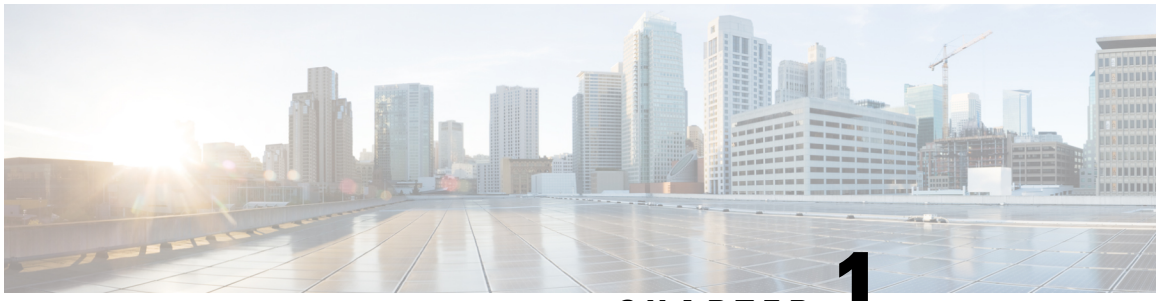
Cisco Cyber Vision Center Appliance Installation Guide, Release 5.5.x

First Published: 2025-09-09

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

Supported Cisco UCS and upgrade procedures

The installation guide covers these Cisco Unified Computing systems:

- Cisco Unified Computing C220 M5
- Cisco Unified Computing C225 M6
- Cisco Unified Computing C225 M8

View these notes about hardware lifecycles before you begin.

- Older hardware generations, such as M5 and M6, are phased out. This maintains performance and security standards.

Hardware	Last day to order
UCS C220 M5	December 31, 2023. For more information, see End-of-Sale and End-of-Life Announcement for the Cisco Cyber Vision Center, M5 series appliance.
UCS C225 M6	June 18, 2026. For more information, see End-of-Sale and End-of-Life Announcement for the Cisco Cyber Vision Center on UCS M6 series appliance.

- The M8 series UCS serves as the current, supported platform for the Cyber Vision Center physical appliance.

Use this guide to find upgrade procedures for:

- Architectures with a Global Center

- Architectures with one Center only

Warnings and notices

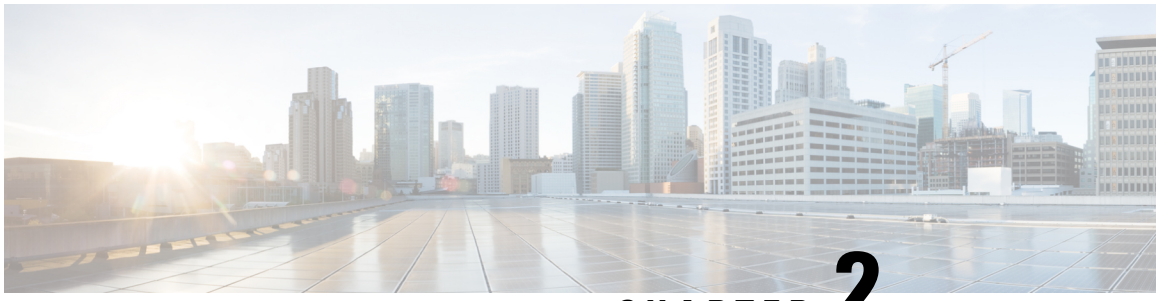
This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

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 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

Information and characteristics

Information and characteristics

The solution can have a 2-tier or 3-tier architecture made of:

- **Edge sensors** which are installed in the industrial network. These sensors are dedicated to capture network traffic, decode protocols using the Deep Packet Inspection engine and send meaningful information to the Center.
- The **Center**, a central platform gathering data from all the Edge Sensors and acting as the monitoring, detection and management platform for the whole solution.
- Optionally, a third-tier **Global Center** to which all Centers are connected, for a central view of all Centers deployed within an organization for alerting, reporting and management functions.

To safeguard the data collected from the industrial network and ensure maximum reliability, the Center includes a RAID storage array. It also includes redundant internal cooling fans (x3) and dual hot-swappable power supplies.

During the installation of the Center, you will have the opportunity to set up Center data synchronization to a Global Center. Although, if you choose to set up a global infrastructure, you must install the Global Center first, then the Centers, and finally, the sensors.

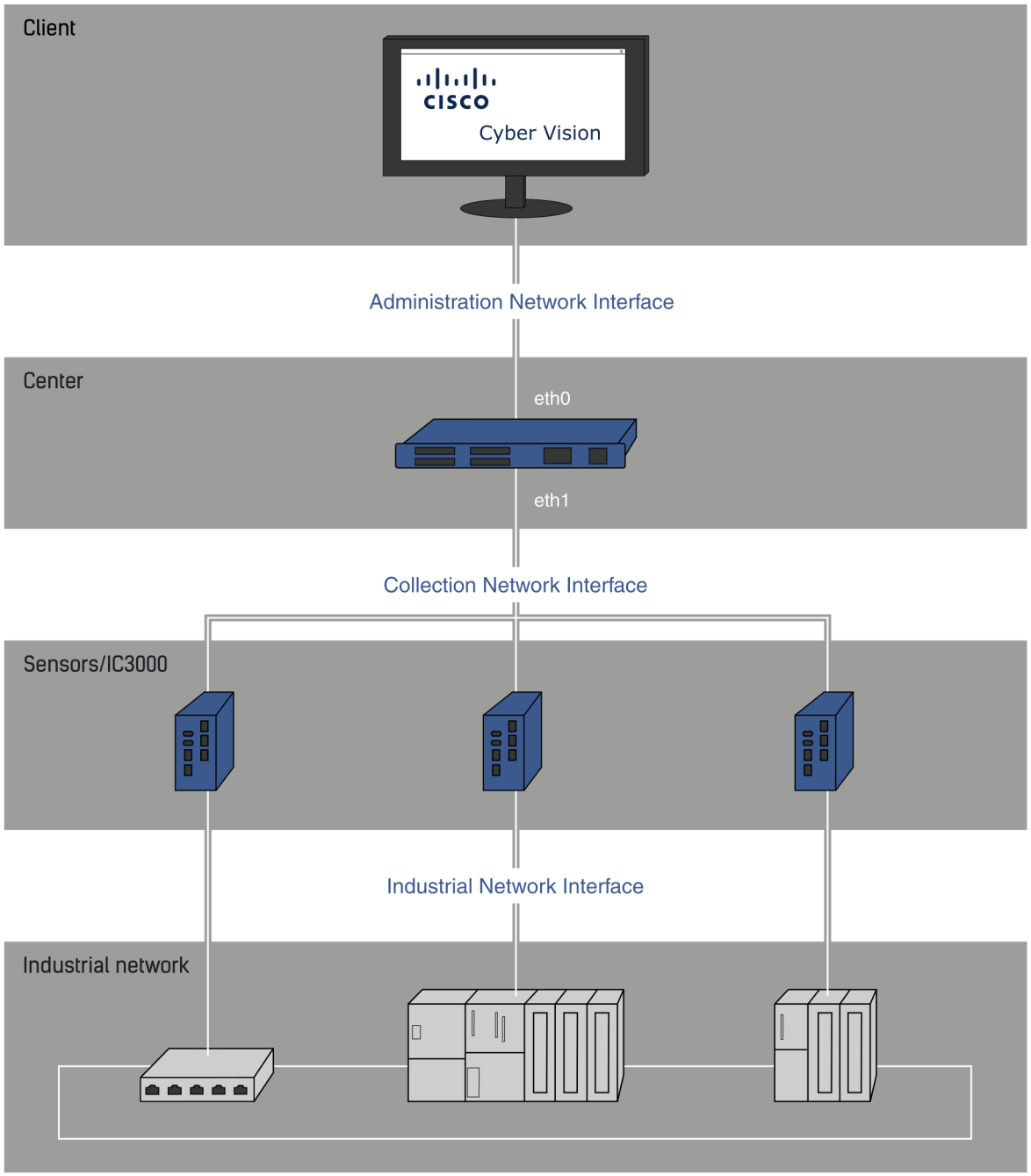
Networks or segments involved

From perspective, three important networks will be involved with the platform:

- The **Administration network**, used to access the Center User Interface (UI) and interact with authorized external services (NTP, DNS, API, SIEM, etc.).
- The **Collection network**, used to manage all sensors. This network must be isolated from the operational traffic plant (separated VLAN/subnet).
- The **Acquisition/Industrial network**, used for all industrial plant traffic and/or external interconnection under consideration that will be analyzed by the sensors (SPAN traffic collected).

Example of a installation (without Global Center):

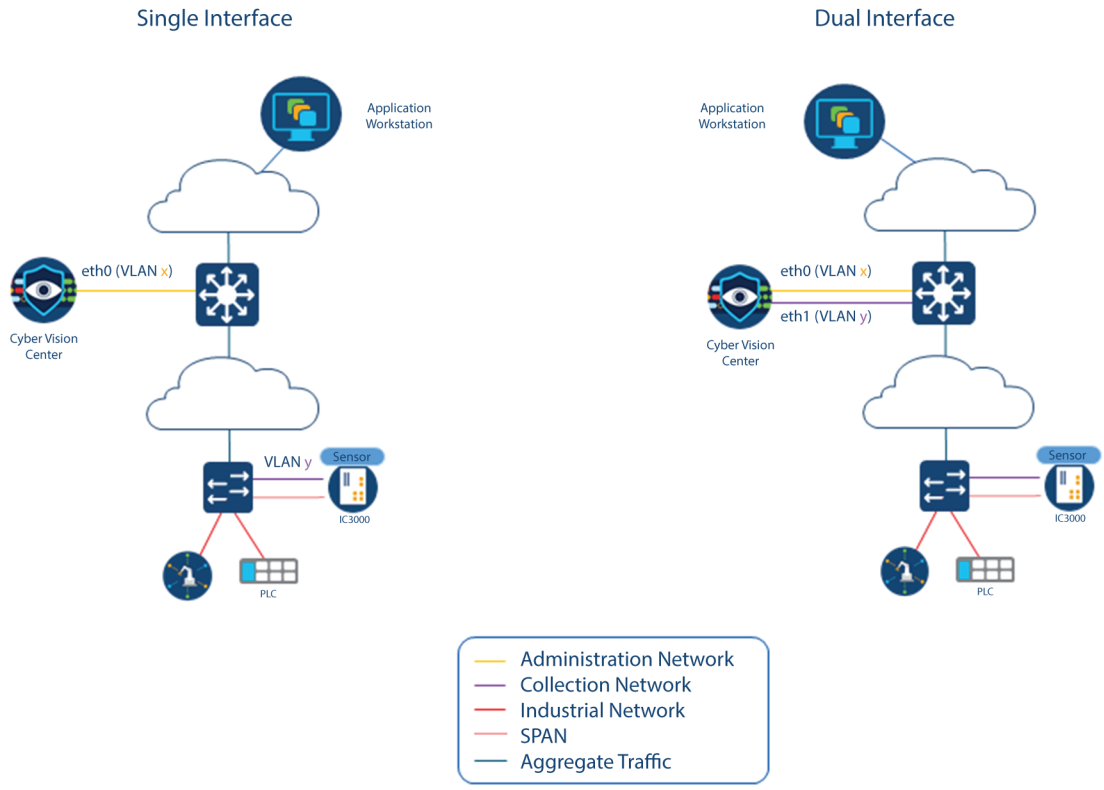
Information and characteristics



Configuring single or dual interface (not applicable to a Global Center)

For security reasons, it is recommended to use the Center on **two separate networks**, respectively connected to the following interfaces:

- The **Administration network interface (eth0)**, which gives access to the user interface.
- The **Collection network interface (eth1)**, which connects the Center to the sensors.



The Center provides two dedicated and separate 10 Gigabit Ethernet network ports to connect to these two networks.

However, in case of incompatibility with the industrial network infrastructure or for limited environments, you can use a single network interface (eth0).

Refer to the Architecture Guide for more information about defining environment configuration.

IPv6 support for Cyber Vision administration services

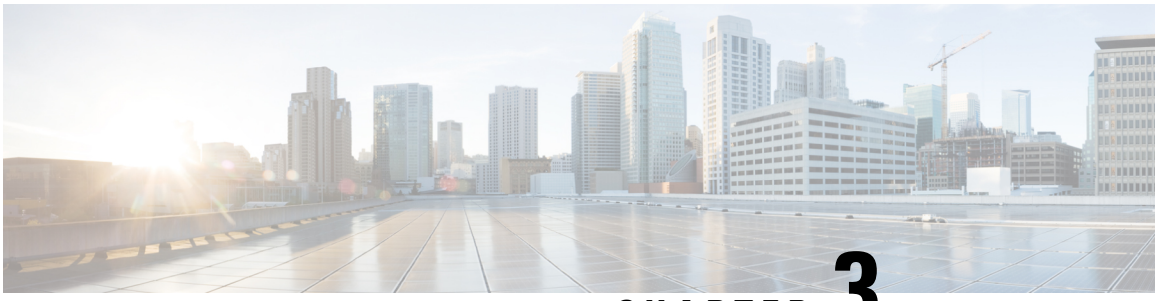
You can use both IPv4 and IPv6 protocols for Cisco Cyber Vision administration services.

You can use IPv6 on Center `eth0` for administration-related access, including:

- Accessing Cisco Cyber Vision from a browser.
- Integrating with external services such as syslog and LDAP.

Consider these limitations:

- License operations work only with direct transport. Transport Gateway and HTTP/HTTPS Proxy are not supported.
- Sensor data collection uses only IPv4, whether performed on `eth0` or `eth1`.



CHAPTER 3

Connect the Center

Connecting centers before power-up

Summary

Connect the Cisco Center before powering it on to configure locally and ensure all network interfaces operate correctly. This helps you prevent connectivity issues and deploy efficiently.

The key components involved in the process are:

- Input devices: Allow you to access and configure the Center locally via monitor and keyboard or serial console.
- Network interfaces: Enable communication between the Center and user interfaces, sensors, or the Global Center, depending on deployment requirements.
- Power supply: Provides the energy you need to operate the Center.

Workflow

The process involves these stages:

1. Connect input devices:
   - For local configuration, connect a monitor to the VGA port and a keyboard to any available USB port.
   - Alternatively, for console access, connect a console cable to the serial console port.
   - The supported models for this configuration include Unified Computing C220 M5, C225 M6, and C225 M8.
2. Connect network interfaces:
   - For Global Center deployments, connect a network cable to the eth0 interface.
   - If the Center has dual network interfaces, connect the administration network cable to the Administration LAN port (eth0) and the collection network cable to the Collection LAN port (eth1).

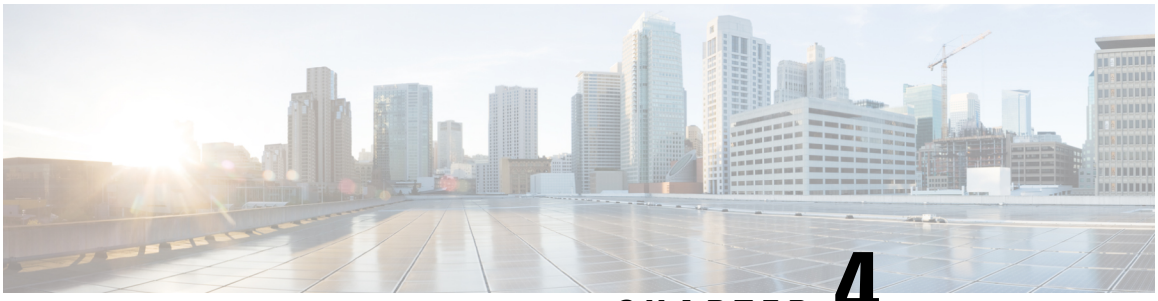
- If the Center has a single network interface, connect the network cable to the eth0 interface to handle both administration and collection traffic.

Note On Unified Computing System, eth0 is port 1 and eth1 is port 2.

3. Connect power supply and power on:
   - Connect the power supply cables to the unit.
   - Locate the power button on the front panel of the Center.
   - Press the power button to power on the unit.

Result

Your Cisco Center is connected, powered on, and ready for you to configure locally and begin network operations.



CHAPTER 4

Configure the Center

You will need to complete two steps to configure the Center:

1. The basic Center configuration through a VGA display and a keyboard or a console, to:
   - Set the Center and the sensor passwords.
   - Synchronize the Center to the NTP server.
   - Configure the Administration and Collection interfaces (n/a for a Global Center or a Center using a single interface).
2. The configuration, through a browser, to:
   - Create an admin account.
   - Configure the Center's data synchronization (Global Center and synchronized Centers only).

- Basic Center configuration, on page 9
- configuration, on page 21

Basic Center configuration

This step will allow you to configure the Center network settings before using it with the user interface.

Required information:

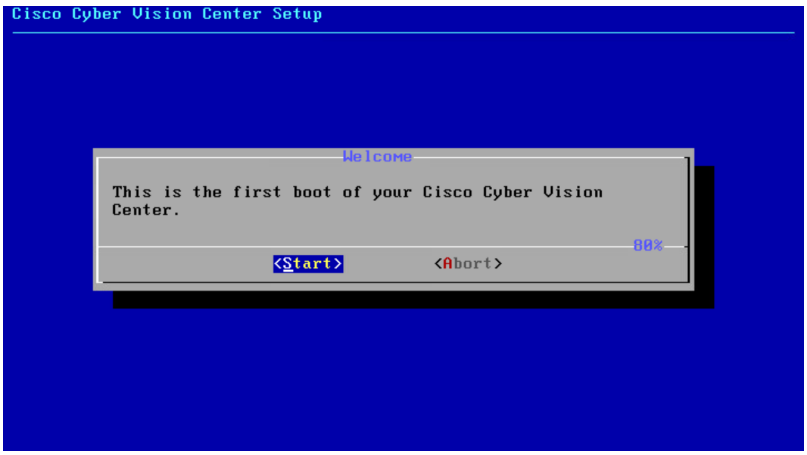
- Local NTP and DNS IP addresses.
- The Collection interface network address (n/a for a Global Center or a Center using a single interface).

In the case of manual Administration network interface configuration:

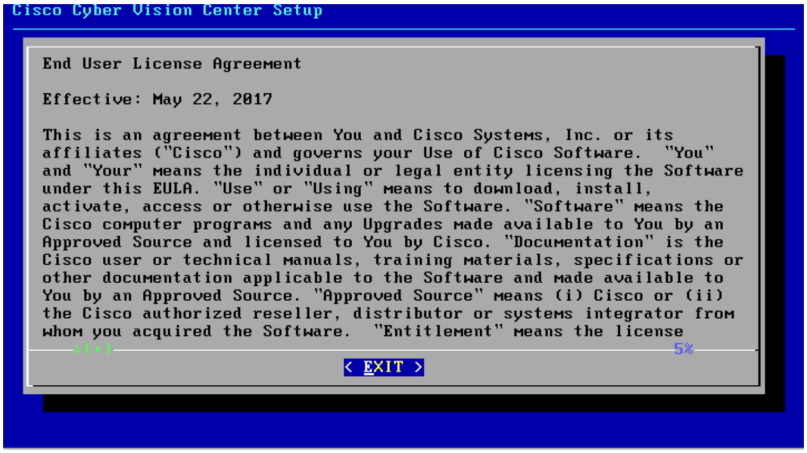
- Its IP address.
- Its netmask (in a two-number format, e.g. 192.168.1.0/24).
- Its default gateway (to reach devices located outside the local network).

