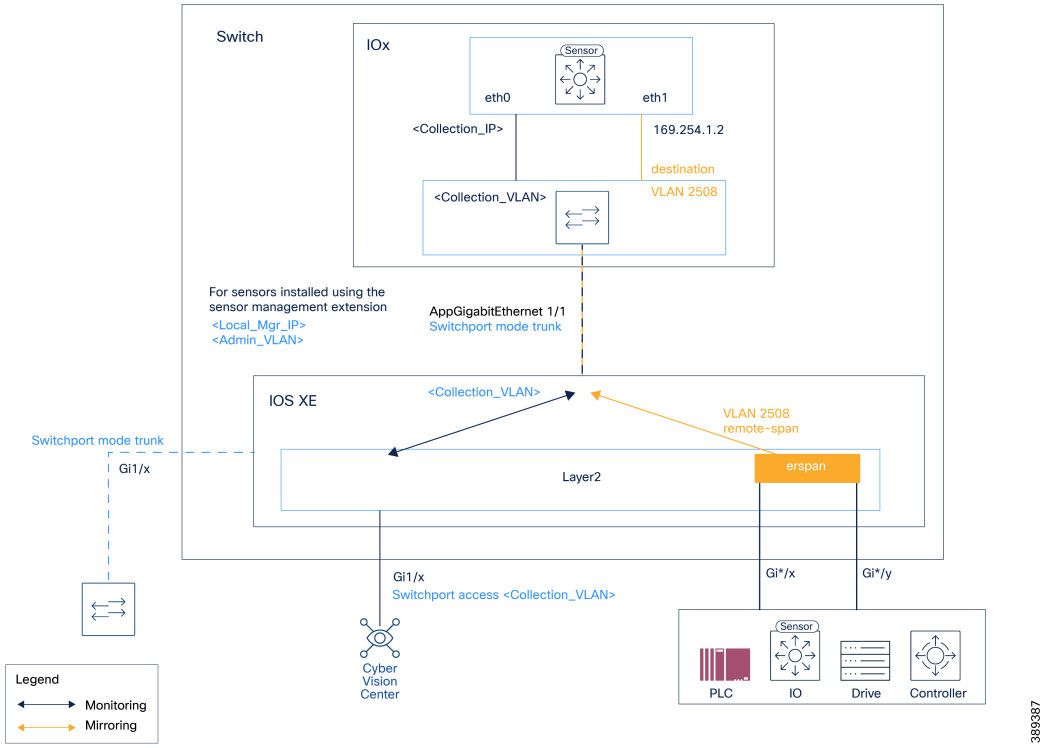
Cisco Catalyst IE3x00 Series Switches

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

Outlines deployment examples and configuration steps for Cyber Vision sensors on Catalyst IE3x00, IE9x00, and 9x00 Series switches across different networks, including ERSPAN and RSPAN setup, VLAN assignments, trunk port configuration, and routing considerations.

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
add several lines:
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

Demonstrates deploying Cyber Vision sensors on Cisco Catalyst IE3x00 switches across multiple networks, including VLAN configuration, native VLAN adjustments, and trunk port setup to ensure sensor communication and avoid conflicts.

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
write memory
```