



Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.1.0

First Published: 2021-01-01

Last Modified: 2021-01-01

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1	About this documentation	1
	Document purpose	1
	Warnings and notices	1

CHAPTER 2	Overview	3
------------------	-----------------	----------

CHAPTER 3	Cisco IC3000 front view	5
------------------	--------------------------------	----------

CHAPTER 4	Connect the Cisco IC3000	7
------------------	---------------------------------	----------

CHAPTER 5	Connect to the with the serial console	9
------------------	---	----------

CHAPTER 6	Installation procedures	13
	Sensor management extension installation	13
	Requirements	13
	Retrieve the sensor management extension file	14
	Install the sensor management extension	14
	Check the Cisco IC3000 firmware version	16
	Check the MGMT interface IP address	16
	Test connectivity between Cisco IC3000 and IOx Local Manager	17
	Create a sensor in Cisco Cyber Vision	18
	Configure the sensor	19
	Manual installation	22
	Requirements	22
	Configure the Cisco IC3000	23
	Prepare and import the provisioning package	27

Enable Active Discovery	28
Manual installation without USB (Local Manager access)	30
Requirements	30
Configure the Cisco IC3000	31
Access the Local manager	35
Install the sensor virtual application	36
Configure the sensor virtual application	38
Import the provisioning package	40
Reboot the Cisco IC3000	42
Enable Active Discovery	42

CHAPTER 7

Upgrade procedures	45
Upgrade through the Local Manager	45
Upgrade with the combined update file	49



CHAPTER 1

About this documentation

- [Document purpose, on page 1](#)
- [Warnings and notices, on page 1](#)

Document purpose

This installation guide describes how to perform a clean installation of Cisco Cyber Vision on a Cisco IC3000 Industrial Compute Gateway.

This documentation is applicable to **system version 4.1.0**.

Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.



Warning

Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.



Important

Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.



Note

Indicates important information on the product described in the documentation to which attention should be paid.



CHAPTER 2

Overview

- [Overview, on page 3](#)

Overview

The Cisco IC3000 Industrial Compute Gateway is an edge computing platform which extends the cloud computing paradigm to the edge of the network. The Cisco IC3000 captures traffic in SPAN mode. It contains 2 RJ45 10/100/1000 BaseT connectors ports and 2 SFP fiber ports to connect switches in port mirroring.

To enroll the Cisco IC3000 in Cisco Cyber Vision, take a moment to look at the [Cisco IC3000 front view](#), then start by [Connect the Cisco IC3000](#), and proceed with one of the installation methods available:

- Use [Sensor management extension installation](#) available on cisco.com (recommended).
- Perform a [Manual installation](#).
- Perform a [Manual installation without USB \(Local Manager access\)](#).

To upgrade the Cisco IC3000, refer to one of the methods available:

- Use the [Upgrade with the combined update file](#).
- If the sensor management was used to deploy the sensor, use the redeploy button from the sensor popup.
- Upgrade through the CLI.



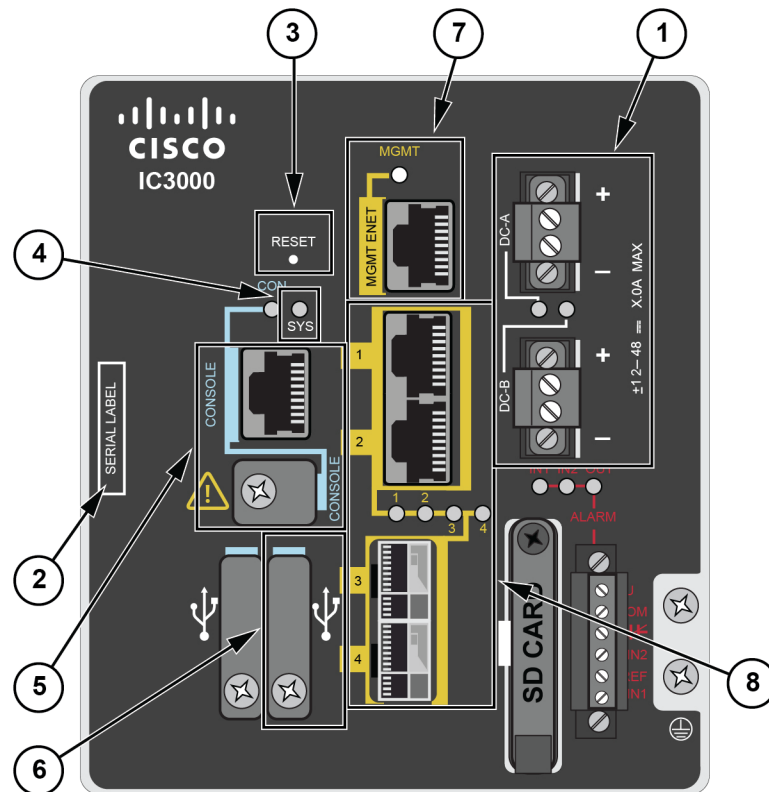
CHAPTER 3

Cisco IC3000 front view

- [Cisco IC3000 front view, on page 5](#)

Cisco IC3000 front view

Before starting, take a moment to note and unscrew the following parts you're going to use during the procedure.



- DC-in connectors (1)
- Serial number (2)
- Reset pinhole (3)

- SYS LED (4)
- Console connectors (5): RJ-45 and mini-USB
- USB port 2 (6)
- MGMT Ethernet port (7): Local Manager and Collection network interfaces
- Industrial Network Interfaces (8): 2x RJ45 10/100/1000 BaseT connectors and 2x SFP fiber ports



CHAPTER 4

Connect the Cisco IC3000

- [Connect the Cisco IC3000, on page 7](#)

Connect the Cisco IC3000

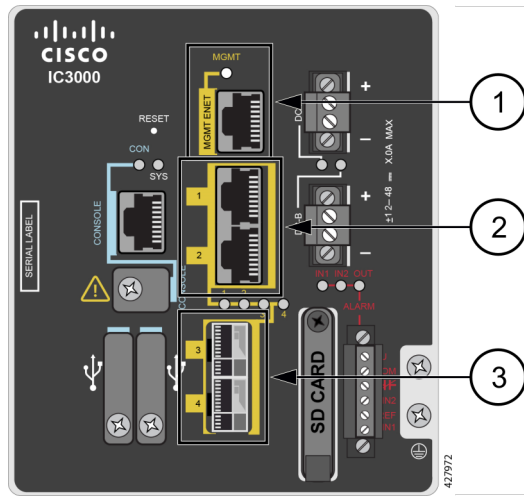
The Cisco IC3000 contains 4 independent ports which can be used to capture in SPAN mode or to do active scanning on the network. Depending on the port usage the corresponding switch port must have the right configuration (SPAN or access).

The Cisco IC3000's Industrial network interface to do the dPI is to be connected to **switches configured in port mirroring only**.

To connect the network interfaces to the Cisco IC3000:

Procedure

- Step 1** Connect the Collection network interface (IC3000 to Center) to the MGMT ENET port **(1)**.
- Step 2** Connect the Industrial network interface (IC3000 to on-site switches) to ports 1, 2, 3, 4 (up to 4 switches configured in port mirroring or access depending on the port usage).
- Step 3**
 - Ports 1 and 2 are RJ45 10/100/1000 BaseT Connectors **(2)**.
 - Ports 3 and 4 are SFP fiber ports **(3)**.





CHAPTER 5

Connect to the with the serial console

- [Connect to the Cisco IC3000 with the serial console, on page 9](#)

Connect to the Cisco IC3000 with the serial console

This section describes how to establish a connection to the Cisco IC3000 from Windows 10 using PuTTY. It is required to perform a sensor management extension installation and to enable Active Discovery (optional) when performing a manual installation.



Note This procedure will also work for other versions of Windows.

Requirements:

- A RJ45 or mini USB console cable.
- A serial console emulator, like PuTTY.

To connect a console to the Cisco IC3000:

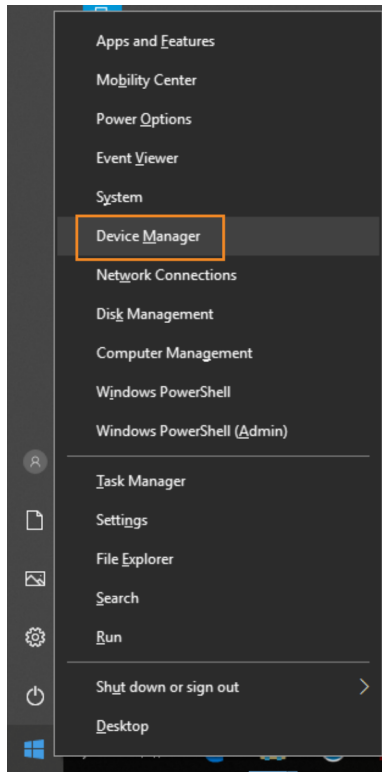
Procedure

Step 1 Download and install on your computer a serial console emulator like PuTTY. Refer to its own documentation to use it.