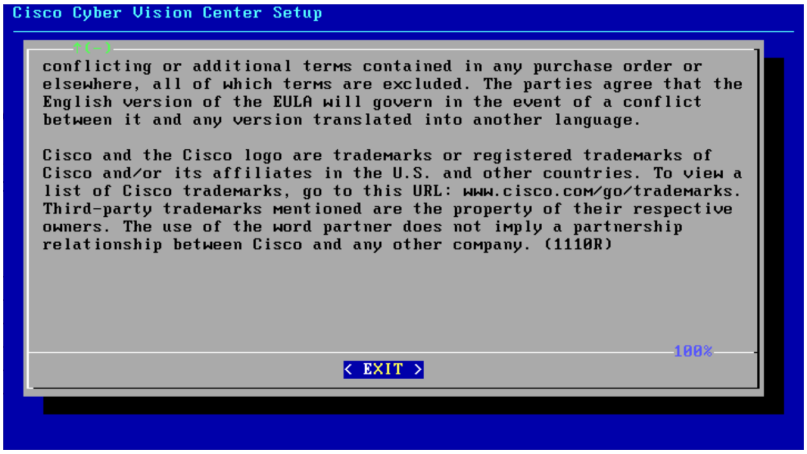
Access the basic Center configuration

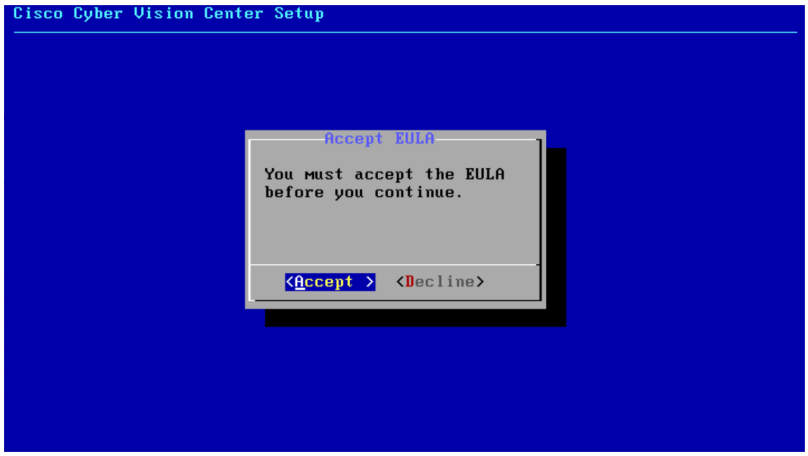
The Center wizard is displayed on your screen as you power on the Center. Enter Start to start configuring the Center.



Accept the End User License Agreement

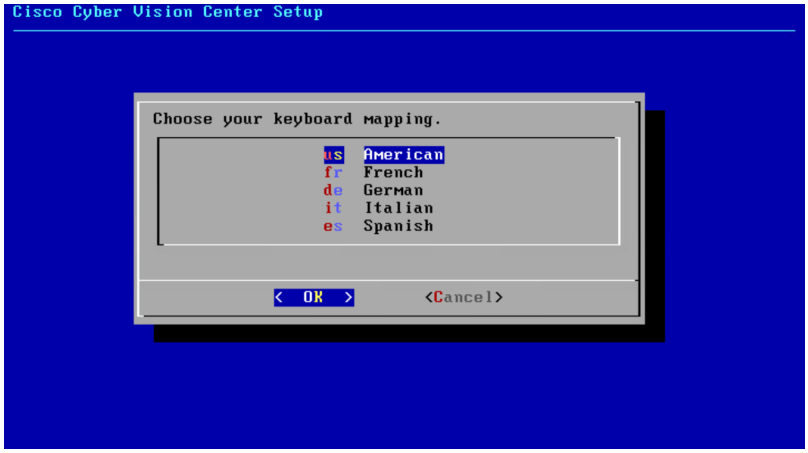






Select the language to match your keyboard

Note By default, the system is configured to work with a US QWERTY keyboard.

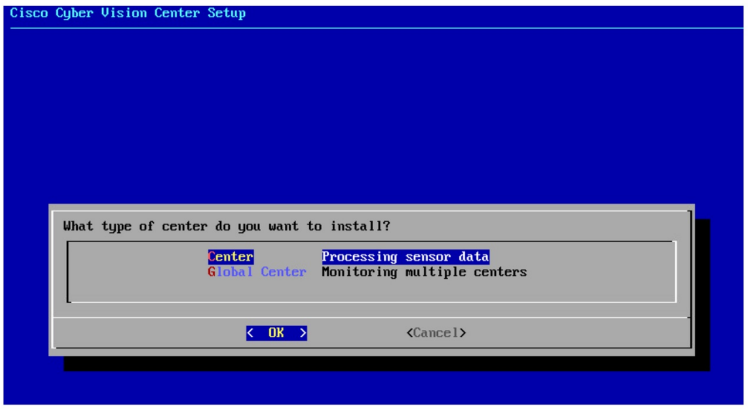


Select the Center type

During this procedure you will choose which type of Center to install. There are two types of Centers:

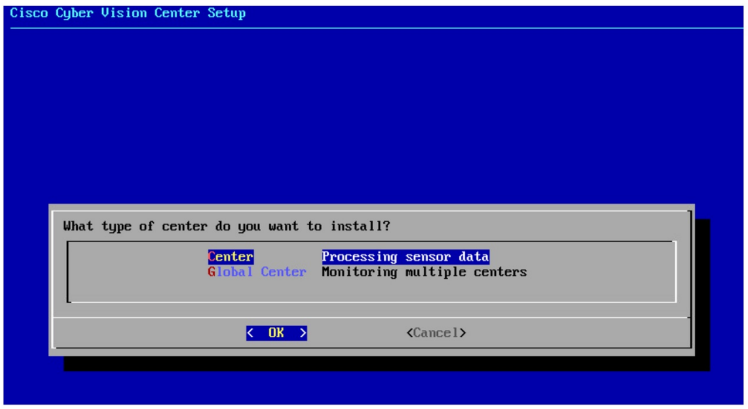
- A **Center** receives metadata from sensors and store them into an internal database (Postrgresql). It can be standalone or synchronized with a Global Center. A Center with sync is similar to a standalone Center from a functionality point of view, except for the link to a Global Center. You must install Centers with sync **after** the Global Center. This will enable the system to enroll and start pushing events to the Global Center.
- A **Global Center** introduces a centralized architecture which collects all industrial insights and events from synchronized Centers and aggregates it on a single global point of view. It will also allow you to manage the knowledge database (KDB) and upgrade the whole platform.

Select the type of Center you want to install.



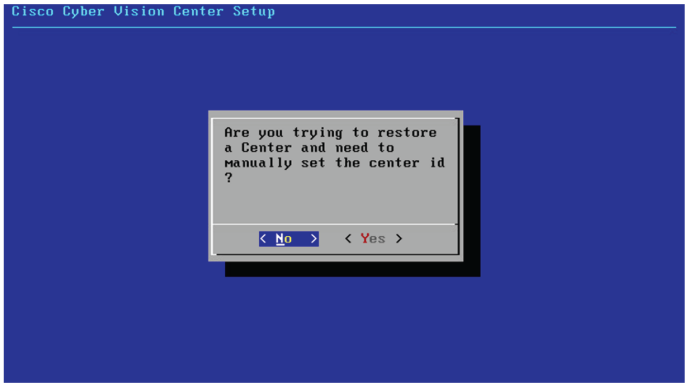
Center

If installing a Center, select the first option.



Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

If you're installing the Center for the first time, this id will be automatically generated. Select No. You will be directed to the next step.

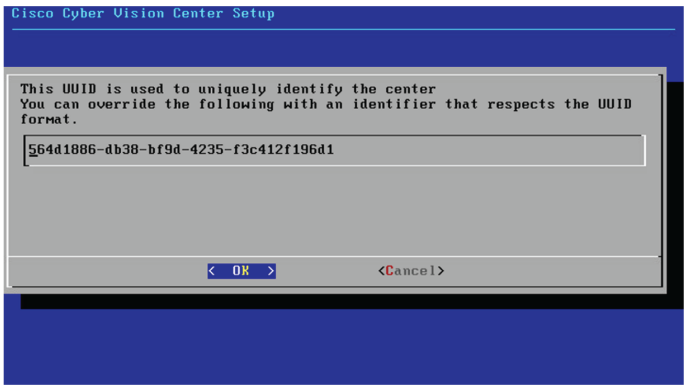


If you're reinstalling the Center and want to restore it, select Yes.

Use the following command from the Global Center's CLI to get a list of all Center's id:

```
sbs-db exec "select name, id from center"
```

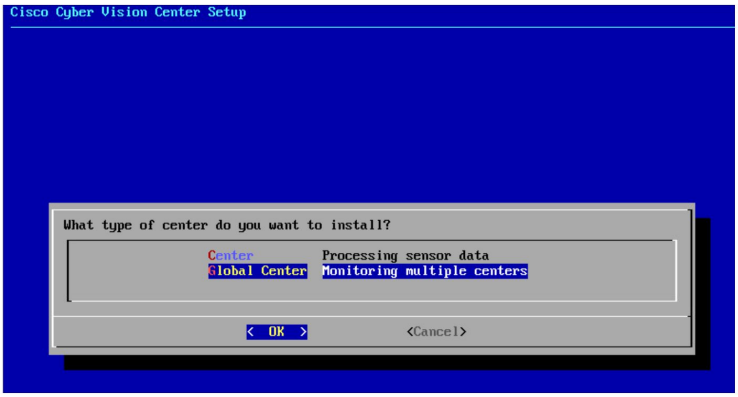
Type the id into the basic Center configuration UUID field.



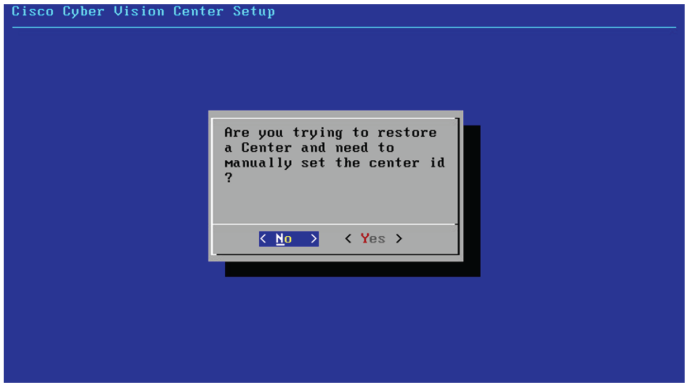
Click OK. You will be directed to the next step.

Global Center

If installing a Global Center, select the second option.



As this step does not apply to a Global Center, select No.



You will be directed to the next step.

Configure the administration network interface

Change the default administration network interface configuration to fit your environment.

The administration network interface supports IPv4 addressing or both IPv4 and IPv6 addressing. You can configure the interface using DHCP or enter the settings manually.

- IPv4: Communication with the sensors will still be done using IPv4.
- IPv6: Cyber Vision uses IPv6 only on the access interface.

Procedure

Step 1 Select either **IPv4** or **IPv4/IPv6** for the administration network interface.

Step 2 If you select **IPv4**:

- Select **DHCP** to allow the system to receive configuration from a DHCP server.
- Select **Manual** to enter the IP address, the netmask (in two-number format), and the gateway.

Step 3 If you choose **IPv4/IPv6**:

a. First, configure **IPv4** as described earlier.

b. Then, for **IPv6**:

- Select **DHCP** to obtain configuration from a DHCP server.
- Select **Manual** to enter the IP address, the prefix length, and the gateway. The system uses router advertisements.
- Select **Manual no RA** to manually enter the IP address, the prefix length, and the gateway. This option ignores router advertisements.

The administration network interface is configured using your chosen addressing and assignment method.

Network interface deployment options

The network interface configuration defines how Cisco Cyber Vision Center connects to your network, supporting both single and dual-interface modes to address different security and deployment needs.

- Single-interface configuration combines administration and collection functions on a single interface (eth0).
- Dual-interface configuration enhances security by physically segregating administrative access (eth0) from sensor data collection (eth1).

The following table compares the dual-interface and single-interface configurations.

Table 1: Comparison of dual-interface and single-interface configurations

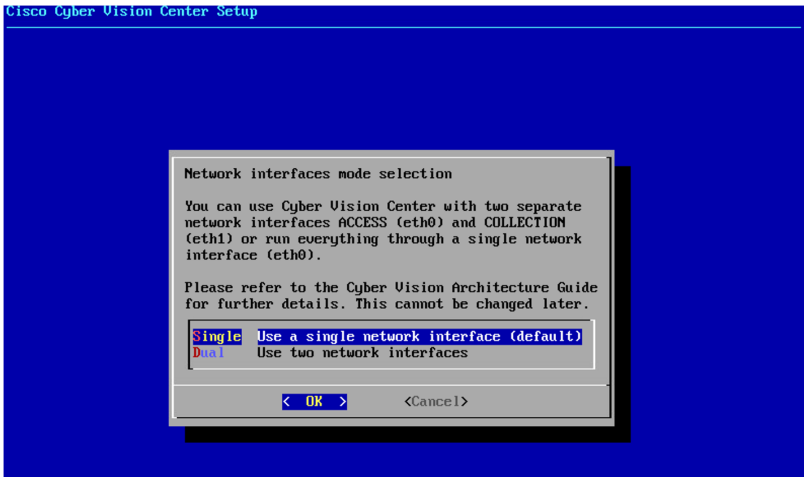
Attributes	Dual-Interface	Single-Interface
Number of interfaces	2 (eth0, eth1)	1 (eth0)
Traffic separation	Yes (administration and collection are isolated)	No (all traffic on single interface)
Security level	Higher	Lower
Recommended use	Standard deployments	Limited infrastructure

Set interfaces (dual or single)

This step is not applicable to a Global Center.

Regarding a Center, it is possible to:

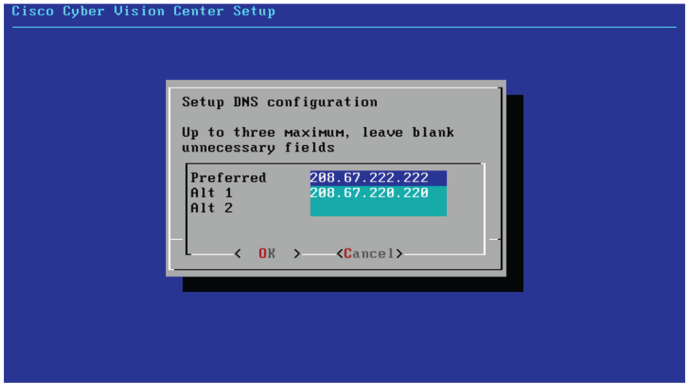
- Use a single interface. In this case, select the Single option.
- Set the Administration and Collection network interfaces on two distinct interfaces (recommended for security). In this case, select the Dual option.



If you choose the Dual option, you will later be directed to: Configure the Center's Collection network interface, on page 19.

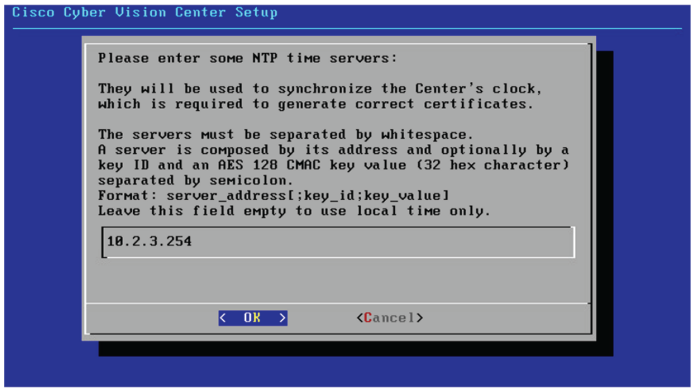
Configure the Center's DNS

Type a DNS server address and optional fallbacks.

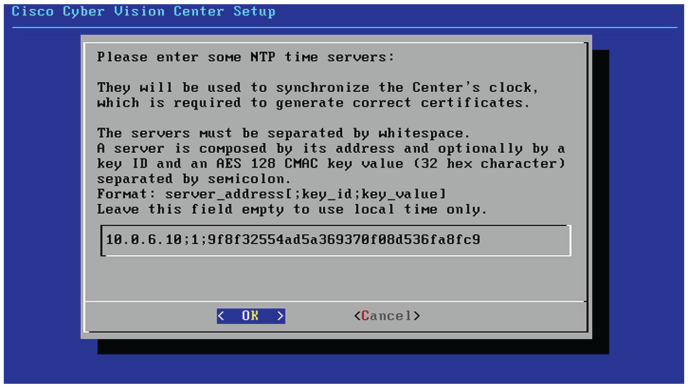


Synchronize the Center and the sensors to NTP servers

Enter IP addresses of local or remote NTP servers (gateway configuration needed) to synchronize the Center and the sensors with a clock reference. Each address must be separated by a space.



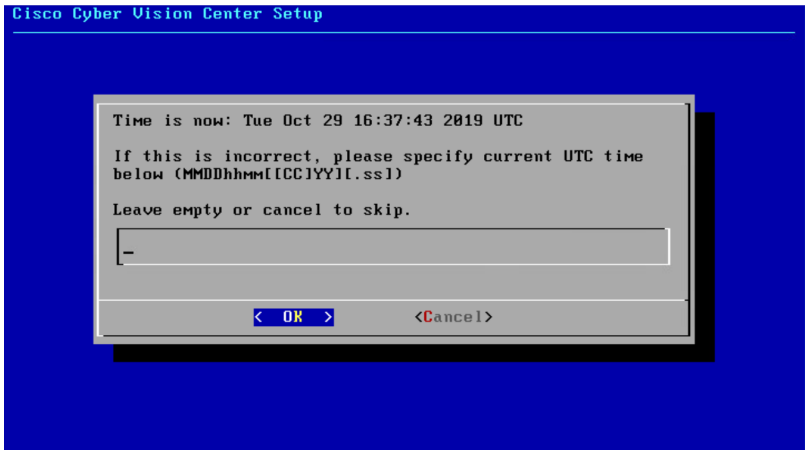
Optionally, add a key ID and an AES A28 CMAC key value separated by a semicolon with the corresponding NTP server.



The synchronization takes a few seconds.

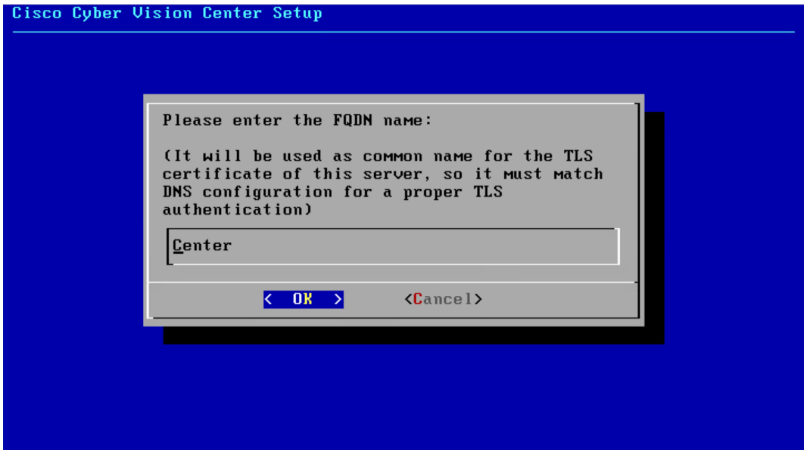
Check that the time is correct, or set the time manually.

Note The time is set in UTC standard.



Give the Center a name

Note This name will be used in the Center certificate.

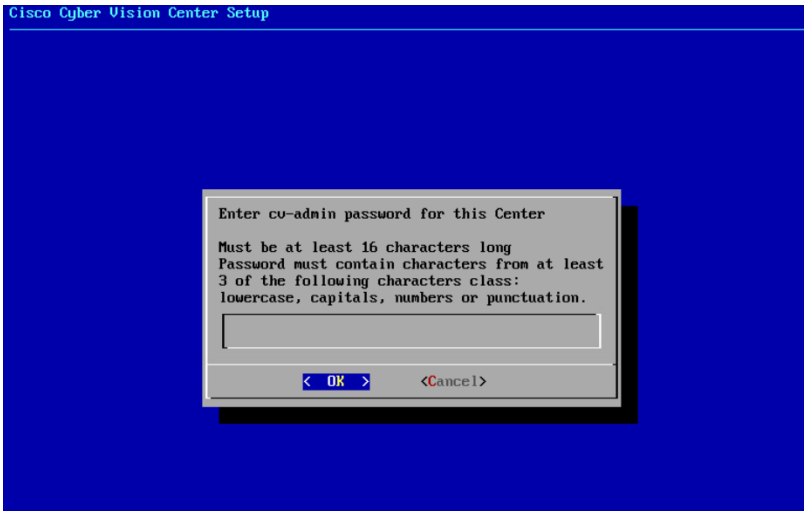


Enter the Center name provided by your administrator or type 'Default' which is a secure value.

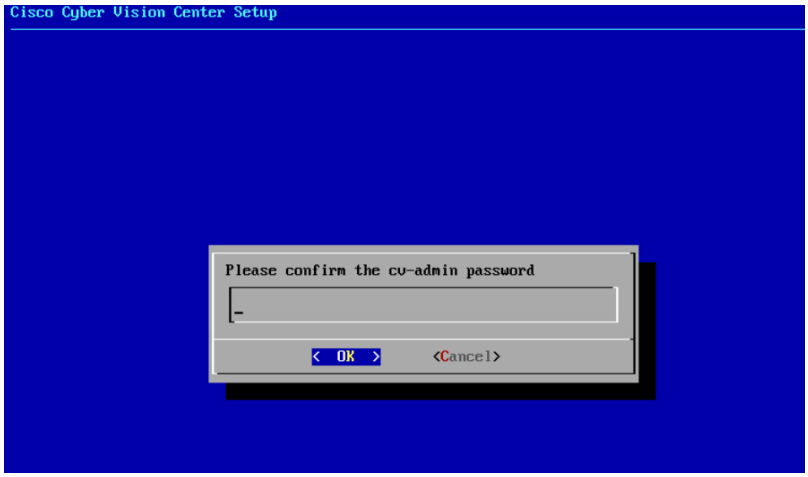
Note This name must match the DNS name you will use to access the Center through SSH or a browser.

Set the Center's password

The administrator account (i.e. cv-admin) password of the Center must be set for security reasons. It is hidden for confidentiality reasons.



Confirm the password.

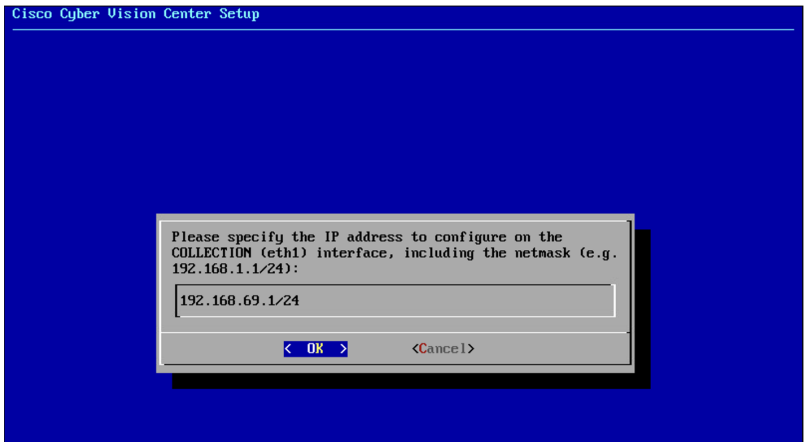


Configure the Center's Collection network interface

This step is not applicable to a Global Center.

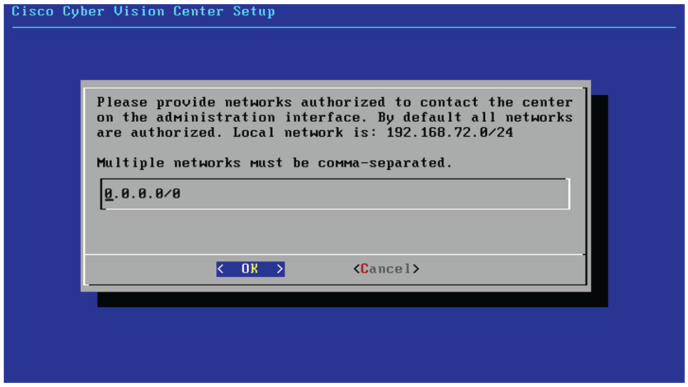
This step will only appear if the dual interface option has been selected during the Set interfaces (dual or single), on page 15 step.

Type the IP address of the Collection network interface:



Authorize networks

This step allows you to restrict IP addresses that can connect to the Administration interface. If no IP is entered, all networks are authorized by default.



Complete basic Cyber Vision Center configuration

Finalize the initial setup of Cyber Vision Center and secure needed addresses for future login and certificate management.

Before you begin

Ensure previous center configuration steps are complete.

Procedure

Step 1 Record the displayed addresses for downloading the CA certificate and accessing Cyber Vision Center.

If you have selected **IPv4/IPv6** in the earlier step, addresses for both IP versions appear.

Step 2 Select **OK** to complete the configuration.

Step 3 Close the configuration window.

Step 4 Open your browser and go to the saved address to access Cyber Vision Center.

You have completed the basic configuration and recorded the essential access and CA certificate addresses.

What to do next

- To connect via CLI (serial console or SSH), use ‘cv-admin’ as the username and the instance ID as the password. This user has limited rights. To elevate permissions, prefix commands with "sudo" or open a root shell with "sudo -i".
- Each Cyber Vision Center includes its own PKI and CA for TLS connections. Install the CA certificate on each client browser. See the instructions in the relevant chapter for steps to install the CA certificate.

configuration

Once the Basic Center configuration is done, you must connect through a web browser to the URL displayed on the last step of the basic configuration wizard (i.e. the Center's IP address). A message saying that the URL is not secure will appear.

- If you plan to use a self-signed certificate, you must Install the certificate in your browser, on page 21 and then access the user interface installation wizard to configure users and sensors.
- If you plan to use an enterprise certificate, you must ignore the security message and perform the following steps in this order:
  1. Access the user interface installation wizard to configure users and sensors.
  2. Configure the security of the user interface itself.

Then, you will configure the Centers data synchronization (Global Center and its Centers' only).

Browser requirements:

supports Chrome 54, Firefox 49 and newer versions.

Install the certificate in your browser

This task explains how to intall a Cisco Cyber Vision self-signed certificate in your browser.

Before you begin

Perform this task if you aim to install a self-signed certificate. If you're planning to use an enterprise certificate, proceed directly with Install , on page 26.

Procedure

Step 1 Open your browser.

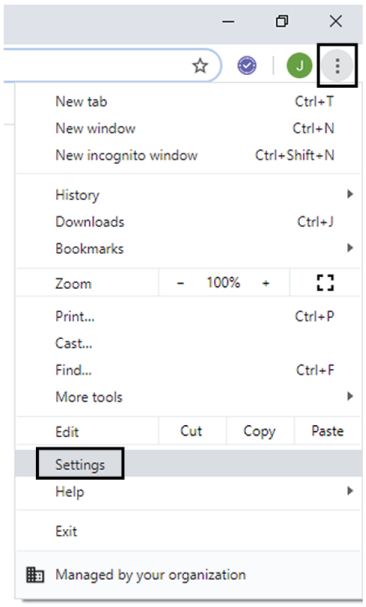
Step 2 Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.

The certificate is downloaded.

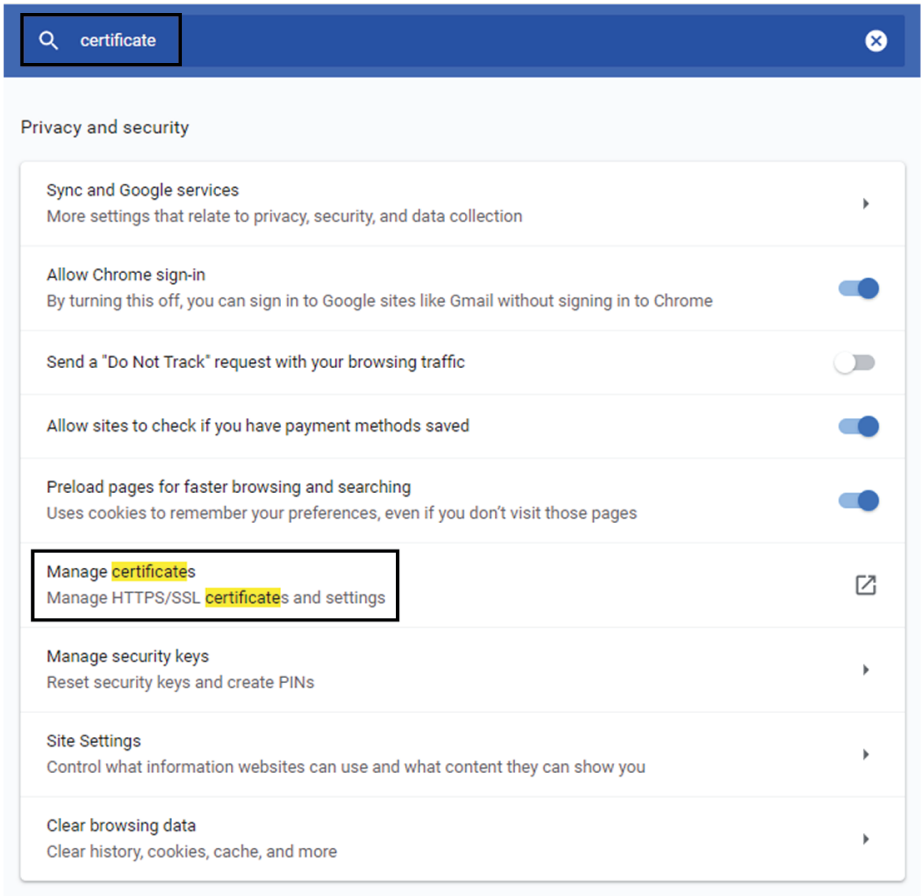
Step 3 Save the certificate on your computer.

Step 4 In the browser, access the settings.

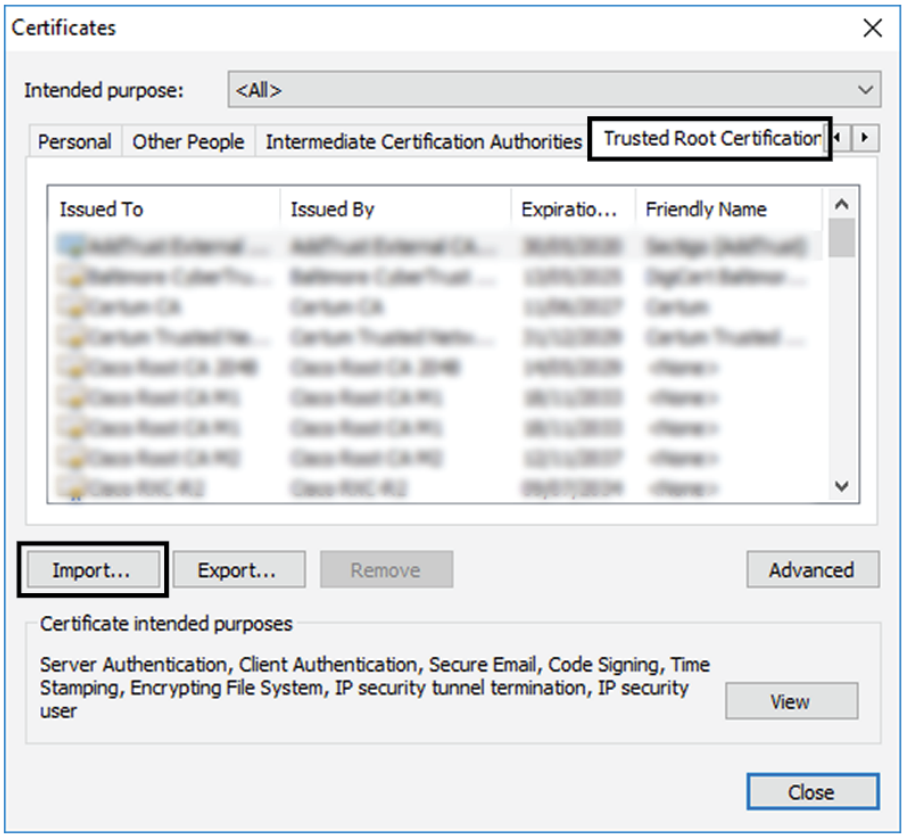
Example: Chrome



Step 5 Type 'certificate' in the search bar and access the certificates management menu.

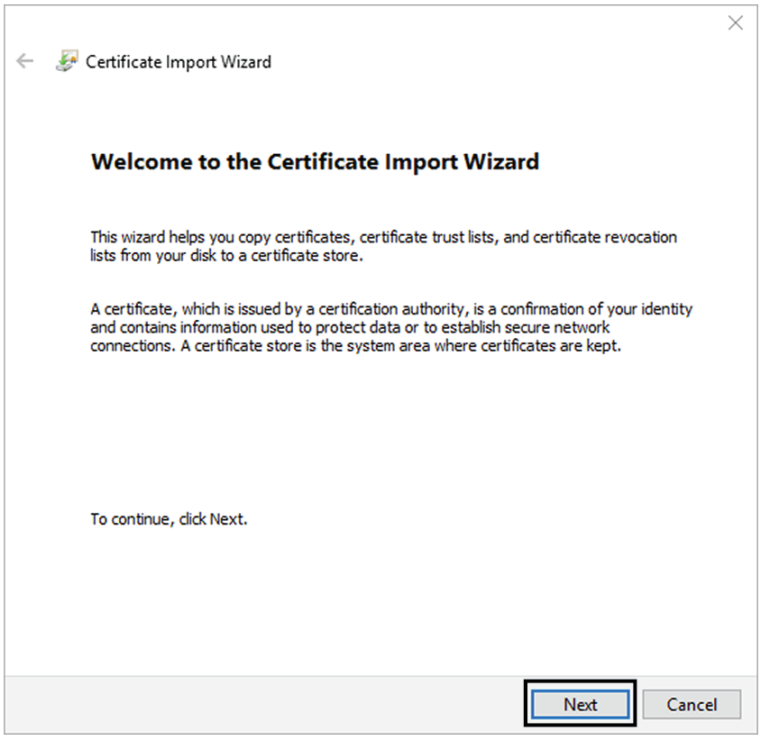


Step 6 Access the Trusted Root Certification tab and click Import.



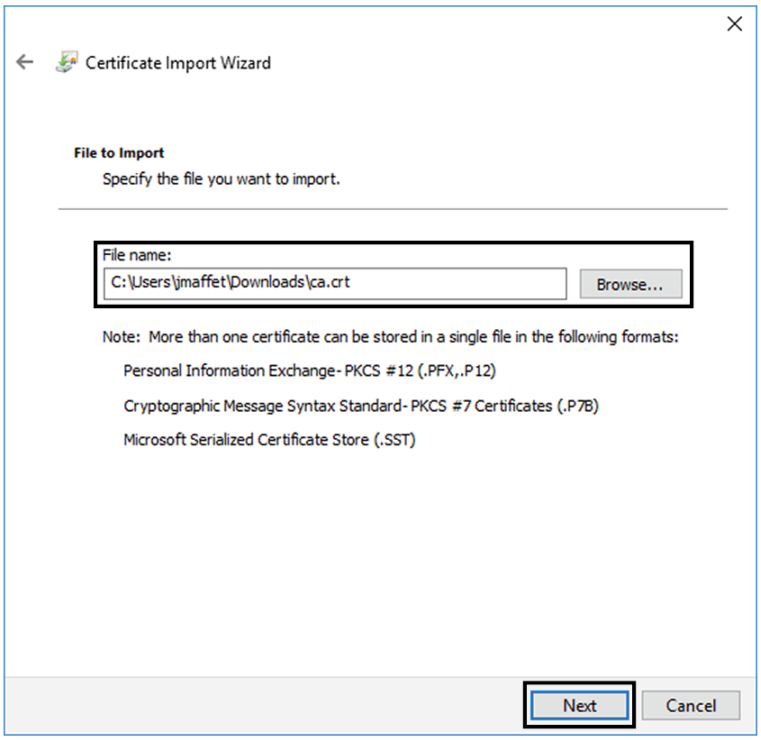
A certificate importation wizard opens.

Step 7 Go to the next step.