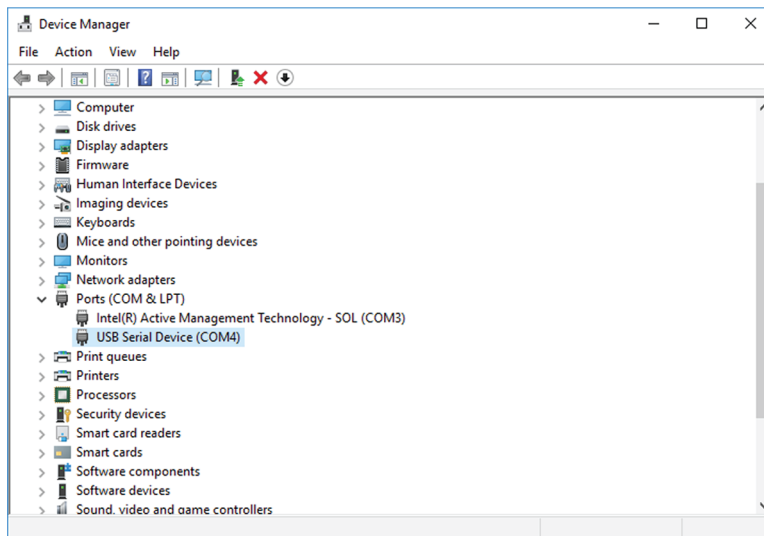
Step 2 Connect your computer to the Cisco IC3000 through its serial port using the RJ45 or mini USB console cable. If you are using **Windows**, you need to identify to which COM port the console is connected.

To identify the COM port:

Step 3 Right click on the Windows Start icon and select "Device Manager".



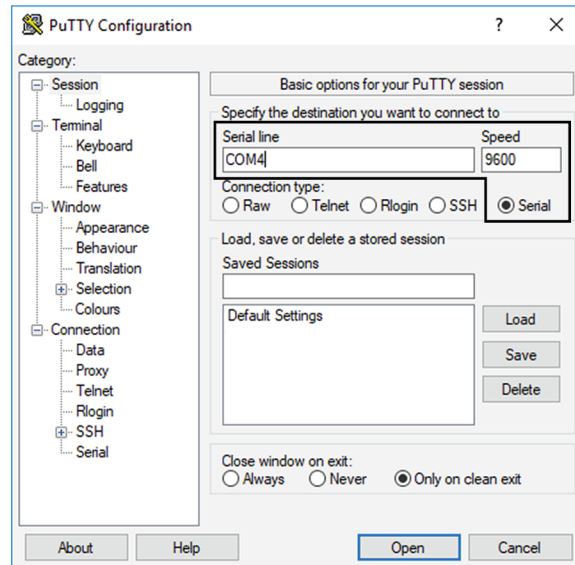
Step 4 Scroll down and click "Ports (COM & LPT)" menu. The COM number appears.



To start a connection to the Cisco IC3000:

- Step 5** Make sure there is no USB drive plugged into the Cisco IC3000.
- Step 6** Disconnect the Cisco IC3000 from the DC Current source.
- Step 7** Open PuTTY.

The following screen appears:



Step 8 Select Serial for the Connection type.

Step 9 Enter "COM<number>" into the serial line field.

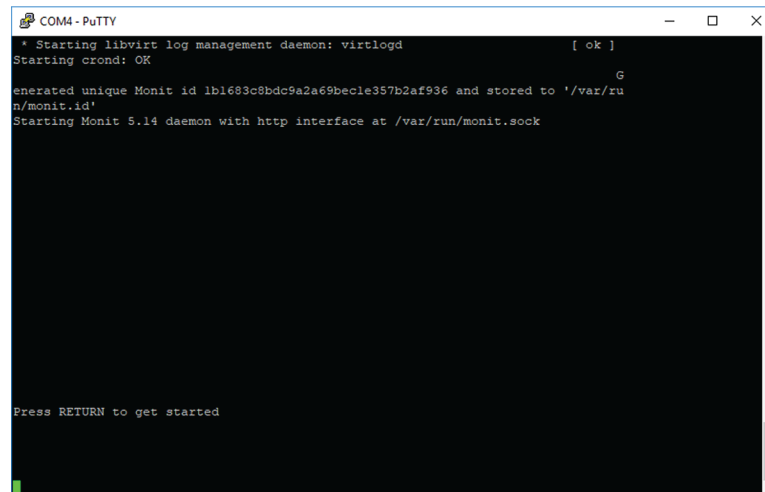
Set speed at 9600.

Step 10 Click Open to display the shell prompt for PuTTY.

Step 11 Connect the Cisco IC3000 to the DC current source.

Wait a few moments. When booting is complete, the shell prompt will ask you to press return to start.

The connection has established with success.





CHAPTER 6

Installation procedures

- [Sensor management extension installation, on page 13](#)
- [Manual installation, on page 22](#)
- [Manual installation without USB \(Local Manager access\), on page 30](#)

Sensor management extension installation

This section explains how to install the Cisco IC3000 thanks to the sensor management extension. You will:

1. Retrieve the sensor management extension on [cisco.com](#).
2. Install the sensor management extension on Cisco Cyber Vision.
3. Connect to the Cisco IC3000 with the serial console and check its firmware version and management interface IP address.
4. Create a new sensor on Cisco Cyber Vision through the Cisco device deployment and proceed to its configuration.

Requirements

The hardware must have an access set to the Local Manager and to the CLI (ssh or console port).

Required material and information:

- An Admin or Product access to Cisco Cyber Vision.
- The network information of the Collection network interface (IP address, subnet mask and gateway).
- A RJ45 or mini USB console cable.
- A serial console emulator, like PuTTY.



Note To be able to use the Cisco Cyber Vision sensor management extension, an IP address reachable by the Center Collection interface must be set on the Collection VLAN.

Retrieve the sensor management extension file

1. On cisco.com, navigate to Cisco Cyber Vision's Software Download page.
2. Download Cisco Cyber Vision Sensor Management Extension for IoX sensor setup. Version of the extension must be the same as the version of the center.

The screenshot shows the Cisco Software Download page for Cyber Vision 3.1.1. The page includes a search bar, a list of releases (3.0.4, All Release, 3, 3.1.1, 3.1.0, 3.0.3, 3.0.2), and a table of file information. The file 'Cisco Cyber Vision Sensor Management Extension for IoX sensor setup' is highlighted with a red box.

File Information	Release Date	Size	
Cisco Cyber Vision Sensor Management Extension for IoX sensor setup CiscoCyberVision-sensor-management-3.1.1.ext	30-Jul-2020	666.87 MB	↓ 🛒 📄
VMware OVA (Center) - CiscoCyberVision-3.1.1.ova CiscoCyberVision-3.1.1.ova	28-Jul-2020	251.81 MB	↓ 🛒 📄
Hyper-V VHDX (Center) - CiscoCyberVision-3.1.1.vhdx CiscoCyberVision-3.1.1.vhdx	28-Jul-2020	312.00 MB	↓ 🛒 📄

Install the sensor management extension

1. In Cisco Cyber Vision, navigate to Admin > Extensions.
2. Click Import extension file and select CiscoCyberVision-sensor-management-<version>.ext.

Extensions

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

Installed extensions

Name	Version
No Data	

Install a new extension

Import extension file

The file upload takes a few minutes.

Extensions

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



Installation
Uploading... Please do not quit or refresh the page.

Extensions


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

✔ **Installation** ×
 Cyber Vision sensor management installed successfully !

Installed extensions

Name	Version	Actions
Cyber Vision sensor management	3.2.0	 

Install a new extension

 Import extension file

Check the Cisco IC3000 firmware version

To ensure a proper installation of the Cisco IC3000, you must check that its firmware version is 1.2.1 or newer.

Procedure

Step 1

To check the version:

Step 2

- Use the following command in the Cisco IC3000 shell prompt:

```
ic3k>show version
```

Example:

```
ic3k>show version
Version: 1.2.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FCH2312Y04M
ic3k>
```

The version should be 1.2.1 or newer.

Check the MGMT interface IP address

Check that the IP address set on the MGMT network is the one you've configured on the Cisco Cyber Vision GUI.

To check the MGMT network interface:

Procedure

Step 1 Use the following command in the Cisco IC3000 shell prompt:

```
ic3k>show interfaces
```

Step 2 Search for the reference "svcbr_0" which corresponds to the MGMT interface.

The IP address you've set as Host Management on Cisco Cyber Vision GUI should follow the mention "inet addr: <IP ADDRESS>".