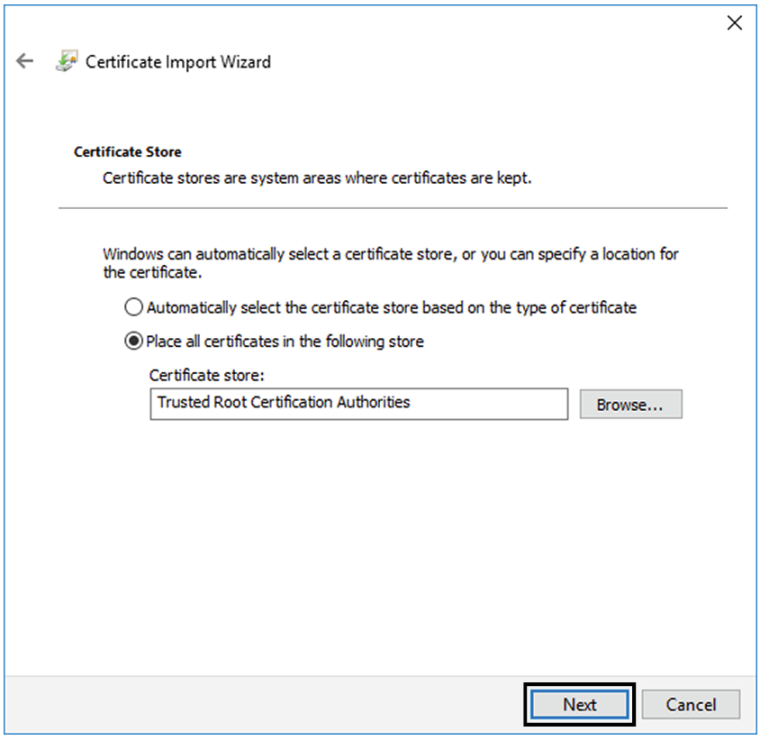


Step 8 Search for the certificate you downloaded earlier.

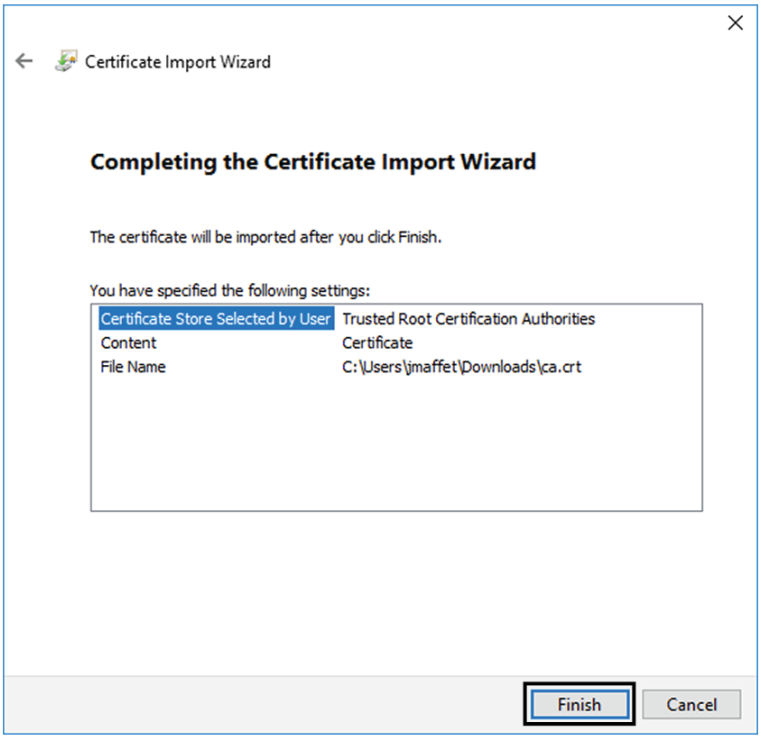
Step 9 Go to the next step.



Step 10 Accept the default values by accessing the next step.



Step 11 The certificate is now considered as trusted by the browser. It will be imported as soon as you will click Finish.



What to do next

Install , on page 26

Install

Access the installation wizard:

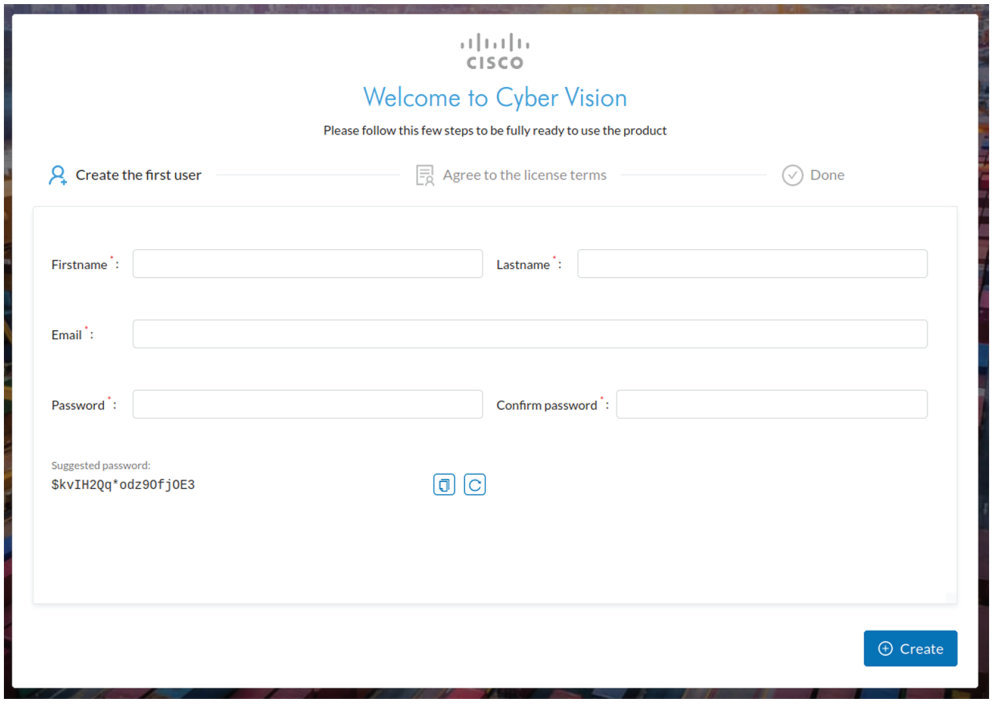
Procedure

Step 1 With your browser, access https://**<CENTERNAME>**/.

Note
Accessing the Center using its name enables HTTPS secure interface. Yet, this requires a DNS or local host configuration to associate the name and the IP address. The Center access through its IP address is possible but the connection is not secure.

Step 2 The setup wizard used for the first access to is displayed:

Step 3 **Create an admin account:**



Step 4

Step 5 Enter the information required.

Note
Email will be asked for login access.

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

- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#$%&’()*+,-./:;<=>?@[]^_{|}.

Passwords should be changed regularly to ensure the integrity of the platform and the industrial network security.

Note
You can reset users using the following command in the Center's CLI:

```
sbs-db reset-users
```

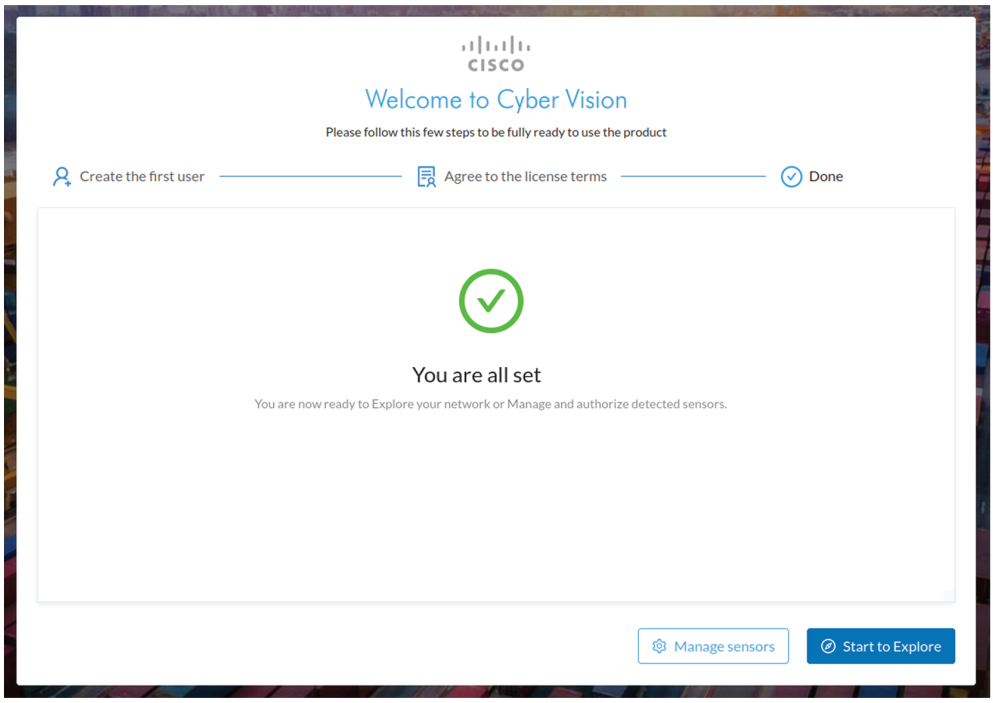
Step 6 **Accept the software license agreement:**

Step 7

Step 8 **Finish the installation:**

The Center is now correctly installed and is ready to operate.

Step 9 Click Start to Explore.



installation is now complete.

What to do next

If you aim to use an enterprise certificate, proceed with Configure the user interface security, on page 29.

If you already installed a self-signed certificate, and if you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 34.

If you already installed a self-signed certificate, and if you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Sensor Installation Guides.

Configure the user interface security

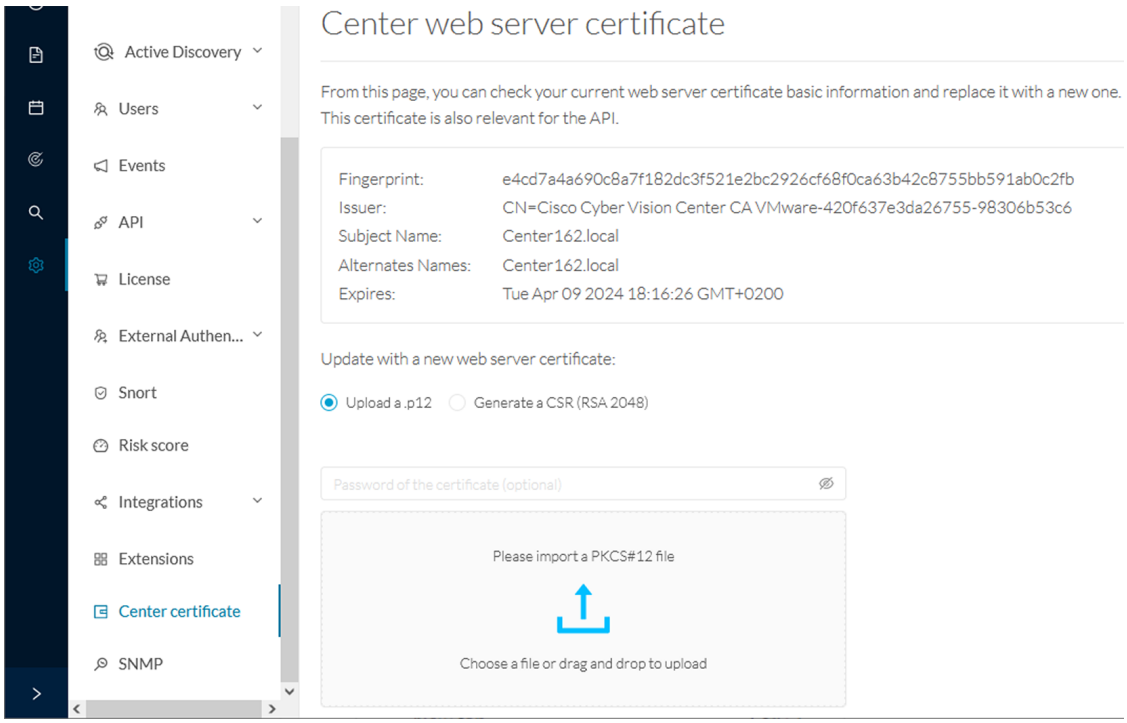
This section explains how to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

Before you begin

Perform this task if you're planning to use an enterprise certificate. You must install Cisco Cyber Vision beforehand.

Procedure

Step 1 To use an enterprise certificate, navigate to Admin > Center certificate.



Step 2 You can upload a .p12 or generate a CSR.

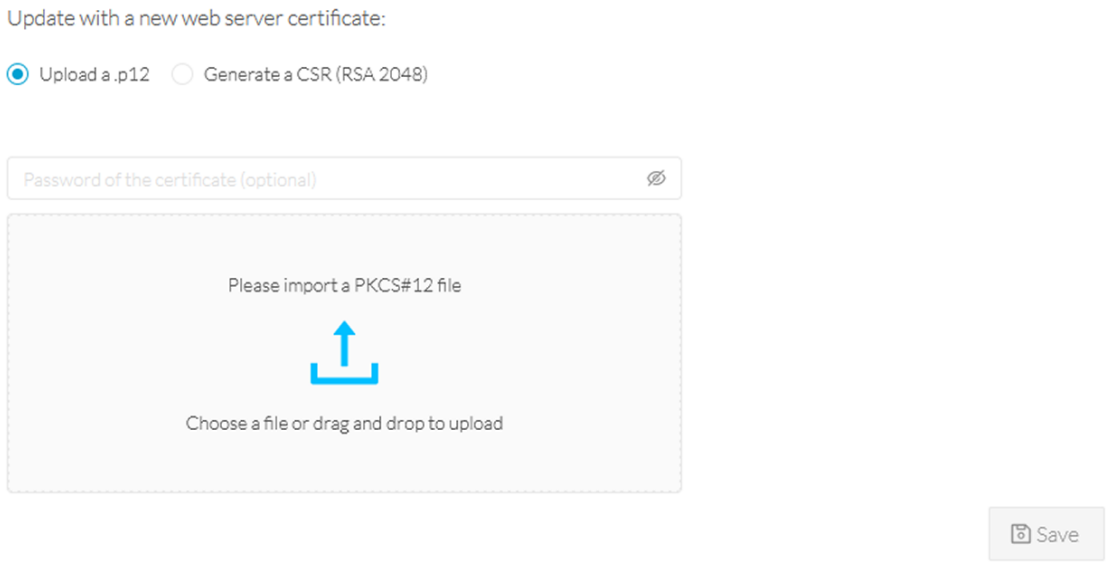
Upload a p12

Before you begin

The p12 (or Microsoft pfx) file must contain a private key, a password, and the field "X509v3 Subject Alternative Name" must contain the Center DNS name.

Procedure

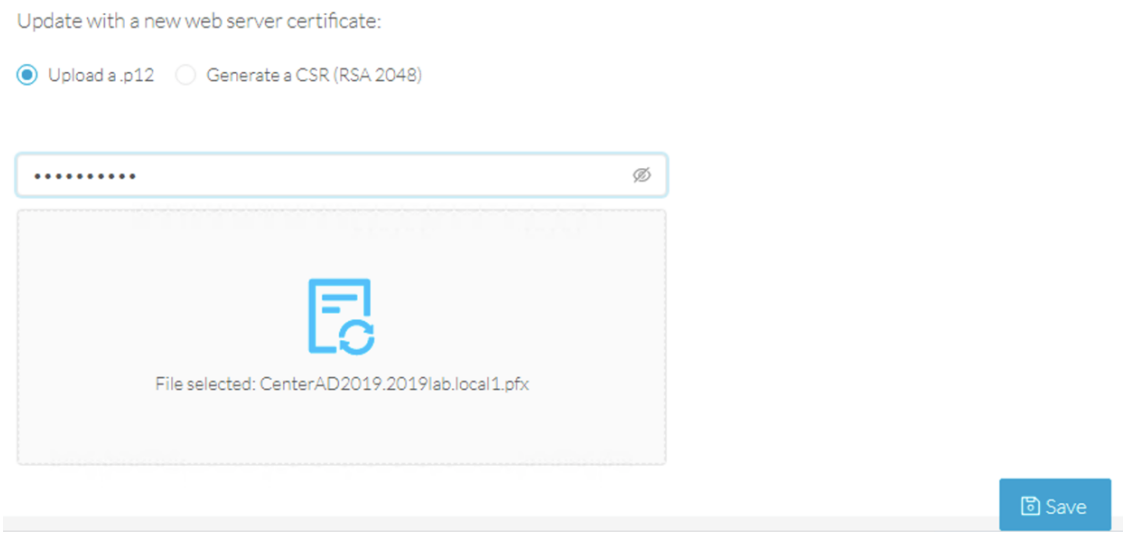
Step 1 Select Upload a .p12.



Click Please import a PKCS12 file and choose you pfx or p12 file generated from your certification server.

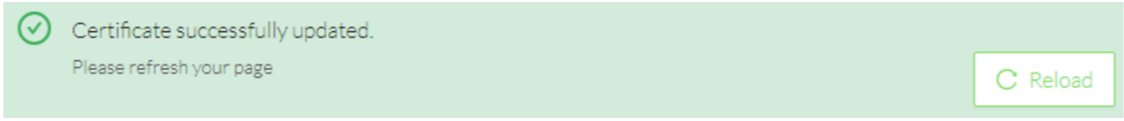
Step 2 Type the certificate password.

Step 3 Click the Import a PKCS#12 file button or drag and drop the file to import it.



Step 4 Click Save.

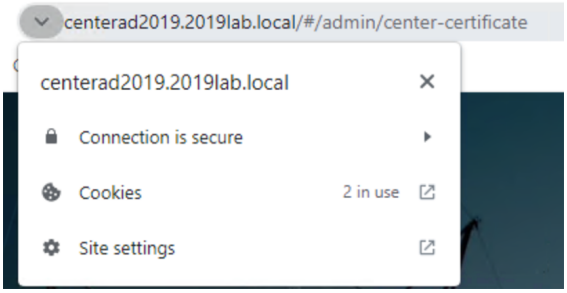
The following message appears:



Step 5 Click Reload.

Step 6 In your browser, use the DNS name to connect to your Cisco Cyber Vision instance.

The error message does not appear and the connection is secure.



What to do next

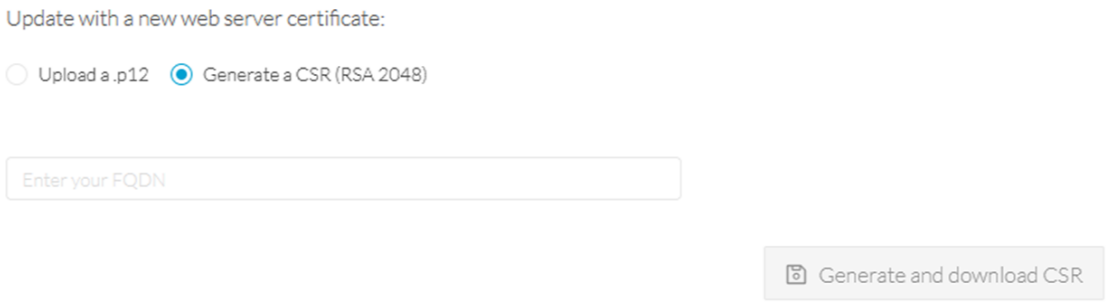
If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 34.

If you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Sensor Installation Guides.

Generate a CSR

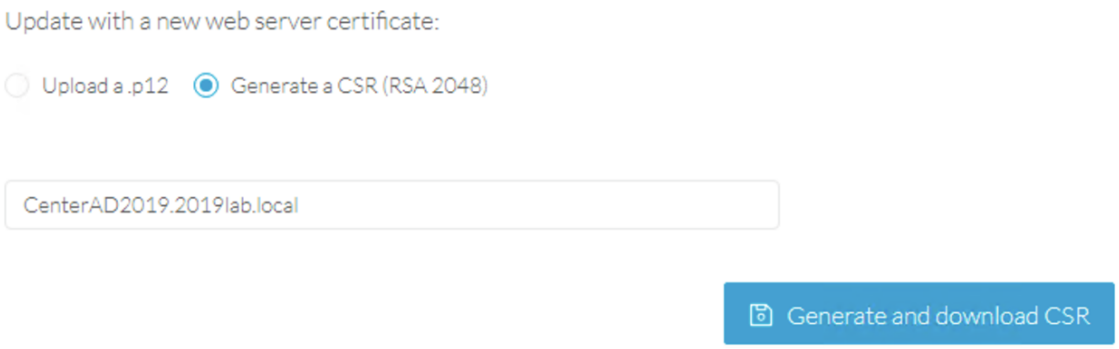
Procedure

Step 1 Select Generate a CSR.



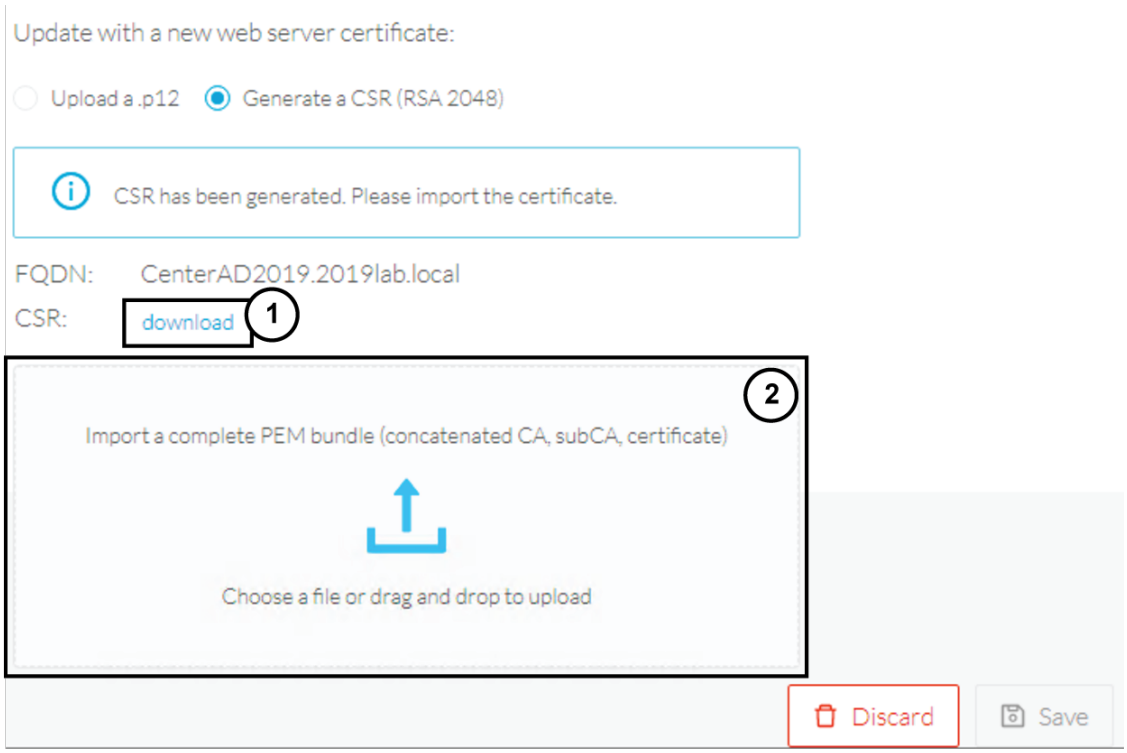
Step 2 Enter the Center FQDN as registered on your DNS server.

Step 3 Click the Generate and download CSR button.



A message indicating that the CSR has been generated is displayed.

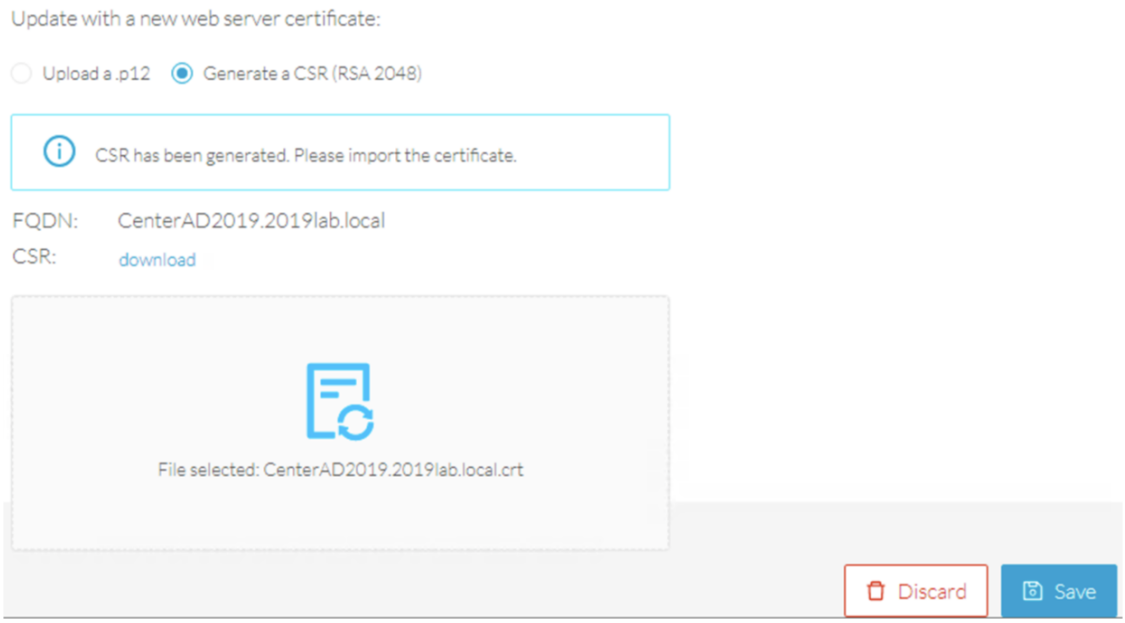
Step 4 Click the download button **(1)**.



A <FQDN>.csr file is downloaded.

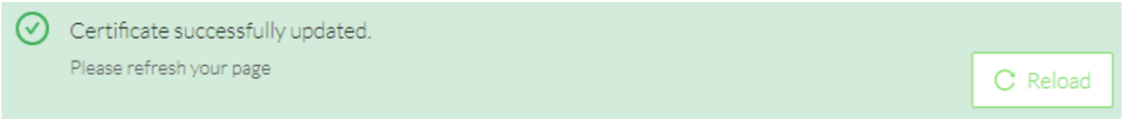
Step 5 Use the <FQDN>.csr file to generate a pem certificate from your enterprise Certification Authority.

Step 6 Once the pem certificate is generated, return to Cisco Cyber Vision and click the Import a complete PEM bundle button **(2)** or drag and drop it to import it.



Step 7 Click Save.

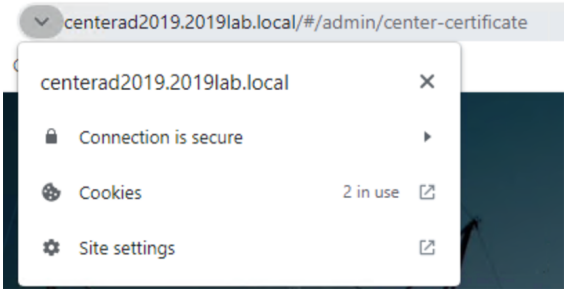
The following message appears:



Step 8 Click Reload.

Step 9 In your browser, use the DNS name to connect to your Cisco Cyber Vision instance.

The error message does not appear and the connection is secure.



What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 34.

If you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Sensor Installation Guides.

Configure Center data synchronization

This step is applicable to the Global Center and its synchronized Centers.

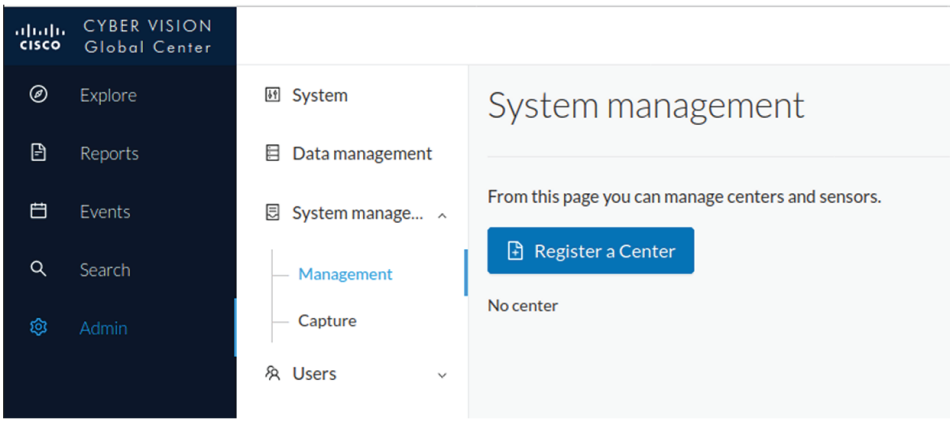
Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists of registering the Center in the Global Center and enrolling the Center to the Global Center. To do so, you need to open each's 's GUI.

Note To differentiate each user interface, check the top left corner of 's "Global Center" or "Center".

Procedure

Step 1 In the Global Center's GUI, navigate to Admin > System Management > Management.

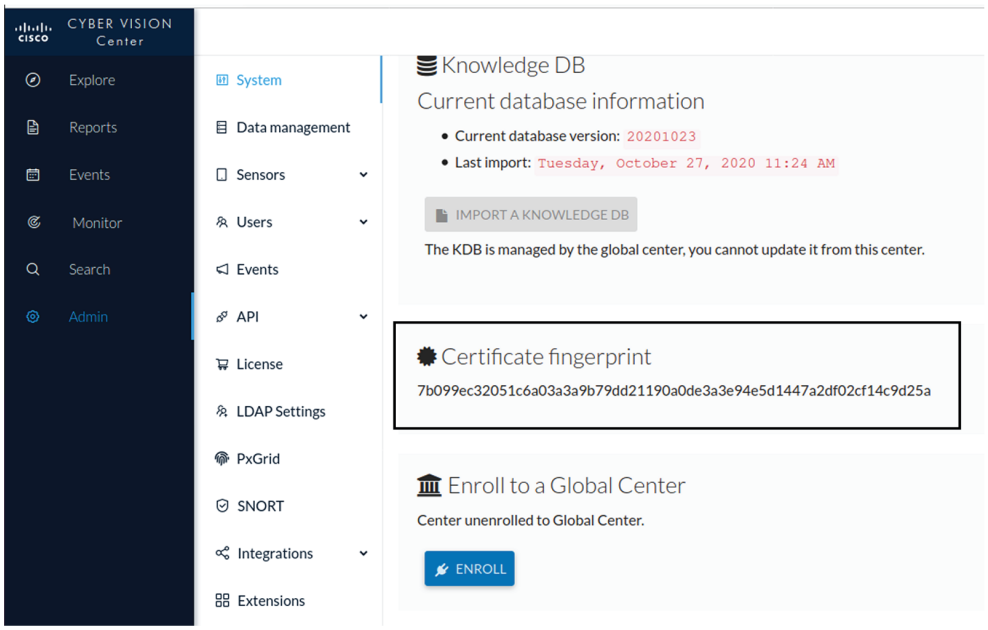
Step 2 Click the **Register a Center** button.



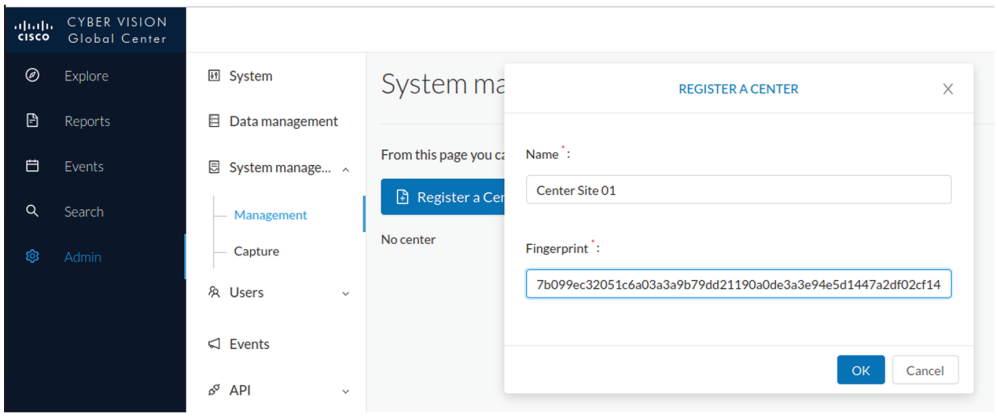
The window "Register a Center" pops up, ready to be filled. Now you must access the Center's GUI to retrieve its fingerprint.

Step 3 In the Center's GUI, navigate to Admin > System.

Step 4 Scroll down to Certificate fingerprint and copy it.

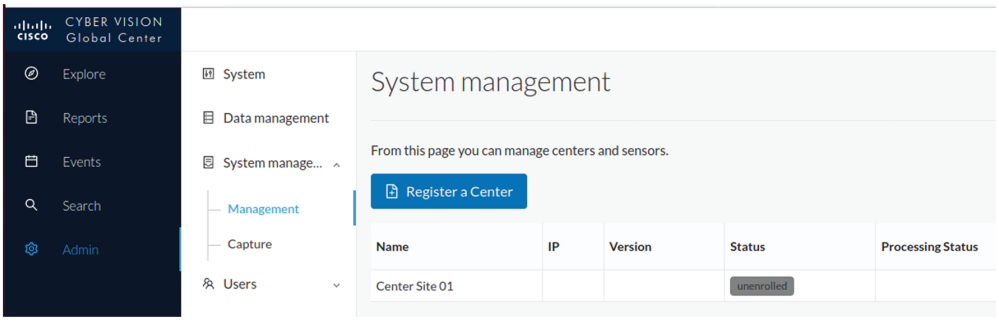


Step 5 In the Global Center's GUI, give a name to the Center, and paste the Center's fingerprint into the corresponding field



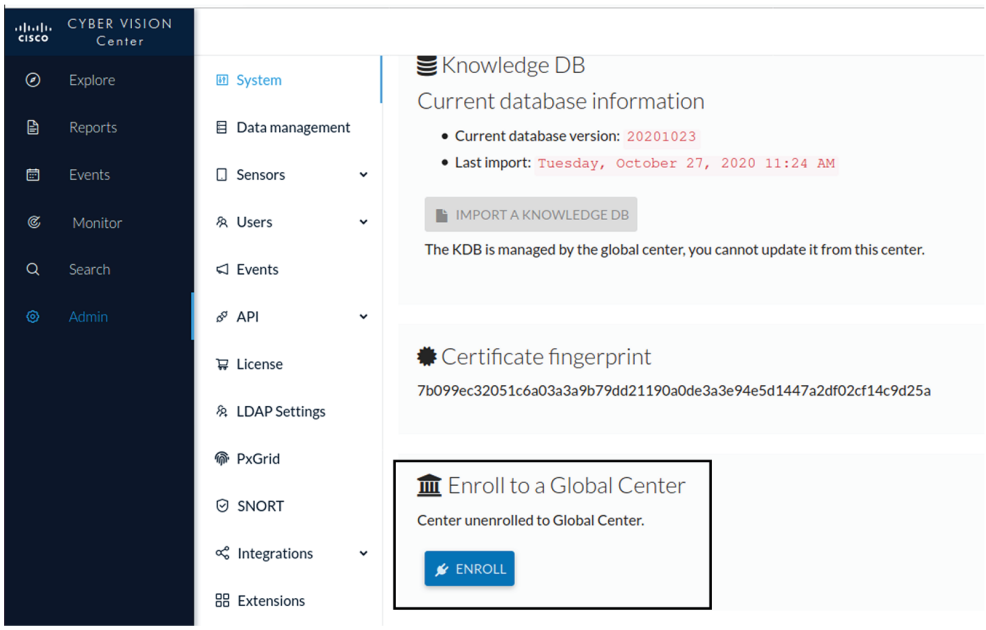
Step 6 Click **OK**.

The Center appears in the list as unenrolled.



At this point you must switch to the Center's GUI and enroll it to the Global Center.

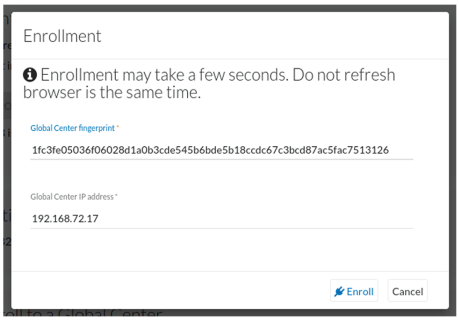
Step 7 In the Center's GUI, scroll down to Enroll a Global Center and click the **Enroll** button.



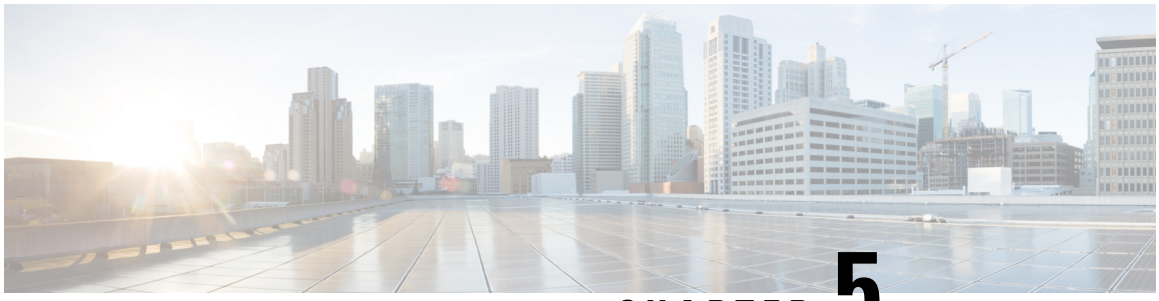
The Enrollment window pops up.

Step 8 Copy the Global Center's fingerprint from its GUI's System administration page (same location as the Center's).

Step 9 Enter the Global Center's IP address and click **Enroll**.



Once the synchronization is complete, it is indicated that the Center is enrolled to the Global Center.