Example:

```
svcbr_0  Link encap:Ethernet  HWaddr d0:ec:35:ca:99:a0
         inet addr:192.168.71.22  Bcast:192.168.71.255  Mask:255.255.255.0
         inet6 addr: fe80::d2ec:35ff:feca:99a0/64  Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:227 errors:0 dropped:0 overruns:0 frame:0
         TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:12676 (12.3 KiB)  TX bytes:1980 (1.9 KiB)
```

Step 3

Test connectivity between Cisco IC3000 and IOx Local Manager

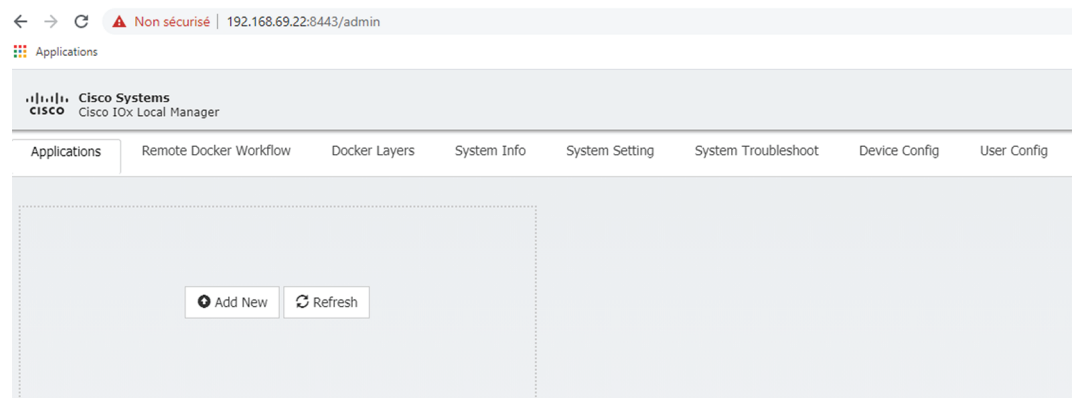
To proceed with the installation, you must first test if you have access to the Cisco IC3000's Cisco IOx Local Manager. To do so:

1. Open Chrome.
2. Access Cisco IOx Local Manager using the Cisco IC3000's MGMT IP address and the MGMT port number, which is 8443:

`https://Management_Address:8443`

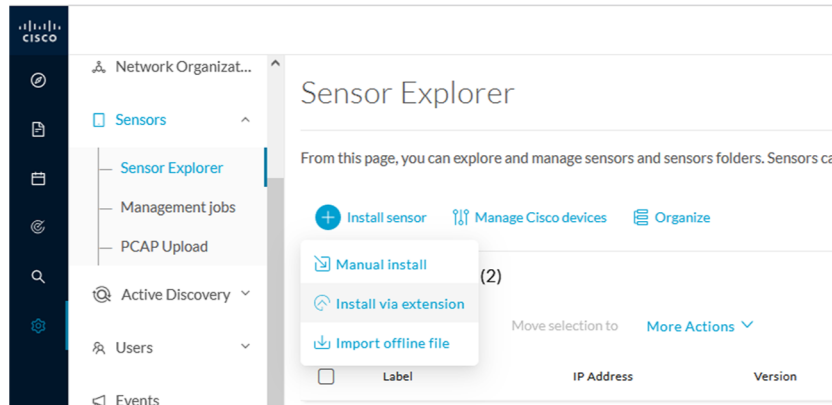
ex: `https://192.168.71.22:8443`

3. If you're able to see the following screen it means that the connectivity between the Cisco IC3000 and IOx Local Manager is on.



Create a sensor in Cisco Cyber Vision

1. In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click Install sensor, then Install via extension.



2. Fill the requested fields so Cisco Cyber Vision can reach the equipment:
 - IP Address: admin address of the equipment
 - Port: management port (8443)
 - User: user with the admin rights of the equipment
 - Password: password of the admin user
 - Capture Mode: Optionally, select a capture mode.

Install via extension

Reach Cisco device

Please fill the fields below to enable Cisco Cyber Vision to reach your device.

IP address*

Port* For example 443 or 8443

Center collection IP

leave blank to use current collection IP

Credentials

Login*

Password*

Capture mode

Optimal (default): analyze the most relevant flows

All: analyze all the flows

Industrial only: analyze industrial flows

Custom: you set your filter using a packet filter in tcpdump-compatible syntax

Exit
Connect

3. Click the Connect button.

The Center will join the equipment and display the second parameter list. For this step to succeed, the equipment needs to be reachable by the Center on its eth0 connection for a Center with single interface or eth1 for a Center with dual interface.

Configure the sensor

Once the Center can join the equipment, you will have to configure the Cisco Cyber Vision IOx sensor app by setting the Collection interface and, if needed, Active Discovery.

While some parameters are filled automatically, you can still change them if necessary.

1. Fill the following parameters for the Collection interface:
 - Collection IP address: IP address of the sensor in the sensor (must be different than the ip address of the device)
 - Collection subnet mask: mask of the Collection IP address
 - Collection gateway: gateway of the Collection IP address (optional)

Install via extension

Configure Cyber Vision IOx sensor app

The device requires additional parameters. Some parameters have been pre-filled. Please complete the remaining fields.

Cisco device: IC3000-2C2F-K9

Collection IP address*

Collection prefix length* Like 24, 16 or 8

Collection gateway

[Exit](#) [Next](#)

2. Select the Application type (passive only or passive and Active Discovery).
3. If selecting Passive and Active Discovery, the following fields will appear to set its interface:

Install via extension

Configure Active Discovery

Please select an application type. If you want to enable Active Discovery on the application, select "Passive and Active Discovery". You will have to add some network interfaces parameters.

Passive only
 Passive and Active Discovery

Select a physical interface

Select the port used to send packets

ETH2 NETWORK

IP address* IP address interface used to do Active Discovery

Prefix length* Like 24, 16 or 8

[Exit](#) [Back](#) [Deploy](#)

Physical interface: port that will be used to send packets.

- Physical interface: port that will be used to send packets.

Configure Active Discovery

Please select an application type. If you want to enable Active Discovery, select the physical interface parameters.

- Passive only**
- Passive and Active Discovery**

Select a physical interface

^

MGMT / Collection (enables DPI on collection interface)

Int1

Int2

Int3

Int4

- IP address of the interface dedicated to Active Discovery.
- Prefix length: subnet mask of the interface.

Select a physical interface

Int2
v

Select the port used to send packets

ETH2 NETWORK

IP address*

192.168.53.23

IP address interface used to do Active Discovery

Prefix length*

24

Like 24, 16 or 8

Back

Deploy

4. Click the Deploy button.

The Center starts deploying the sensor application on the target equipment. This can take a few minutes. Once the deployment is finished, a new sensor appears in the sensors list.

If Active Discovery has been enabled, the Active Discovery status will switch to Available and the Active Discovery button will be displayed in the right side panel as you click the sensor in the list.

The sensor status will turn to connected.

Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
				Connected	Pending data	Enabled	2 minutes

Note You can change the Active Discovery configuration by clicking the Active Discovery button. However, for changes to be applied, you will have to download a new provisioning package and deploy it on the hardware.

Manual installation

This section explains how to install the Cisco IC3000 manually. You will generate and retrieve the provisioning package from the Cisco Cyber Vision, and manually import it into the Cisco IC3000. The last step, which is optional, consists in enabling Active Discovery.

Requirements

The hardware must have an access set to the Local Manager and to the CLI (ssh or console port).

Required material and information:

- An Admin or Product access to Cisco Cyber Vision.
 - The serial number of the Cisco IC3000 to be configured (located on the hardware's front view).
 - The Cisco IC3000 and sensor network information.
 - The Cisco Cyber Vision Sensor application to collect from cisco.com, i.e. CiscoCyberVision-IOx-IC3K-<version>.tar.
 - A console cable, for the connection to the hardware's console port.
- OR
- An Ethernet cable, for the connection to one of the hardware's port.

Configure the Cisco IC3000

Login to Cisco Cyber Vision GUI to create and configure a new Cisco IC3000. During this step, you will have to set the Local Manager's and the Cisco IC3000 Sensor Application's network parameters to retrieve the provisioning package.

Requirements:

- An Admin or Product access to Cisco Cyber Vision.
- An IP addressing scheme for the Local Manager and the Collection Network Interfaces.



Important

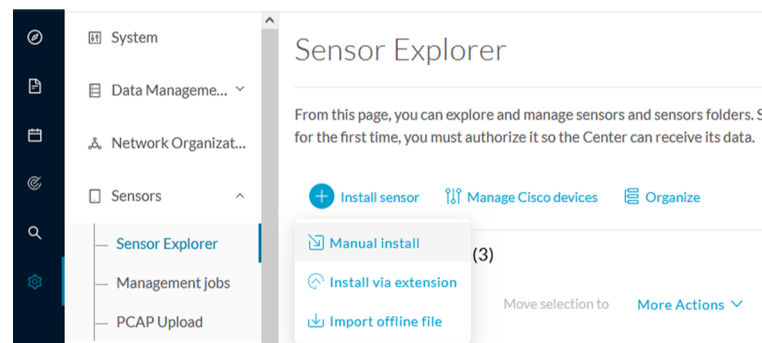
Make sure network information entered below is set accordingly to your network infrastructure and won't result in conflict. Any mistake could bring you to perform a factory reset of the Cisco IC3000 and to start the whole procedure again.

To create and configure the Cisco IC3000 in the GUI:

Procedure

Step 1 Login to Cisco Cyber Vision.

Step 2 Navigate to Admin > Sensors > Sensor Explorer.



Step 3 Click Manual install.

The manual sensor installation opens.

Step 4 Select Cisco Cisco IC3000 as hardware model.

Manual install

Select hardware model

The manual installation is provided to deploy Cisco IOx Sensor, Cisco IC3000 Industrial Compute Gateway and Sentryo sensors. Please select an hardware below to start configuration.

- Cisco IC3000
- Cisco IOx Application
- Sentryo SENSOR3
- Sentryo SENSOR5
- Sentryo SENSOR7

[Exit](#)[Next](#)

Important Two types of configuration are needed: - **Cisco Cisco IC3000 configuration** is to set the Local Manager Network to access the Cisco IC3000 device for configuration and troubleshooting purposes. - **Sensor configuration** is to set the Cisco Cyber Vision Sensor Application's to the Collection Network Interface for normal operation of Cisco Cyber Vision. Consequently, **two IP addresses belonging to different subnetworks** must be set accordingly to your network configuration. Pay attention to the contextual help to guide you through the configuration and keep these information stored for a later use.