CHAPTER 5

Configure a Center DPI

Configure a Center DPI

This section describes how to configure a Center DPI, that is, a virtual sensor in the Center.

Requirements:

Make sure an ethernet interface is available for the Center DPI traffic, depending on:

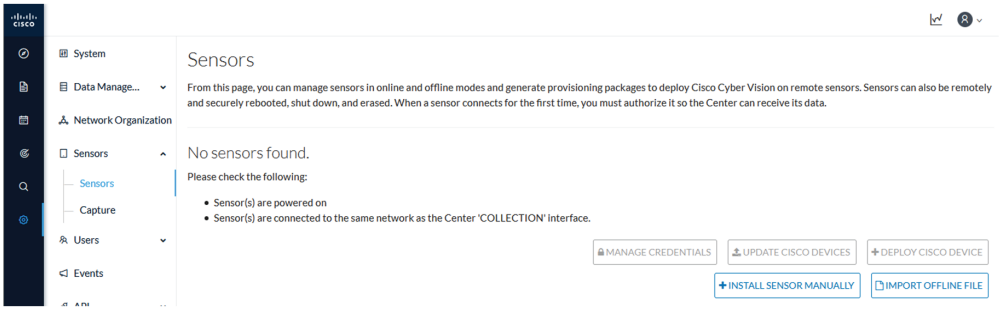
- If the server has a dual interface, that is, the Administration interface is on eth0 and the Collection interface is on eth1, then eth2 will be used for the Center DPI.
- If the server has a single interface, that is, the Administration and Collection interfaces are on the same interface, then eth1 will be used for the Center DPI.

In the example below, the server has a single interface.

To configure a Center DPI:

Procedure

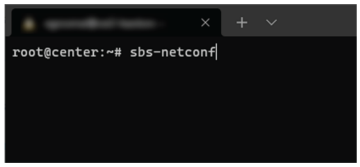
Step 1 Access the sensors administration page.



Step 2 Open the Center shell prompt and type the following command:

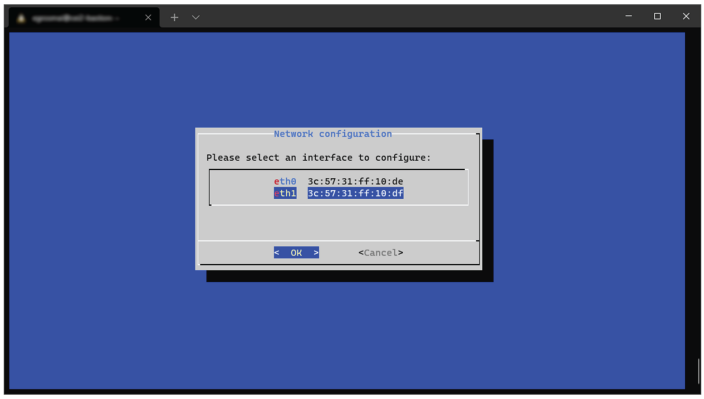
Configure a Center DPI

sbs-netconf

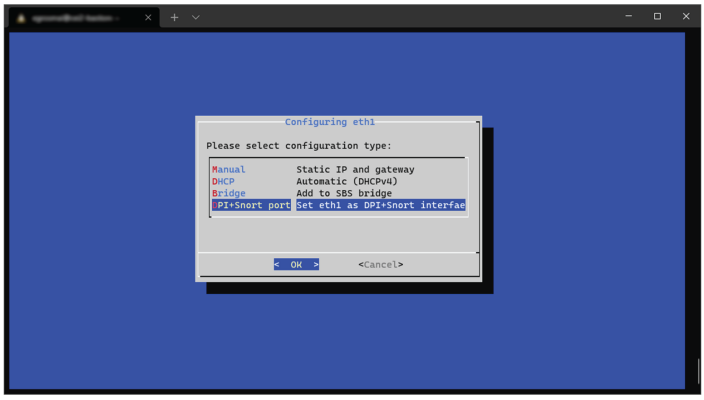


Step 3 In the case of a single interface, select the eth1 interface.

In the case if a dual interface, select eth2.

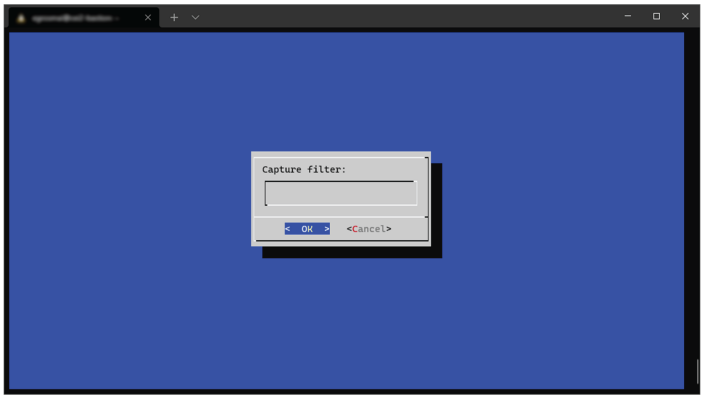


Step 4 Select the interface as DPI+Snort port.

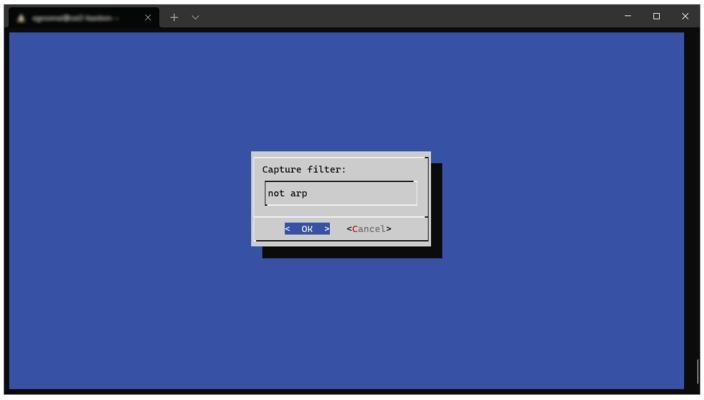


Step 5 Configure a capture filter mode. You can do that later in the sensor page clicking the Capture mode button.

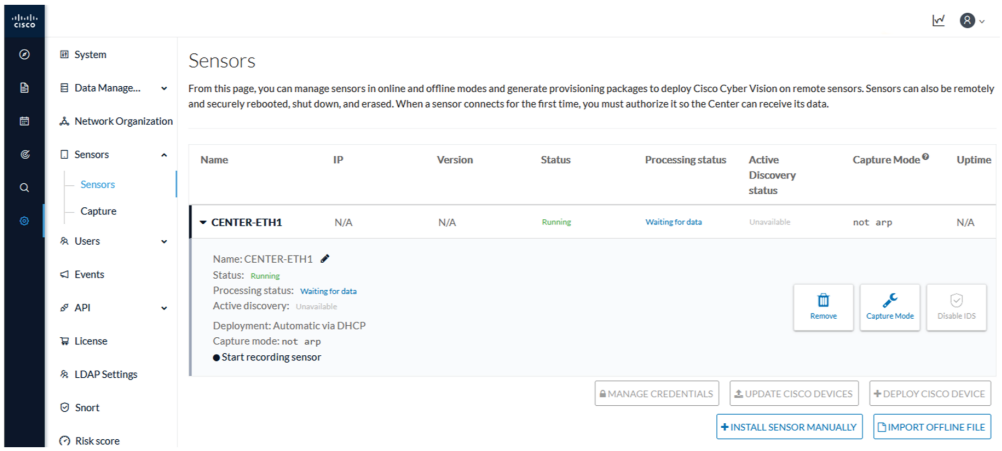
For more information on how to configure a capture mode filter, refer to the GUI user guide.



For example, you can type "not arp".



In the administration sensor page, the new virtual sensor appears and is ready to receive data.



Center DPI

Cyber Vision Center Deep Packet Inspection (DPI) is a virtual sensor that

- operates within the center environment,
- analyzes industrial network traffic at a granular level by inspecting application flows locally, and
- adds metadata to the Cyber Vision Center for centralized storage, analytics, and visualization.

Configure Center DPI

Enable Center DPI to function as a virtual sensor in Center for monitoring and analyzing network traffic.

Before you begin

Ensure you have an available Ethernet interface for Center DPI traffic:

- SPAN:
  - Single interface: eth1
  - Dual interfaces: eth2
- ERSPAN:
  - Single interface: eth0
  - Dual interfaces: eth0 and eth1
  - For optimal performance, use a dedicated interface if possible.

Procedure

Step 1 Open the Center shell prompt and run the `sbs-netconf` command.

Step 2 Select the interface to configure, based on your SPAN or ERSPAN setup.

Step 3 Select the configuration type as **DPI+Snort port**.

Step 4 Select an encapsulation type.

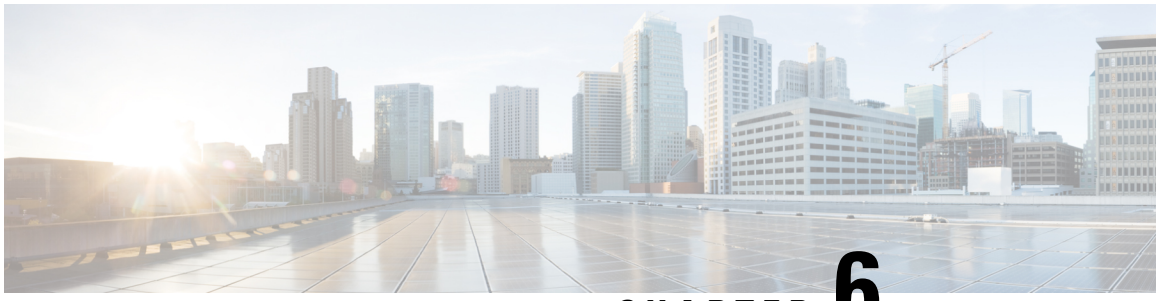
- **None** for SPAN configurations.
- **erspan2** for ERSPAN type 2 remote SPAN.
- **erspan3** for ERSPAN type 3 remote SPAN.

Step 5 If you select **erspan2** or **erspan3** as the encapsulation type, enter an IPv4 address to receive traffic.

A new sensor is created and appears in **Admin** > **Sensors** > **Sensor Explorer**, ready to monitor network traffic based on the chosen configuration.

What to do next

- To view traffic statistics from the new sensor, navigate in the Center interface to **Explorer** > **All Data** > **Device list** and select the device for more details.
- To disable Snort on the Center DPI interface, follow these steps.
  1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
  2. Select the sensor and click **Disable IDS**.



CHAPTER 6

Configure Center synchronization with Global Center

Synchronizing Global Centers

Use this process to synchronize a Center with a Global Center so that data from multiple Centers can be viewed in a single application.

Summary

This process includes registering the Center, enrolling it with the Global Center, completing the initial synchronization, and monitoring synchronization status.

Workflow

These stages describe the synchronization process.

1. Register the Center in the Global Center.
2. Enroll the Center with the Global Center.
3. Allow the initial synchronization to complete.
4. Monitor the synchronization status in the Global Center.
5. Unenroll the Center when synchronization is no longer required.

Result

After enrollment succeeds, the Global Center displays synchronized data and status information for the enrolled Center.

Synchronize a Center with a Global Center

Use this procedure to establish synchronization between a Global Center and a Center.

This procedure applies to a Global Center and the Centers that synchronize with it.

To complete this procedure, open the user interface of both the Global Center and the Center.

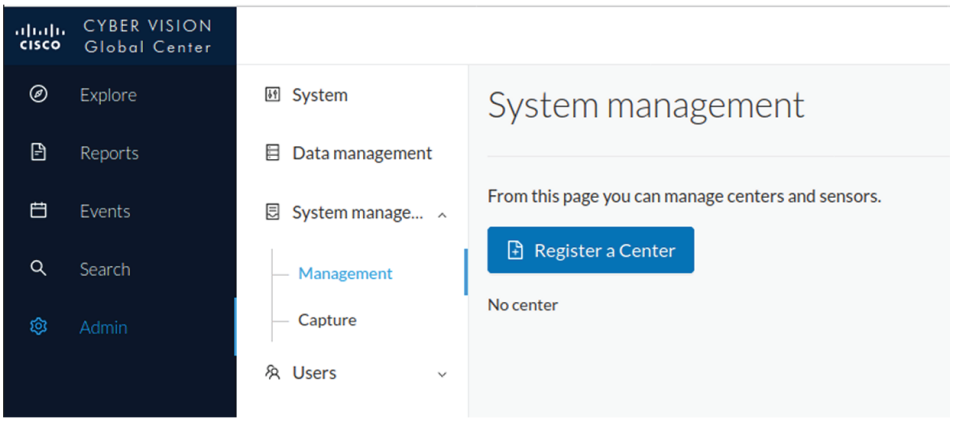
Before you begin

- Ensure that the Global Center is installed and accessible.
- Ensure that the Center is installed and accessible.
- Ensure that the required network connectivity between the Center and the Global Center is in place.
- Ensure that certificate fingerprints can be retrieved from both systems.

Procedure

Step 1 In the Global Center, navigate to **Admin > System Management > Management**.

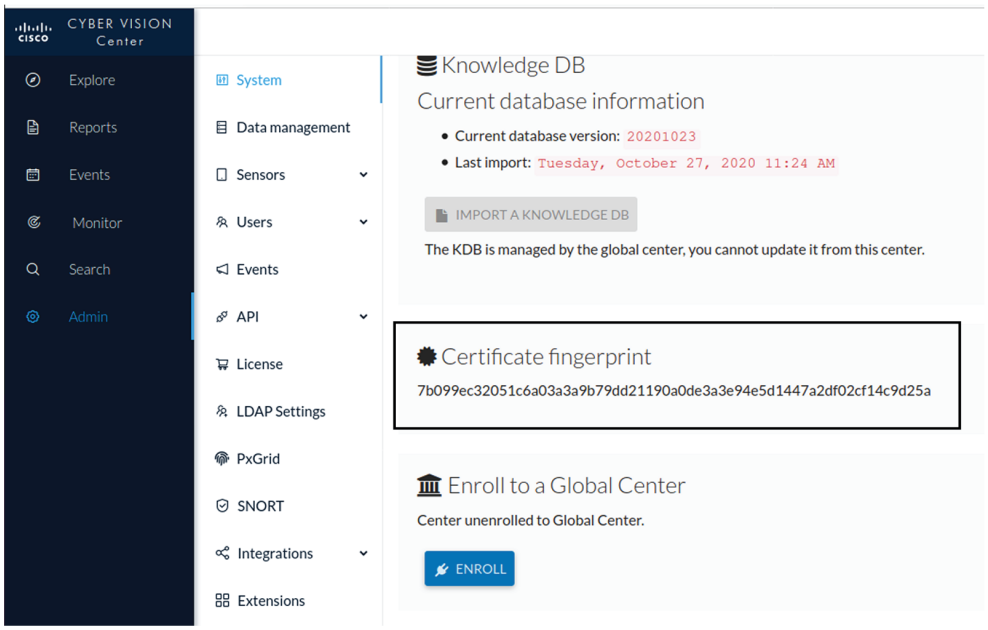
Step 2 Click the **Register a Center** button.



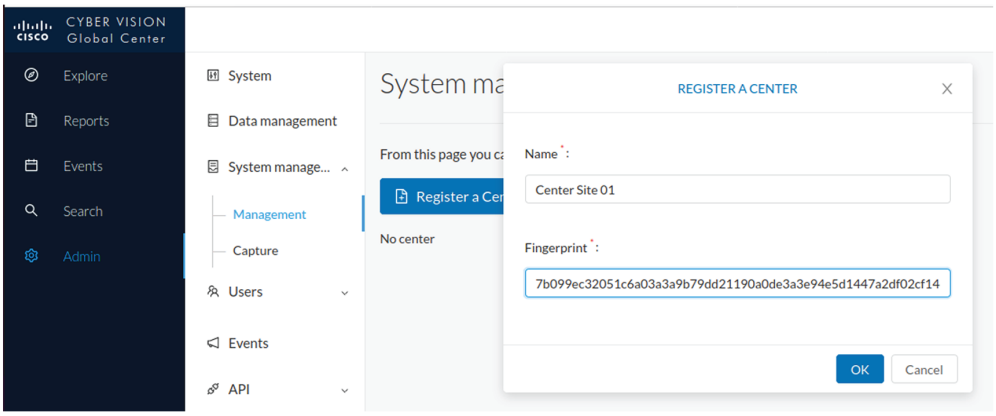
The Register a Center window opens. Leave it open while you retrieve the Center fingerprint.

Step 3 In the Center, navigate to **Admin > System**.

Step 4 Scroll down to Certificate fingerprint and copy it.

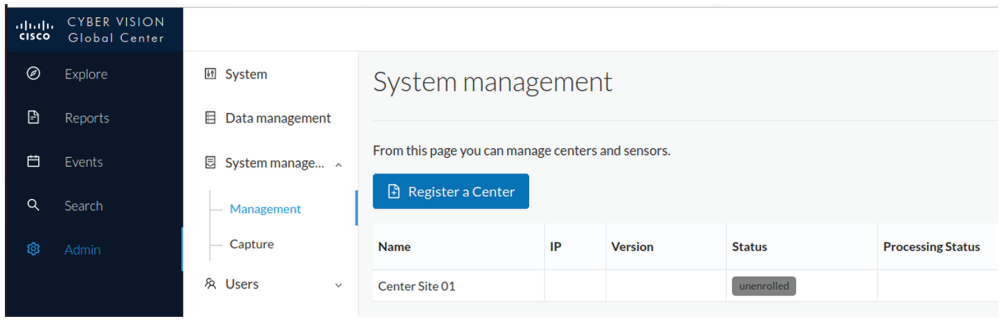


Step 5 In the Global Center, enter a name for the Center and paste the Center fingerprint into the corresponding field.



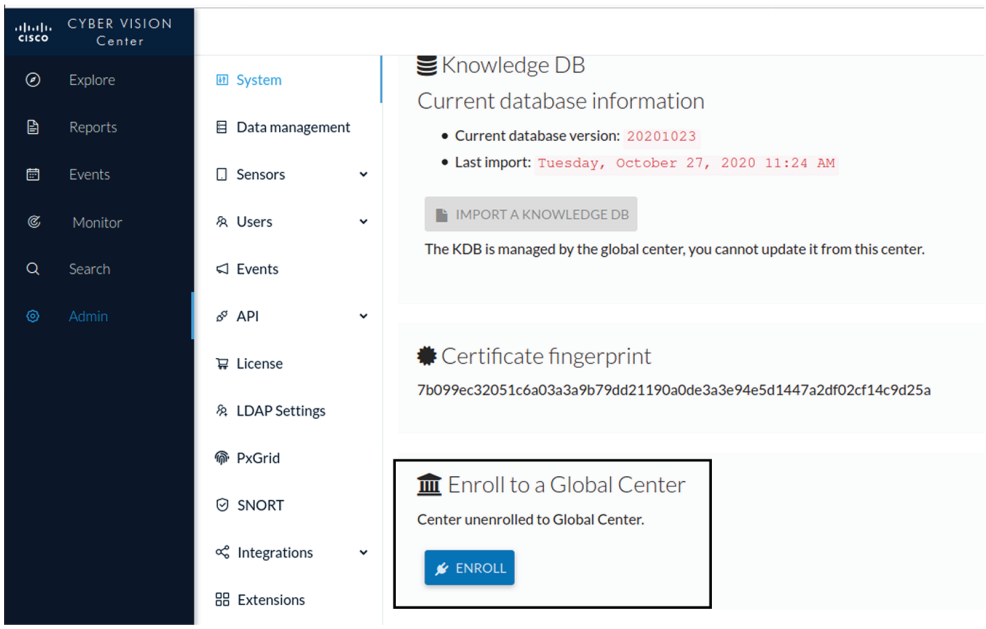
Step 6 Click **OK**.