To set Cisco Cisco IC3000 Local Manager:

Fill the following fields to set the Local Manager's network parameters and login:

Manual install

Configure provisioning package

Please fill the fields below to add configuration to the provisioning package to install.

Cisco IC3000 Local Manager

Serial number*

FCH2309Y01Z

Host management IP address*

192.168.49.22

Host management netmask*

255.255.255.0

For example 255.255.255.0 or 255.255.0.0

Host management gateway*

192.168.49.254

Local manager user name*

admin

- Step 5** Type the Cisco IC3000s' serial number. It is available on the hardware's front view.
- Step 6** Type the Host Management's IP address, netmask and gateway. They must be set to access the Local Manager of the Cisco IC3000 device.
- Step 7** Type the Local Manager admin user name. The login is "admin" by default. You must use the default login in case a factory reset is performed and thus to avoid starting the whole procedure again.

The user name will be asked later to log in to IOx Local Manager and in case of troubleshooting and configuration. Therefore, make sure to keep this piece of information stored.

To set the Sensor application:

Fill the following fields to set Cisco Cyber Vision Sensor Application's network parameters. These correspond to the Collection Network Interface within Cisco Cyber Vision's infrastructure.

Sensor Application

IP address*

192.168.49.23

Netmask*

24

For example 24, 16 or 8

Center collection IP

leave blank to use current collection IP

Gateway

Capture mode:

- Optimal (default): analyze the most relevant flows**
- All: analyze all the flows
- Industrial only: analyze industrial flows**
- Custom: you set your filter using a packet filter in tcpdump-compatible syntax**

it

Back

Create sensor

- Step 8** Type Cisco Cyber Vision Cisco IC3000 Application's IP address and subnet mask.
The Center IP and gateway are optional.
You can select the default capture mode and change it later.

- Step 9** Click Create Sensor.

To get the provisioning package:

- Step 10** Set the Local Manager's password for troubleshooting. Make sure to keep this piece of information stored as it will be asked to access IOx Local Manager and for further troubleshooting and configuration purposes.
- Step 11** Click the link to download the provisioning package.

Manual install

Download provisioning package

The provisioning package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up or added in the right location of your IOx Application.

Password*

●●●●●●●●

Confirm password*

●●●●●●●●

 Good ⓘ

[↓ Download package](#)

<it

Finish

Step 12

Click Finish. A message saying that the sensor has been successfully created is displayed.

Manual install

Done!

The sensor has been created in Cyber Vision app and the provisioning package has been generated.

What's next?

[Back to Sensor Explorer](#)

The Cisco IC3000 status switches to Disconnected.

Important Do not install several provisioning package on the Cisco IC3000. The provisioning package will NOT overwrite a previously installed one with incorrect network information or a misconfigured password. In such case, a factory reset will have to be performed.

Prepare and import the provisioning package

To deploy the provisioning package in the Cisco IC3000:

Procedure

- Step 1** Unzip and extract the downloaded provisioning package files at the root directory of a USB drive formatted as FAT32.
- The new file is named with the Cisco IC3000's serial number.
- Make sure the provisioning package name is strictly the Cisco IC3000 serial number. Any space or duplicate number will result in an unsuccessful installation.
- Step 2** Disconnect the Cisco IC3000 from the DC Current source. The USB drive must be plugged at the Cisco IC3000 boot.
- Step 3** Plug the USB drive on port 2 of the Cisco IC3000.
- Step 4** Connect the sensor to the DC Current source.
- Wait a few moments. The Cisco IC3000 status changes to Enrolled on the Cisco Cyber Vision GUI.
- Step 5** Unplug the USB drive from port 2.
- The status should quickly change to Connected.

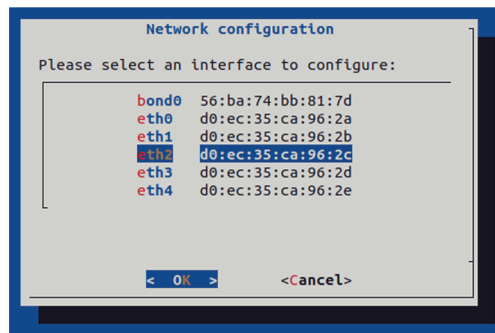
Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
[Redacted]	[Redacted]	[Redacted]	[Redacted]	Discovered	Discovered		N/A
[Redacted]	[Redacted]	[Redacted]	[Redacted]	Discovered	Discovered		N/A
FCH2309Y01Z	192.168.49.23	4.1.0+202202151504	[Redacted]	Connected	Pending data	Enabled	2 minutes

The provisioning package has been installed successfully on the Cisco IC3000 and traffic starts to appear in Cisco Cyber Vision.

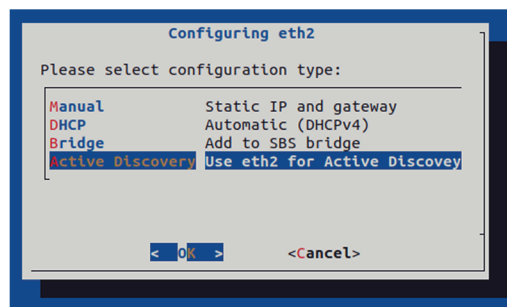
Enable Active Discovery

1. Connect to the Cisco IC3000 console and type the following command to set the Active Discovery interface.

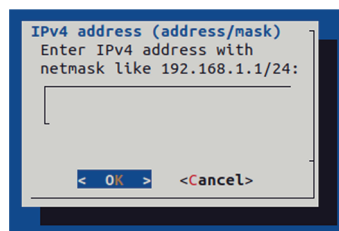

```
root@sensor:~# sbs-netconf
```
2. Choose which interface to configure between eth1, eth2, eth3 and eth4.



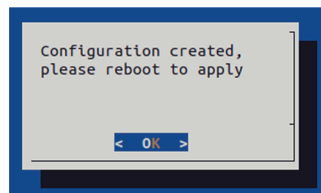
3. Select Active Discovery and make sure the right interface will be used for Active Discovery.



4. Type the subnetwork IP address dedicated to Active Discovery.



5. Select OK.



6. Type the following command to reboot the sensor.

```
root@sensor:~# reboot
```

7. On the Cisco Cyber Vision Sensor Explorer page, the sensor's Active Discovery status will switch to Enabled, and the Active Discovery button will appear on the sensor's right side panel. This may take a few moments.

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely managed. For the first time, you must authorize it so the Center can receive its data.

[+ Install sensor](#)
[Manage Cisco devices](#)
[Organize](#)

Folders and sensors (3)

[Filter](#)
0 Selected
Move selection to
[More Actions](#)

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status
<input type="checkbox"/>	FCW2445P6X5				Disconnected
<input type="checkbox"/>	FCW2445P6X5				Disconnected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected

Label: FCW2445P6X5
 Serial Number: FCW2445P6X5
 IP address: 192.168.49.21
 Version: 4.1.0+202202151440
 System date: Feb 24, 2022 4:13:06 PM
 Deployment: Sensor Management Extension
 Active Discovery: Enabled
 Capture mode: All

System Health
 Status: Connected
 Processing status: Normally processing
 Uptime: a day

[Go to statistics](#)

[Start Recording](#)

[Move to](#)

[Capture mode](#)
[Redeploy](#)

[Uninstall](#)
[Active Discovery](#)



Note You can change the Active Discovery configuration by clicking the Active Discovery button. However, for changes to be applied, you will have to download a new provisioning package and deploy it on the hardware.

Manual installation without USB (Local Manager access)

This section explains how to install the Cisco IC3000 manually without USB. You will:

1. Create and configure a new sensor on Cisco Cyber Vision to retrieve its provisioning package.
2. Install and configure the virtual sensor application on the Local Manager to deploy the provisioning package on the Cisco IC3000.
3. The last step, which is optional, consists in enabling Active Discovery on the Cisco IC3000.

Requirements

The hardware must have an access set to the Local Manager and to the CLI (ssh or console port).

Required material and information:

- An Admin or Product access to Cisco Cyber Vision.
- A Local Manager user account and password.
- The serial number of the Cisco IC3000 to be configured (located on the hardware's front view).
- An IP addressing scheme for the Local Manager and the Collection Network Interfaces.

- The Cisco Cyber Vision Sensor application to collect from cisco.com, i.e. CiscoCyberVision-IOx-IC3K-<version>.tar.

Configure the Cisco IC3000

Login to Cisco Cyber Vision GUI to create and configure a new Cisco IC3000. During this step, you will have to set the Local Manager's and the Cisco IC3000 Sensor Application's network parameters to retrieve the provisioning package.

Requirements:

- An Admin or Product access to Cisco Cyber Vision.
- An IP addressing scheme for the Local Manager and the Collection Network Interfaces.



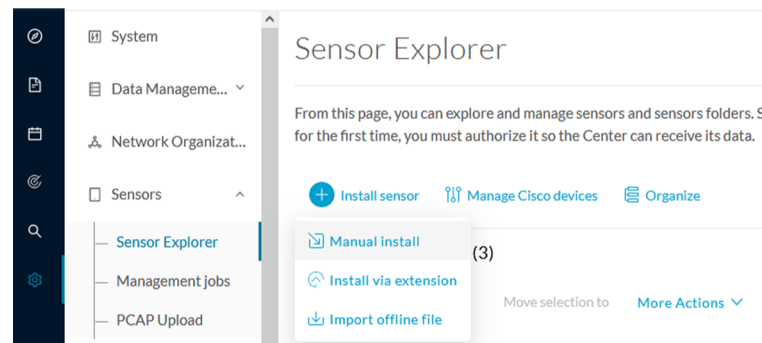
Important

Make sure network information entered below is set accordingly to your network infrastructure and won't result in conflict. Any mistake could bring you to perform a factory reset of the Cisco IC3000 and to start the whole procedure again.

To create and configure the Cisco IC3000 in the GUI:

Procedure

- Step 1** Login to Cisco Cyber Vision.
- Step 2** Navigate to Admin > Sensors > Sensor Explorer.



- Step 3** Click Manual install.
The manual sensor installation opens.
- Step 4** Select Cisco IC3000 as hardware model.

Manual install

Select hardware model

The manual installation is provided to deploy Cisco IOx Sensor, Cisco IC3000 Industrial Compute Gateway and Sentryo sensors. Please select an hardware below to start configuration.

- Cisco IC3000
- Cisco IOx Application
- Sentryo SENSOR3
- Sentryo SENSOR5
- Sentryo SENSOR7

[Exit](#)[Next](#)

Important Two types of configuration are needed: - **Cisco Cisco IC3000 configuration** is to set the Local Manager Network to access the Cisco IC3000 device for configuration and troubleshooting purposes. - **Sensor configuration** is to set the Cisco Cyber Vision Sensor Application's to the Collection Network Interface for normal operation of Cisco Cyber Vision. Consequently, **two IP addresses belonging to different subnetworks** must be set accordingly to your network configuration. Pay attention to the contextual help to guide you through the configuration and keep these information stored for a later use.

To set Cisco Cisco IC3000 Local Manager:

Fill the following fields to set the Local Manager's network parameters and login:

Manual install

Configure provisioning package

Please fill the fields below to add configuration to the provisioning package to install.

Cisco IC3000 Local Manager

Serial number*

FCH2309Y01Z

Host management IP address*

192.168.49.22

Host management netmask*

255.255.255.0

For example 255.255.255.0 or 255.255.0.0

Host management gateway*

192.168.49.254

Local manager user name*

admin

- Step 5** Type the Cisco IC3000s' serial number. It is available on the hardware's front view.
- Step 6** Type the Host Management's IP address, netmask and gateway. They must be set to access the Local Manager of the Cisco IC3000 device.
- Step 7** Type the Local Manager admin user name. The login is "admin" by default. You must use the default login in case a factory reset is performed and thus to avoid starting the whole procedure again.

The user name will be asked later to log in to IOx Local Manager and in case of troubleshooting and configuration. Therefore, make sure to keep this piece of information stored.

To set the Sensor application:

Fill the following fields to set Cisco Cyber Vision Sensor Application's network parameters. These correspond to the Collection Network Interface within Cisco Cyber Vision's infrastructure.

Sensor Application

IP address*

192.168.49.23

Netmask*

24

For example 24, 16 or 8

Center collection IP

leave blank to use current collection IP

Gateway

Capture mode:

- Optimal (default): analyze the most relevant flows**
- All: analyze all the flows
- Industrial only: analyze industrial flows**
- Custom: you set your filter using a packet filter in tcpdump-compatible syntax**

it

Back

Create sensor

- Step 8** Type Cisco Cyber Vision Cisco IC3000 Application's IP address and subnet mask.
The Center IP and gateway are optional.
You can select the default capture mode and change it later.

- Step 9** Click Create Sensor.

To get the provisioning package:

- Step 10** Set the Local Manager's password for troubleshooting. Make sure to keep this piece of information stored as it will be asked to access IOx Local Manager and for further troubleshooting and configuration purposes.
- Step 11** Click the link to download the provisioning package.

Manual install

Download provisioning package

The provisioning package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up or added in the right location of your IOx Application.

Password*

●●●●●●●●

Confirm password*

●●●●●●●●

 Good ⓘ

[↓ Download package](#)

<it

Finish

Step 12

Click Finish. A message saying that the sensor has been successfully created is displayed.

Manual install

Done!

The sensor has been created in Cyber Vision app and the provisioning package has been generated.

What's next?

[Back to Sensor Explorer](#)

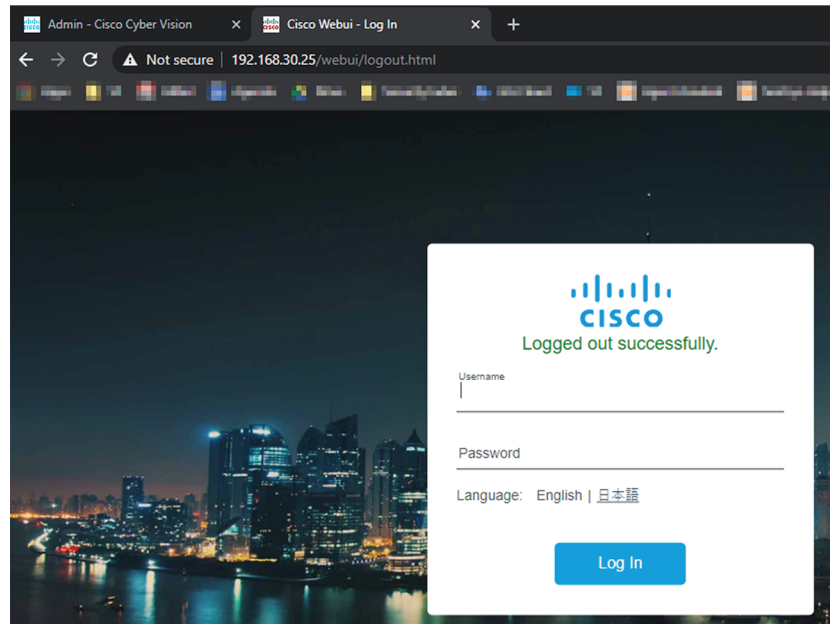
The Cisco IC3000 status switches to Disconnected.

Important Do not install several provisioning package on the Cisco IC3000. The provisioning package will NOT overwrite a previously installed one with incorrect network information or a misconfigured password. In such case, a factory reset will have to be performed.

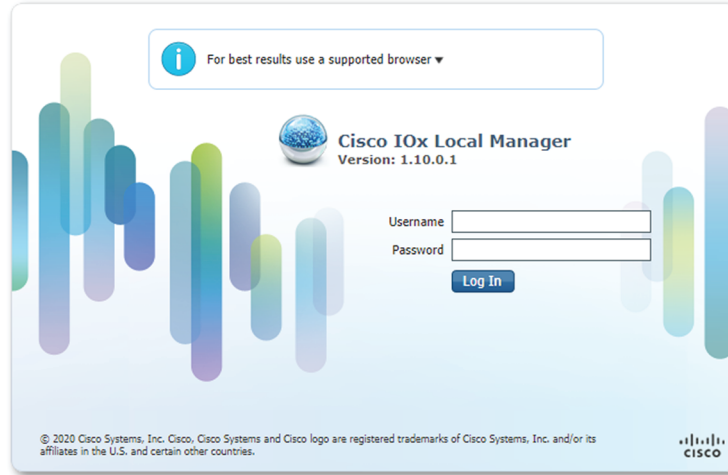
Access the Local manager

1. Open a browser and navigate to the IP address you configured on the interface you are connected to.
2. Log in using the Local Manager user account and password.

Install the sensor virtual application

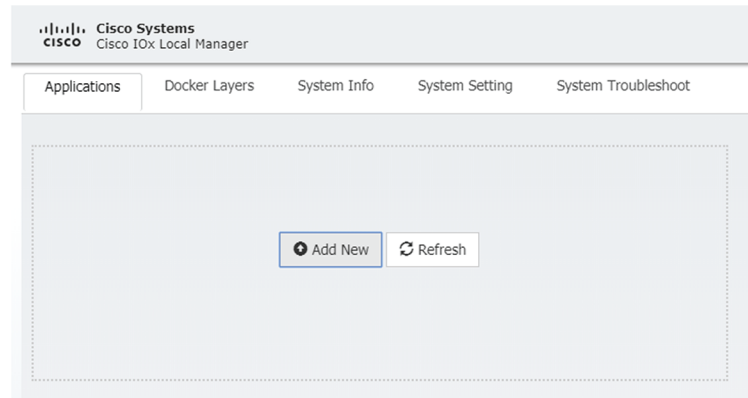


3. Once logged into the Local Manager, navigate to Configuration > Services > IOx.
4. Log in using the user account and password.

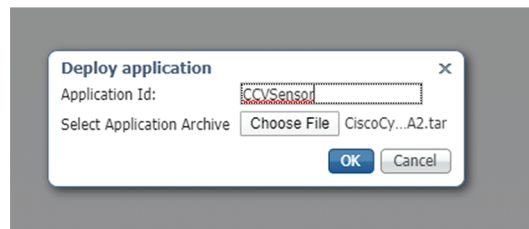


Install the sensor virtual application

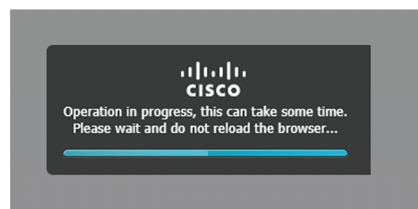
Once logged in, the following menu appears:



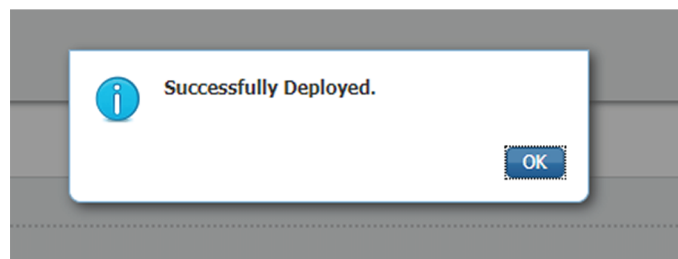
1. Click Add New.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file
(i.e. "CiscoCyberVision-IOx-IC3K-<version>.tar")



The installation takes a few minutes.