The Center appears in the list as unenrolled.



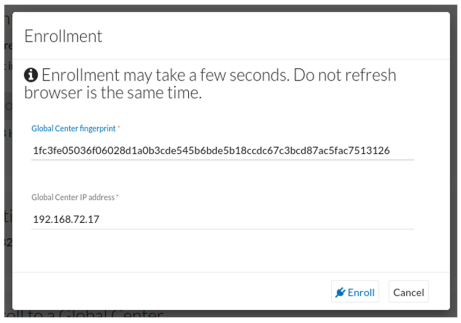
Switch to the Center and enroll it with the Global Center.

Step 7 In the Center, scroll down to **Enroll a Global Center** and click the **Enroll** button.



Step 8 In the Global Center, copy the Global Center fingerprint from the System administration page.

Step 9 Enter the Global Center fingerprint and IP address, and click **Enroll**.



The Center is shown as enrolled with the Global Center after synchronization is complete.

The Center is enrolled with the Global Center, synchronization begins, and the Center status changes to connected in the Global Center.

What to do next

If additional Centers must be synchronized, repeat this procedure for each one.

Unenroll the Center

Use this procedure to remove a synchronized Center from a Global Center.

Use this procedure when a Center must be removed from synchronization, for example during maintenance or replacement of the Center or the Global Center.

Before you begin

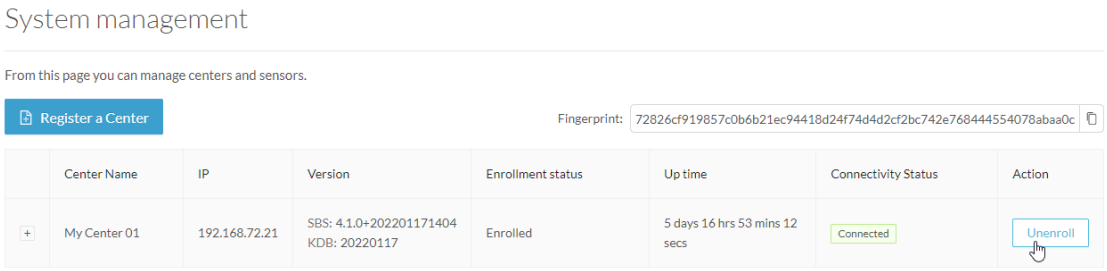
You can unenroll a Center when you need to replace, move, or remove it from a Global Center. Unenrollment deletes the Center data from the Global Center.

Procedure

Step 1 In Cisco Cyber Vision, navigate to **Admin** > **System Management** > **Management**.

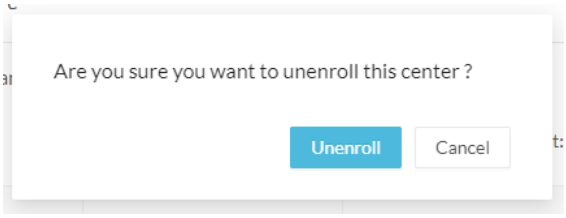
All Centers associated with the Global Center are listed.

Step 2 Click **Unenroll** for the required Center.



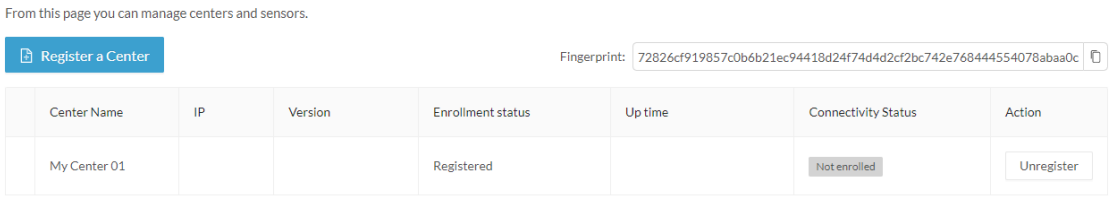
If you are replacing a Global Center, unenroll all its synchronized Centers.

Step 3 In the confirmation dialog box, click **Unenroll** to start the process.



All Center data is deleted from the Global Center. The Center is ready to be enrolled again in the same Global Center or in another Global Center.

Step 4 If the Center is later enrolled in another Global Center, it remains listed in its former Global Center as **Not enrolled**. You can use the **Unregister** button to remove it from the list.



The Center is unenrolled from the Global Center and can be enrolled again in the same Global Center or in another Global Center later.

What to do next

If you are replacing a Global Center, repeat this procedure for each synchronized Center before decommissioning the original Global Center.

Force unenrollment of a Center

When a synchronized Center has been disconnected for a long time, for example because of a hardware failure, you can force its unenrollment from the Global Center. This deletes all data for that Center from the Global Center and allows the Center to be replaced.

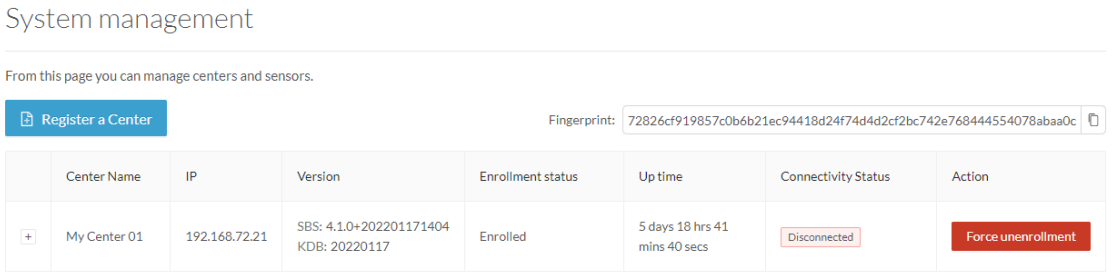
Important Make sure that the disconnected Center is permanently unavailable before performing this action. Because all data for the Center is deleted from the Global Center, a Center that later attempts to send data again can cause significant data synchronization issues.

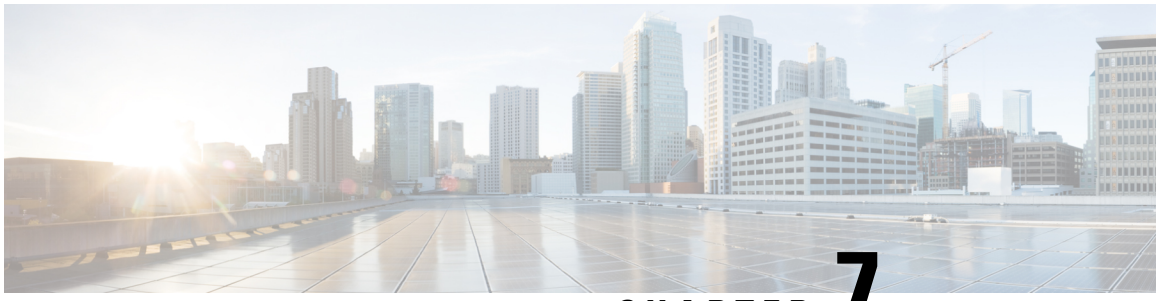
1. In Cisco Cyber Vision, navigate to **Admin > System Management > Management**.

   All Centers associated with the Global Center are listed.

2. For the disconnected Center, click **Force unenrollment** in the **Action** column.

All data for that Center is deleted from the Global Center, and the Center is removed from the list.





CHAPTER 7

Upgrade procedures

Architecture with a Global Center

Check the Global Center and Centers' health

It is highly recommended that you check the health of the Centers connected to the Global Center and of the Global Center itself before proceeding to the update. To do so:

Procedure

Step 1 Connect to the Center in SSH.

Step 2 Type the following command:

```
systemctl --failed
```

The number of listed sbs-* units should be 0, otherwise the failure must be fixed before proceeding with the update.

```
root@Center21:~# systemctl --failed
0 loaded units listed.
root@Center21:~#
```

If one or several sbs services are in failed state like below, it has to be fixed before proceeding to the update.

```
root@Center21:~# systemctl --failed
  UNIT                 LOAD   ACTIVE SUB    DESCRIPTION
● sbs-marmotd.service loaded failed failed marmotd persistence service

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

1 loaded units listed.
root@Center21:~#
```

Usually, a reboot of the Center is enough to solve the issue. If not, contact the product support.

Step 3 Repeat the previous steps for the other Centers and the Global Center.

Update the Global Center

In the case of a distributed architecture, **you must first update the Global Center, then its Centers**.

You can do so through the corresponding Center's application or using its Command Line Interface.

To update the Global Center:

- Through the application:
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-combined-<VERSION>.dat
  2. Navigate to Admin > System.
  3. Click **System Update**.
  4. Browse to select the update file.
- Through the Command Line Interface (CLI):
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-center-<VERSION>.dat
  2. Launch the update using the following command:

     ```
     sbs-update install /data/tmp/CiscoCyberVision-update-center-<VERSION>.dat
     ```

To update the Centers:

Connect to each Center's application or CLI and repeat the same procedure used to update the Global Center.

Update the sensors

The update of the sensors is done from their corresponding Center (not from the Global Center). You must repeat the following procedures from each of your Centers to cover all sensors of your industrial network. Procedures differ between hardware sensors and IOx sensors.

Update hardware sensors

To update hardware sensors:

If you used the combined file to update the Center which owned the sensor, the hardware sensors (IC3000 and Sentryo Sensors) were updated at the same time.

If not, the update needs to be done from the Command Line Interface (CLI):

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-update-sensor-<VERSION>.dat

Step 2 Launch the update using the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-<VERSION>.dat
```

Update IOx sensors

To update IOx sensors:

If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable by the Center.

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-sensor-management-<VERSION>.ext

Step 2 In , navigate to Admin > Extensions.

Step 3 In the Actions column, click the **Update** button, and browse to select the update file.

If one or several sensors were not updated by the extension update:

Step 4 Navigate to Admin > Sensors > Sensor Explorer.

Step 5 Click **Manage Cisco devices**, then click **Update Cisco devices**.

A pop up with all remaining IOx sensors connected to the Center appears. Click **Update**.

If you have not installed one or several sensors with the sensor management extension, you can upgrade them with the sensor package from the platform's local manager or from the platform's Command Line Interface. This procedure is detailed in the corresponding sensor installation guide.

- Cisco IE3x00 and Cisco IR1101 file names: CiscoCyberVision-IOx-aarch64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64-<VERSION>.tar
- Catalyst 9300 and Catalyst 9400 file names: CiscoCyberVision-IOx-x86-64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<VERSION>.tar

Architecture with a single Center

Update the Center

You can update the Center through its application or using its Command Line Interface.

- Through the application:
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-combined-<VERSION>.dat
  2. Navigate to Admin > System.
  3. Click **System Update**.
  4. Browse to select the update file.

- Through the Command Line Interface (CLI):
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-center-<VERSION>.dat
  2. Launch the update using the following command:

     ```
     sbs-update install /data/tmp/CiscoCyberVision-update-center-<VERSION>.dat
     ```

Update the sensors

Sensor upgrade is done from the Center. Update procedures differ between hardware sensors and IOx sensors.

Update hardware sensors

To update hardware sensors:

If you used the combined file to update the Center which owned the sensor, the hardware sensors (IC3000 and Sentryo Sensors) were updated at the same time.

If not, the update needs to be done from the Command Line Interface (CLI):

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-update-sensor-<VERSION>.dat

Step 2 Launch the update using the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-<VERSION>.dat
```

Update IOx sensors

To update IOx sensors:

If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable by the Center.

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-sensor-management-<VERSION>.ext

Step 2 In , navigate to Admin > Extensions.

Step 3 In the Actions column, click the **Update** button, and browse to select the update file.

If one or several sensors were not updated by the extension update:

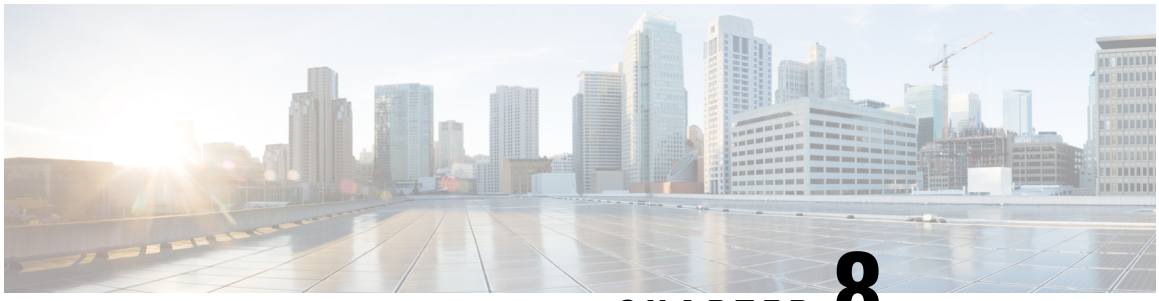
Step 4 Navigate to Admin > Sensors > Sensor Explorer.

Step 5 Click **Manage Cisco devices**, then click **Update Cisco devices**.

A pop up with all remaining IOx sensors connected to the Center appears. Click **Update**.

If you have not installed one or several sensors with the sensor management extension, you can upgrade them with the sensor package from the platform's local manager or from the platform's Command Line Interface. This procedure is detailed in the corresponding sensor installation guide.

- Cisco IE3x00 and Cisco IR1101 file names: CiscoCyberVision-IOx-aarch64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64-<VERSION>.tar
- Catalyst 9300 and Catalyst 9400 file names: CiscoCyberVision-IOx-x86-64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<VERSION>.tar



CHAPTER 8

Certificate renewal

The certificates generated by have a validity of two years.

Certificates renewal should be automatic. However, manual procedures to renew the Global Center certificate and Centers with sync exist in case automatic ones are not possible.

- Renew the certificate of a Center, on page 57

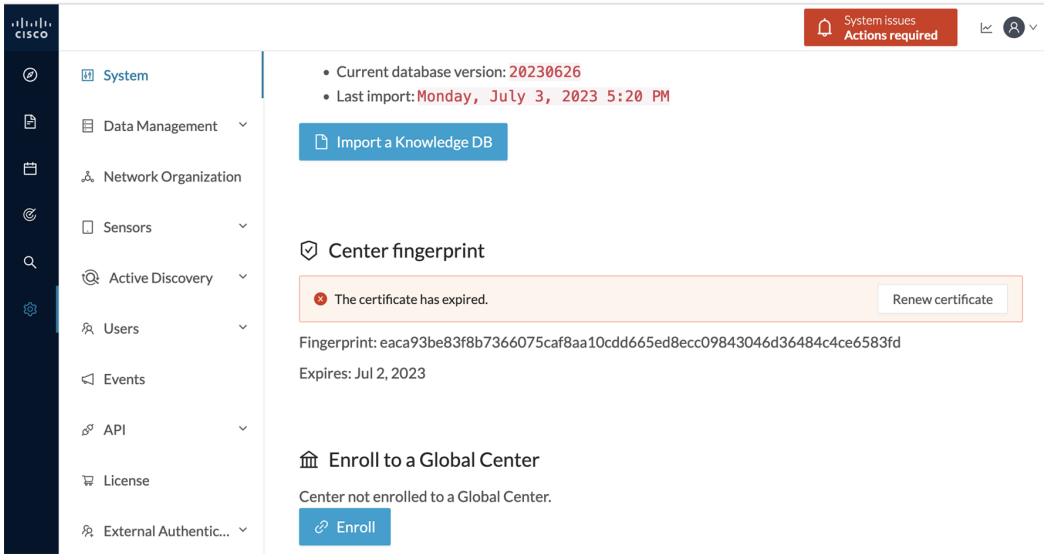
Renew the certificate of a Center

This procedure applies to Centers, Global Centers and Centers with sync. Extra steps are required to update fingerprints in the case of an architecture with a Global Center.

Procedure

Step 1 In , navigate to Admin > System.

Step 2 Slide down to Center fingerprint.



A message indicates that the certificare has expired.

Step 3 Click **Renew certificate**.

A warning page will be displayed at next login.

Step 4 Click **Advanced**, then **Accept the Risk and Continue**.

What to do next

In the case you're performing a certificate renewal within a Global Center architecture, you must follow the procedures below to update fingerprints according to the Center type.

Update the Global Center fingerprint

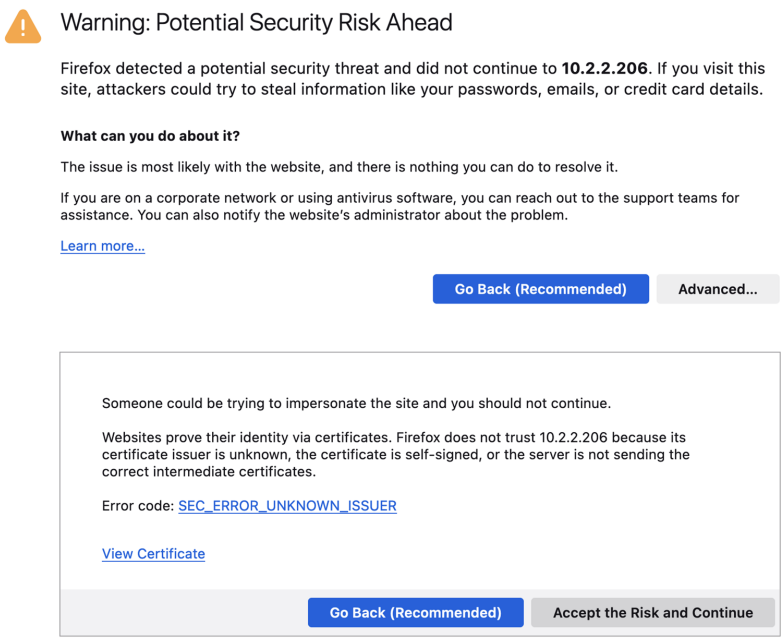
Before you begin

You need access to the Global Center and to all its Centers with sync.

Procedure

Step 1 Access the **Global Center**.