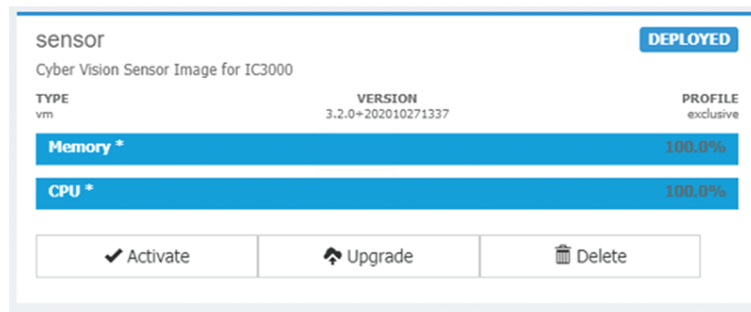
When the application is installed, the following message is displayed:



Configure the sensor virtual application

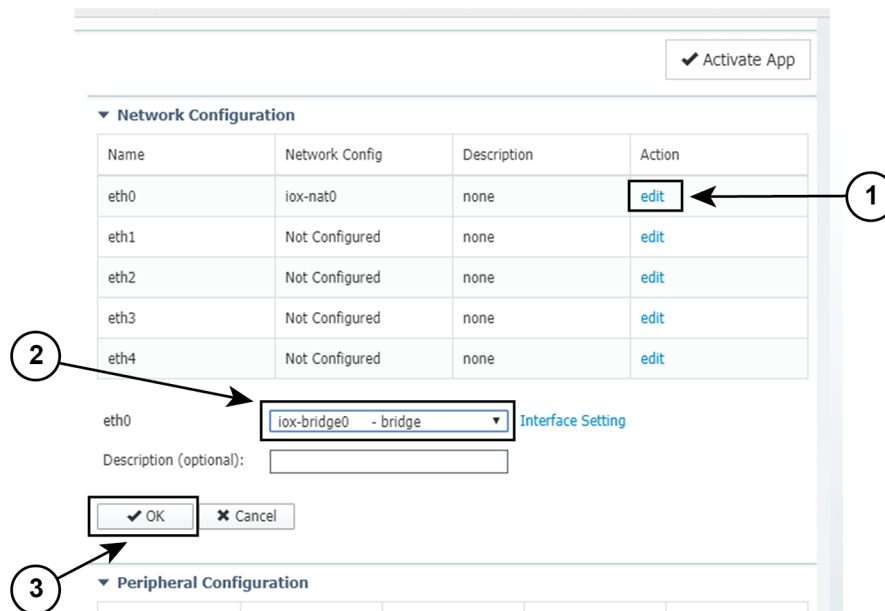
Procedure

Step 1 Click Activate to launch the configuration of the sensor application.



To map the Sensor network interfaces:

Step 2 Access Applications > Resources.



Step 3 Under Network Configuration, click Edit in the eth0 line (1).

Step 4 Set eth0 as iox-bridge0 (2).

Step 5 Click OK (3).

Step 6 A message saying that the network interface has been changed displays. Click OK.

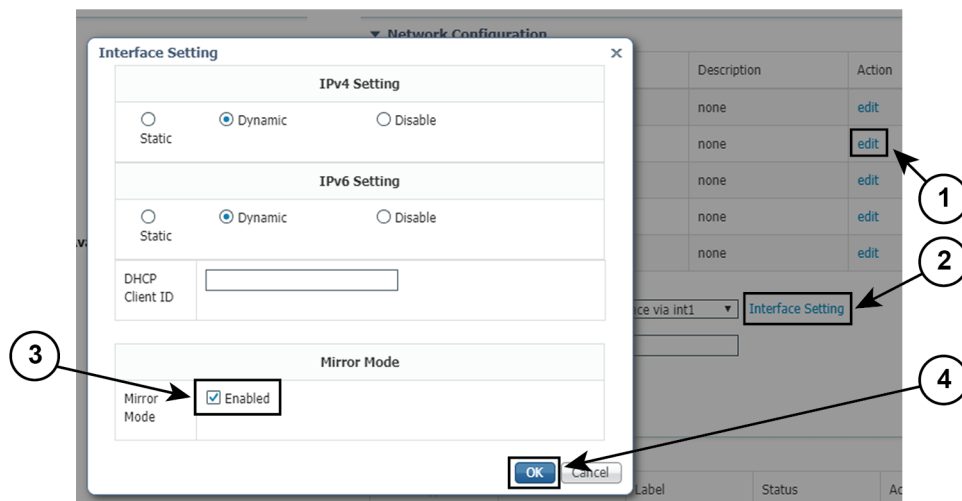
Step 7 Set the network interfaces eth1, eth2, eth3 and eth4 by repeating the previous steps and using the table below. You must click OK each time you map a new interface for changes to be taken into consideration.

Each network interface must be mapped like below:

Name	Network Configuration
eth0	iox-bridge0
eth1	int1
eth2	int2
eth3	int3
eth4	int4

To set eth1, eth2, eth3 and eth4 as mirrored ports:

- Step 8** Click Edit beside eth1 (1).
- Step 9** Click Interface Settings (2).
- Step 10** Tick Enabled for Mirror Mode (3).
- Step 11** Click OK (4).

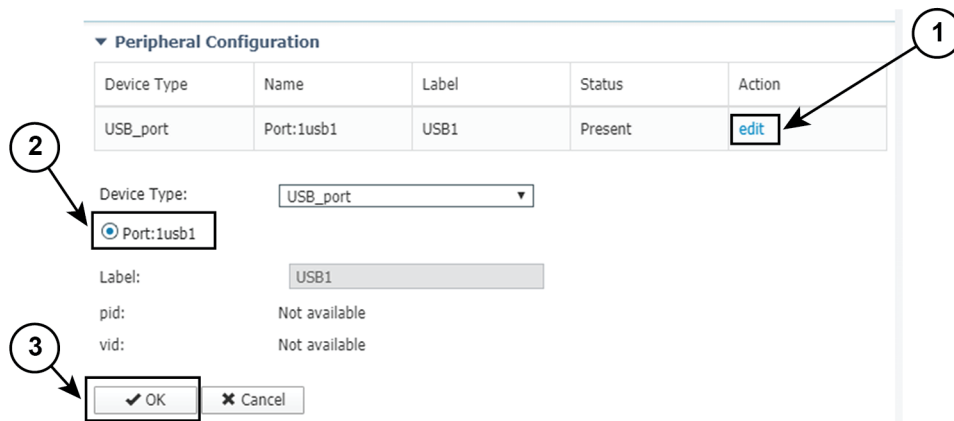


- Step 12** Repeat the above steps for eth2, eth3 and eth4.

To set the peripheral configuration:

- Step 13** Under Peripheral Configuration, click Edit (1).
- Step 14** Tick Port: 1usb1 (2).
- Step 15** Click OK (3).

Import the provisioning package

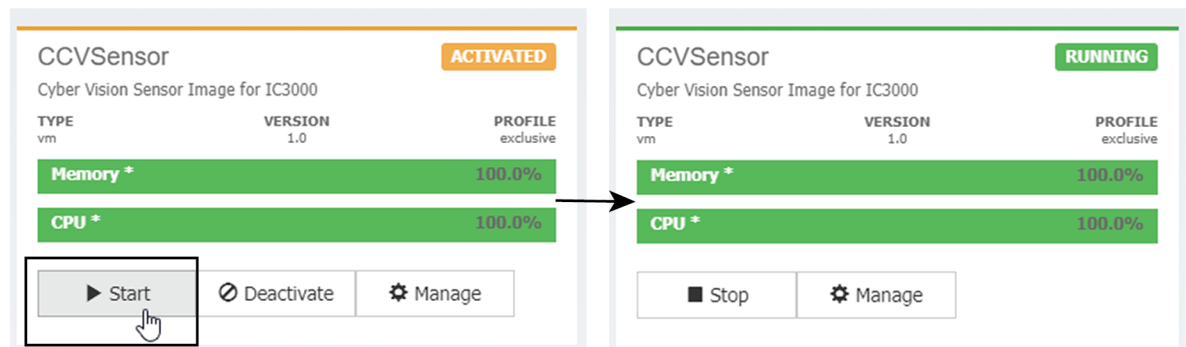


Step 16 Click Activate App on the page top right corner.

To start the Sensor Application:

Step 17 Access the Applications tab again.

Step 18 Click Start.

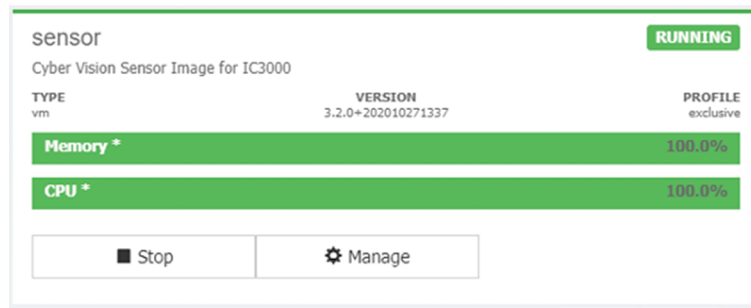


The application moves from Activated to Running state.

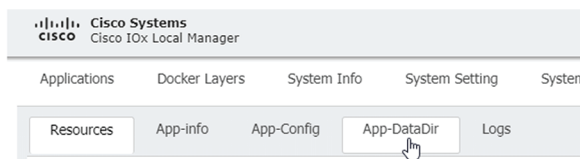
Step 19

Import the provisioning package

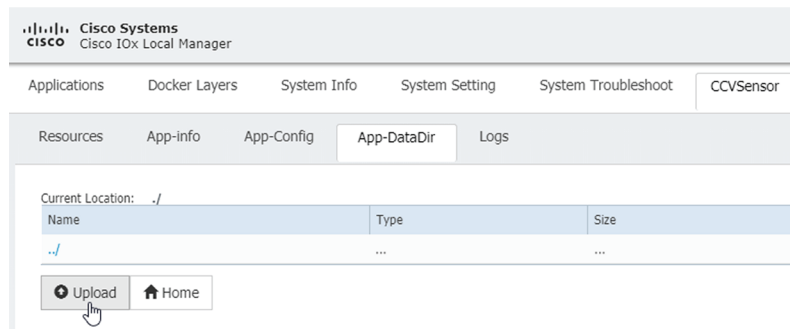
1. In the Local Manager, in the IOx configuration menu, click Manage.



2. Navigate to App_DataDir.



3. Before browsing the file, you must unzip the provisioning package.
4. Click Upload.



5. Navigate to the folder with the sensor serial name (i.e. FCH2312Y03F) > appconfigs, and select cybervision-sensor-config.zip.



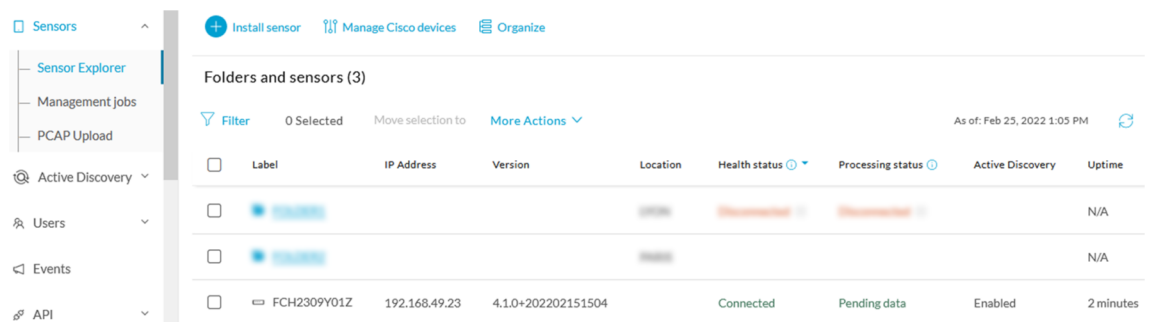
6. Make sure the path contains the entire file name (with .zip).



7. Click OK.

Reboot the Cisco IC3000

1. Disconnect the Cisco IC3000 from the DC Current source.
2. Connect the Cisco IC3000 to the DC Current source.
Wait a few moments for the boot to complete.
3. After a few seconds, the sensor appears as connected in Cisco Cyber Vision.



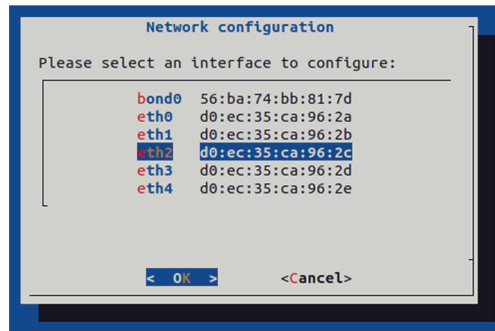
4. The Cisco IC3000 has been successfully installed. If the Cisco IC3000 has been connected to the Industrial Network, traffic starts to appear in Cisco Cyber Vision.

Enable Active Discovery

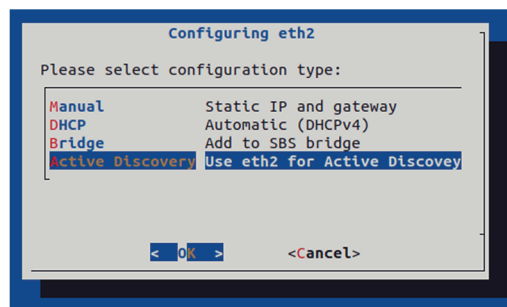
1. Connect to the Cisco IC3000 console and type the following command to set the Active Discovery interface.

```
root@sensor:~# sbs-netconf
```

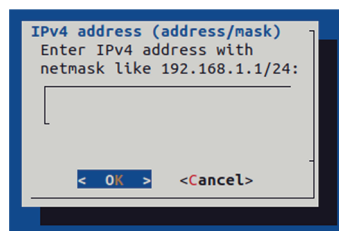
2. Choose which interface to configure between eth1, eth2, eth3 and eth4.



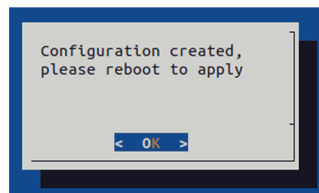
3. Select Active Discovery and make sure the right interface will be used for Active Discovery.



4. Type the subnetwork IP address dedicated to Active Discovery.



5. Select OK.



6. Type the following command to reboot the sensor.

```
root@sensor:~# reboot
```

7. On the Cisco Cyber Vision Sensor Explorer page, the sensor's Active Discovery status will switch to Enabled, and the Active Discovery button will appear on the sensor's right side panel. This may take a few moments.

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely managed. For the first time, you must authorize it so the Center can receive its data.

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Folders and sensors (3)

[Filter](#) 0 Selected [Move selection to](#) [More Actions](#)

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status
<input type="checkbox"/>	FCW2445P6X5				Disconnected
<input type="checkbox"/>	FCW2445P6X5				Disconnected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected

FCW2445P6X5

Label: FCW2445P6X5 [✎](#)
 Serial Number: FCW2445P6X5
 IP address: 192.168.49.21
 Version: 4.1.0+202202151440
 System date: Feb 24, 2022 4:13:06 PM
 Deployment: Sensor Management Extension
 Active Discovery: Enabled
 Capture mode: All

System Health
 Status: Connected
 Processing status: Normally processing
 Uptime: a day

[Go to statistics](#)

[Start Recording](#)

[Move to](#)

[Capture mode](#)

[Redeploy](#)

[Uninstall](#)

[Active Discovery](#)



Note You can change the Active Discovery configuration by clicking the Active Discovery button. However, for changes to be applied, you will have to download a new provisioning package and deploy it on the hardware.



CHAPTER 7

Upgrade procedures

- [Upgrade through the Local Manager, on page 45](#)
- [Upgrade with the combined update file, on page 49](#)

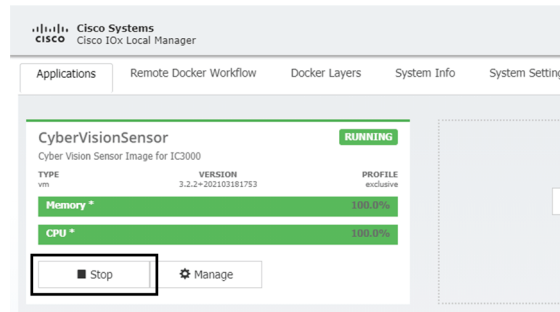
Upgrade through the Local Manager

The following section explains how to upgrade the sensor through the Local Manager.

In the Cisco Cyber Vision sensor administration page, the sensor is in 3.2.2. In the example below, we will upgrade the sensor to Cisco Cyber Vision version 3.2.3.

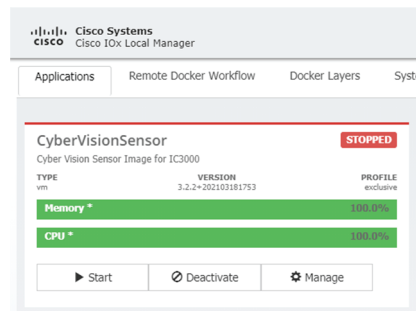
Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	27m 37s

1. Access the Local Manager.
2. Stop the application.



The operation takes a few moments.

The application status switches to STOPPED.



In Cisco Cyber Vision, the sensor status moves to Disconnected.

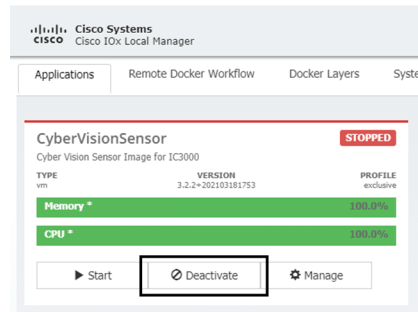
Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FOC2334V00H	192.168.69.20	3.2.3+202104292032	Connected	Pending data	Unavailable	All	4d 1h 5m 12s
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Disconnected SSH	Disconnected	Unavailable	All	N/A

S/N: FCH2312Y047
 Name: FCH2312Y047 ✎
 IP address: 192.168.70.20
 Version: 3.2.2+202103181753
 System date (UTC): Friday, April 30, 2021 9:42 AM
 Status: Disconnected
 Processing status: Disconnected
 Active discovery: Unavailable
 Deployment: Manual
 Capture mode: All
[Go to statistics](#)

Remove
Erase
Get Provision...
Capture Mode
Enable IDS
Shutdown
Reboot

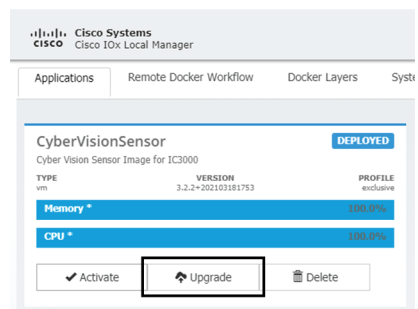
[UPDATE CISCO DEVICES](#)
[DEPLOY CISCO DEVICE](#)
[INSTALL SENSOR MANUALLY](#)
[IMPORT OFFLINE FILE](#)

- In the Local Manager, click the Deactivate button.

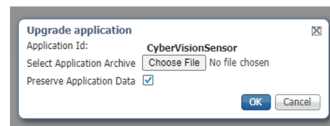


The application status moves to "DEPLOYED".

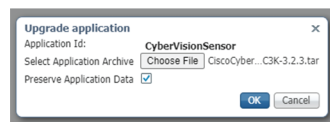
4. Click Upgrade.



The pop up Upgrade application appears.

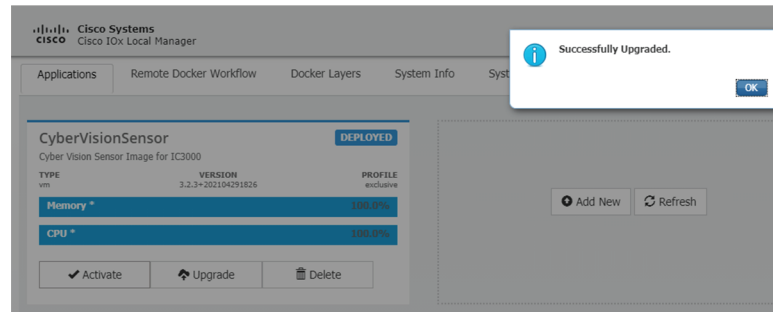


5. Select the option Preserve Application Data.
6. Select the new version of the application archive file.
e.g. Cisco-Cyber-Vision-IOx-IC3K-3.2.3.tar



The operation takes a few moments.

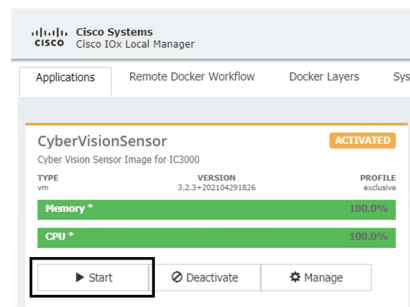
A message indicating that the sensor has been successfully upgraded is displayed.



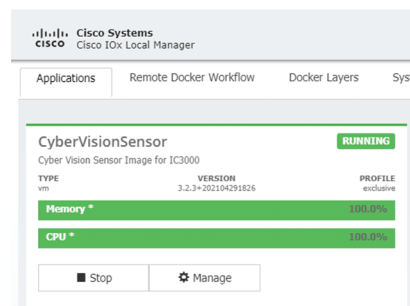
7. Check the number of the new version.
8. Click Activate.
9. Check configurations.

It can happen that network configurations are lost during the upgrade. If they are, refer to [Configure the sensor virtual application](#) and do as explained.

10. Click the Activate App button.
The application status moves to ACTIVATED.
11. Click the Start button.



The application status changes to RUNNING.



In Cisco Cyber Vision, the sensor is upgraded from version 3.2.2 to 3.2.3 and its status moves to Connected.

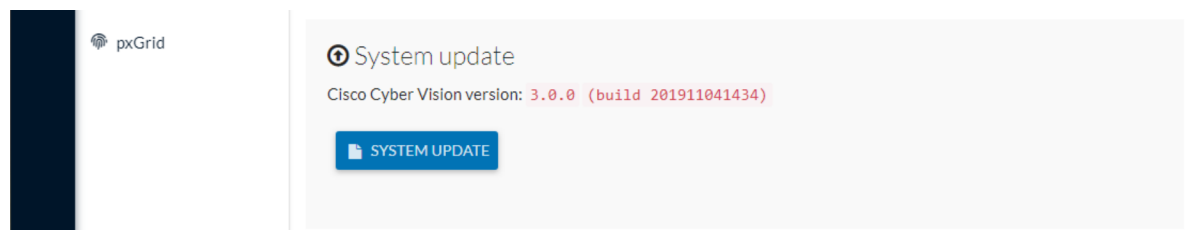
Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode [®]	Uptime
▶ FOC2334V00H	192.168.69.20	3.2.3+202104292032	Connected	Pending data	Unavailable	All	4d 2h 17m 23s
▼ FCH2312Y047	192.168.70.20	3.2.3+202104291826	Connected	Pending data	Unavailable	All	1m 22s

S/N: FCH2312Y047
 Name: FCH2312Y047 ✎
 IP address: 192.168.70.20
 Version: 3.2.3+202104291826
 System date (UTC): Friday, Apr 11 30, 2021 10:02 AM
 Status: Connected
 Processing status: Pending data
 Active discovery: Unavailable
 Deployment: Manual
 Uptime: 1m 22s
 Capture mode: All
 ● Start recording sensor
 📊 Go to statistics

Remove
Erase
Get Provision...
Capture Mode
Enable IDS
Shutdown
Reboot

UPDATE CISCO DEVICES
DEPLOY CISCO DEVICE
INSTALL SENSOR MANUALLY
IMPORT OFFLINE FILE

Upgrade with the combined update file



Version releases usually include updates for both the Cisco IC3000 sensors and the Center (i.e. combined updates). If operating conditions make it possible, you can update the Center and all its Cisco IC3000 online sensors at once from the user interface. You can proceed to a combined update without opening a shell prompt and using SSH.



Note

Combined updates are applied to the Center and all its Cisco IC3000 online sensors. Make sure (by accessing the sensor administration page) that all your Cisco IC3000 sensors are connected and SSH is authorized between the Center and the sensors before proceeding to a combined update.



Important

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

Requirements:

- A combined update, available on cisco.com.

To verify that the file you just downloaded is healthy, it is recommended to use the SHA512 checksum provided by Cisco.

To do so (Windows users):

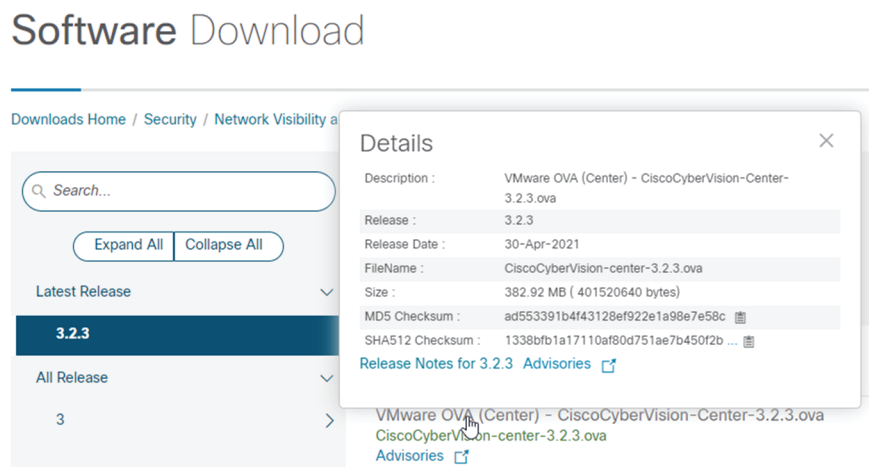
Procedure

- Step 1** Access Cisco Cyber Vision download page.
- Step 2** Download the file.
- Step 3** Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:
Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List

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

Algorithm : SHA512
Hash      : 13388f81a17110af80d751ae7b450f2829cc84c854f550f3888e684236865ec9edf7773fd05d1055c7f1ef76e68c2b8a9cfe69ab
          : 18622e480888eb89e94d816
Path      : C:\Users\ \Downloads\CiscoCyberVision-center-3.2.3.ova
```

- Step 4** In the download page, mouse over the file and copy the SHA512 checksum.



- Step 5** Compare both checksums.
- If both checksums are identical it means the file is healthy.
 - If the checksums do not match try to download the file again.
 - If, after downloading the file again the checksums still don't match, please contact Cisco support.

To update the Center and all its Cisco IC3000 online sensors:

- Step 6** Access the Cisco Cyber Vision's user interface.
- Step 7** Access System administration > System and use the System update button.
- Step 8** Select the update file CiscoCyberVision-update-combined-<VERSION>.dat
- Step 9** Confirm the update.

As the Center and sensors updates proceed, you are redirected to a holding page. Once the update is finished the Center and the sensors need to reboot and you will be logged out from the user interface.

- Step 10** Log in again to the user interface.

Step 11

If some sensors were offline when the update occurred, the same procedure can be used as many times as necessary to update all sensors.