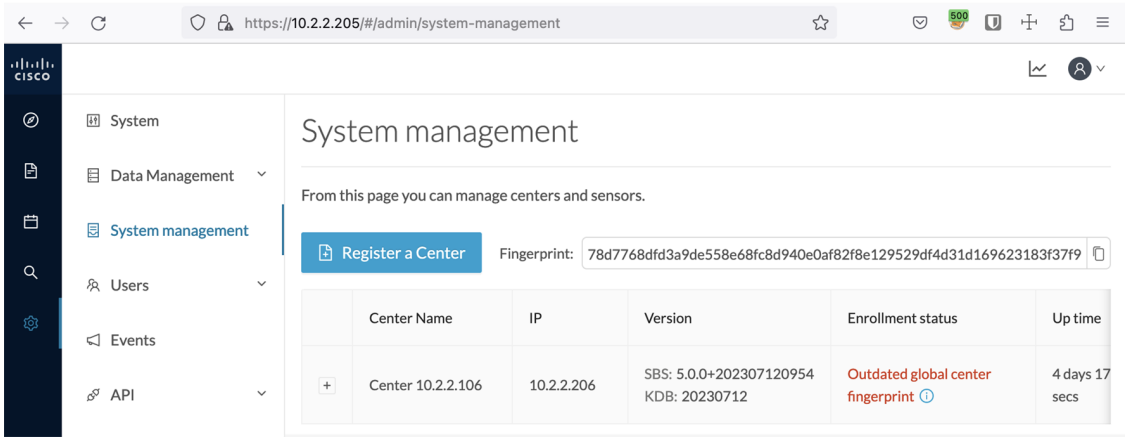
This warning page indicates that the certificate has been renewed.



Step 2 Click **Advanced**, then **Accept the Risk and Continue**.

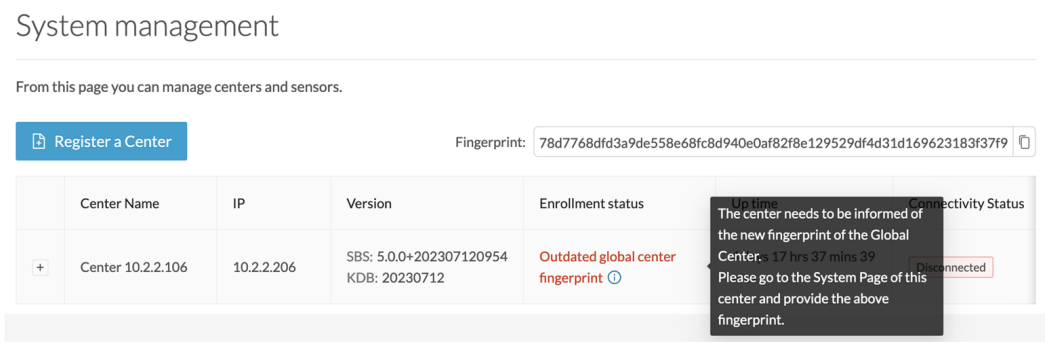
Step 3 Login to the Global Center.

Step 4 Navigate to the System management page.



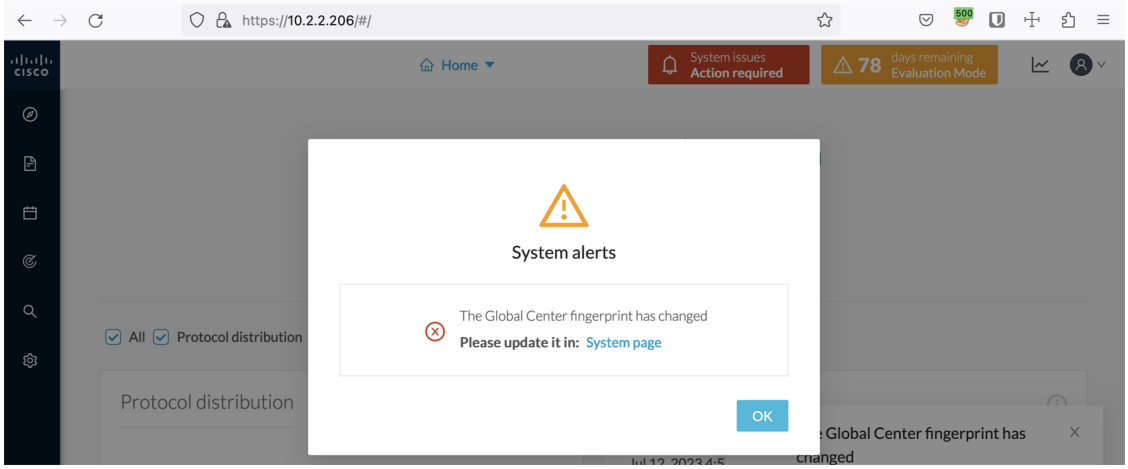
In the Center list, you can see the Center with sync which must be updated with the Global Center's fingerprint.

Step 5 Copy the Global Center fingerprint.



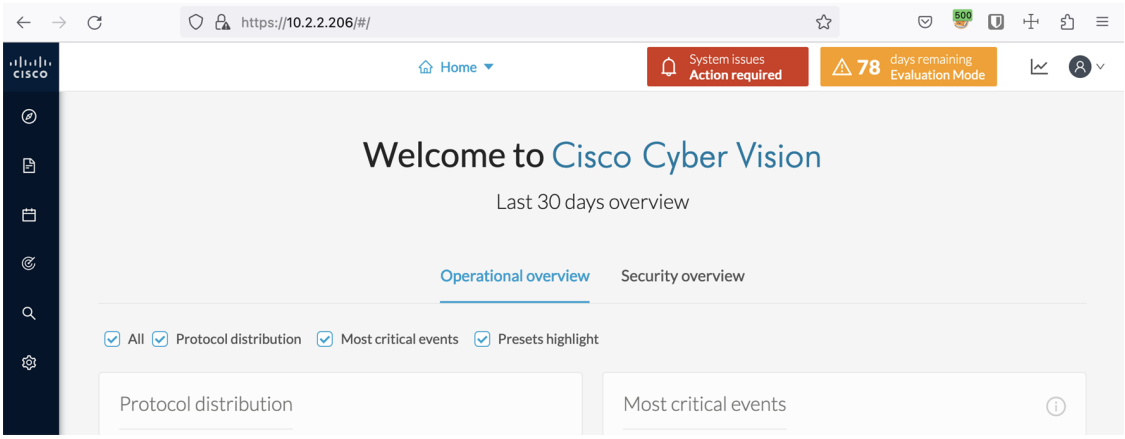
Step 6 Login to the **Center with sync**.

The following system alert pops up, indicating that the Global Center fingerprint has changed with a link to the administration system page to update it.

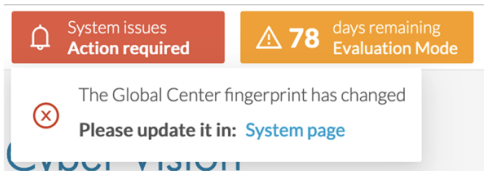


Step 7 Click **OK**.

A red banner is displayed at the top of 's user interface.



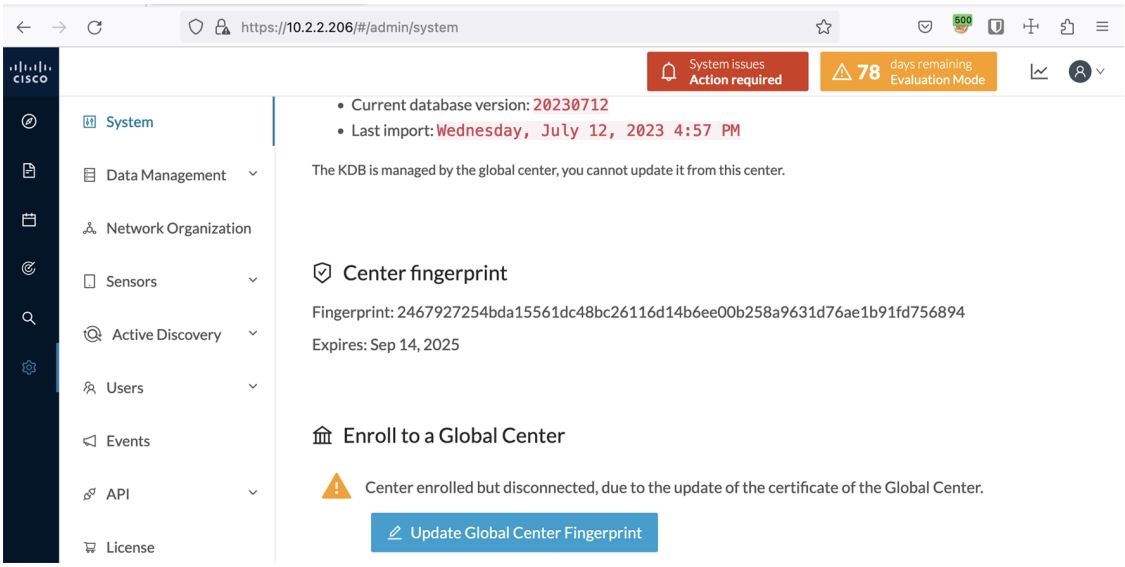
If you click the red banner, you will see the same message that appeared in the previous popup, with a link to the System page to update the Global Center fingerprint.



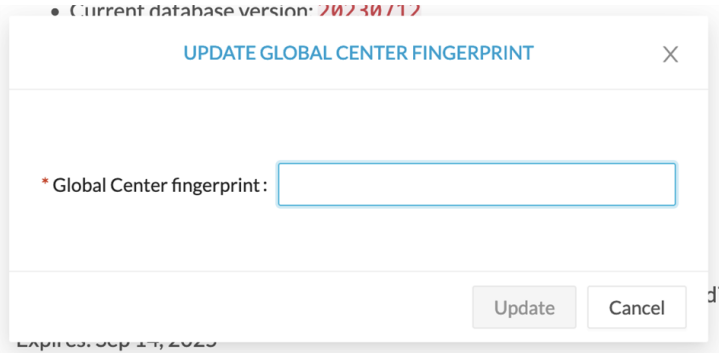
Step 8 In the System page, slide down to Enroll to a Global Center.

It is indicated that the Center is enrolled but disconnected.

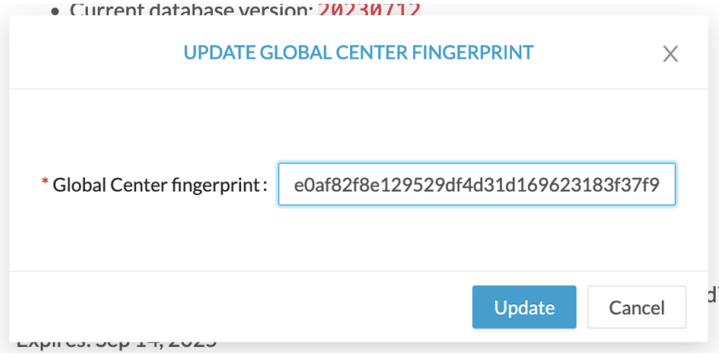
Step 9 Click **Update Global Center Fingerprint**.



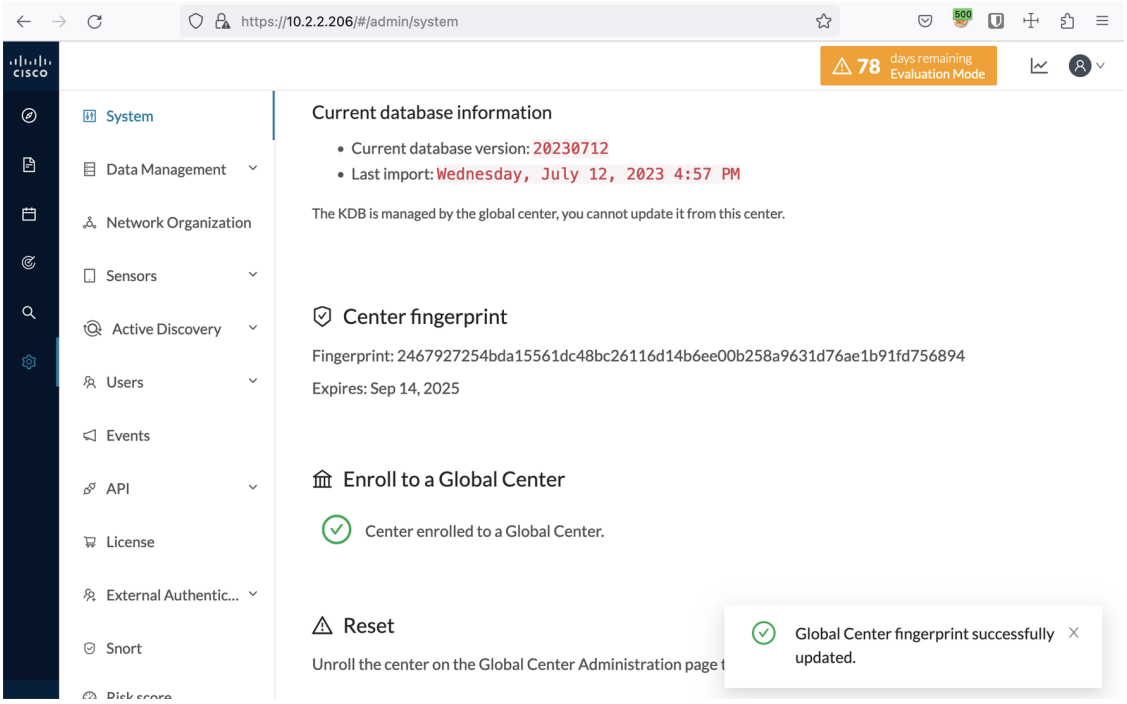
The Update Global Center fingerprint window pops up.



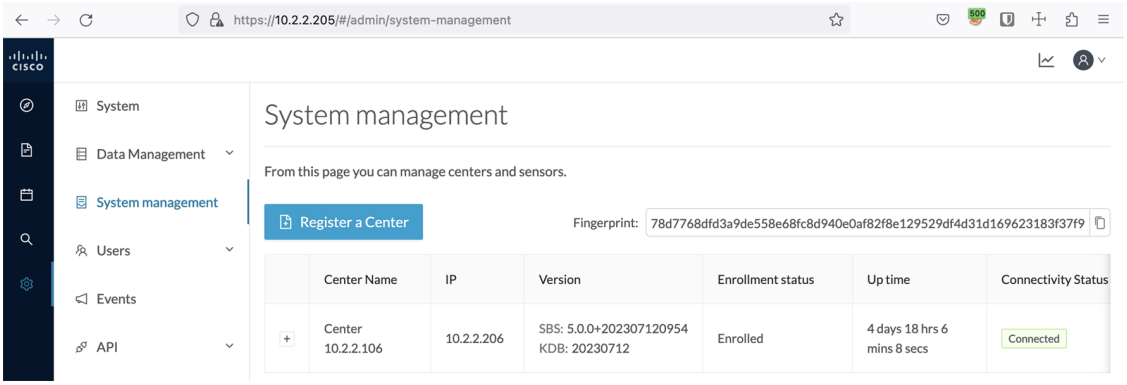
Step 10 Paste the Global Center fingerprint and click **Update**.



A message indicating that the Global Center fingerprint successfully updated appears and the Global Center enrollment status switches to enrolled.



In the Global Center System management page the Center appears as Connected.



What to do next

Repeat the previous steps for each Center with sync.

Update a Center with sync fingerprint

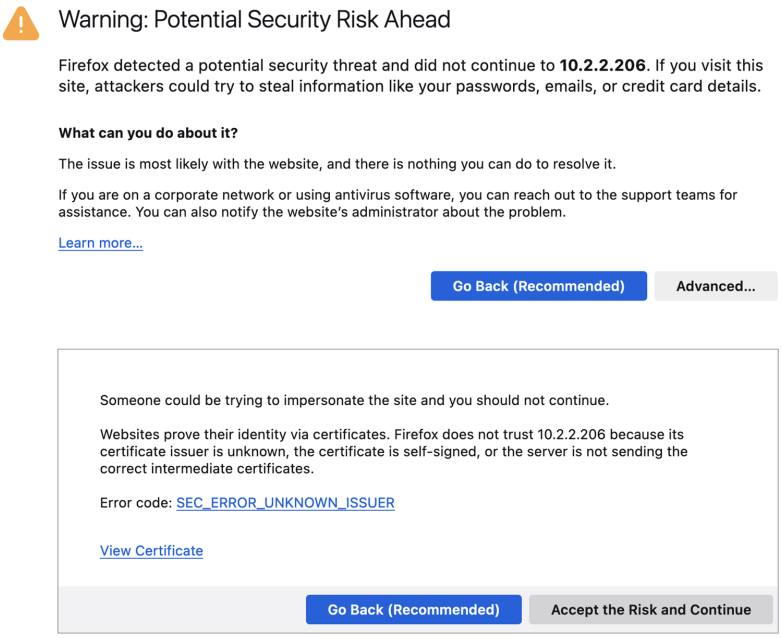
Before you begin

You need access to the Center with sync and its Global Center.

Procedure

Step 1 Access the **Center with sync**.

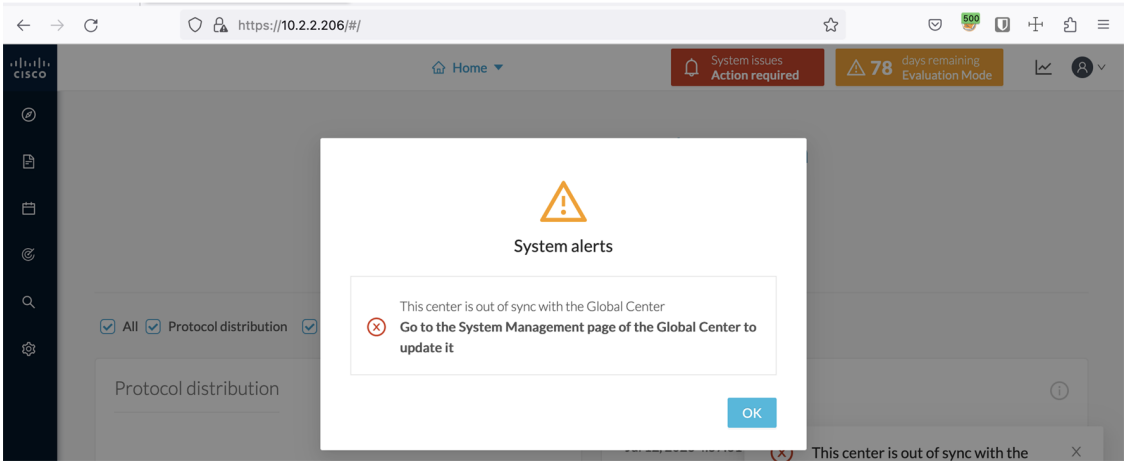
This warning page indicates that the certificate has been renewed.



Step 2 Click **Advanced**, then **Accept the Risk and Continue**.

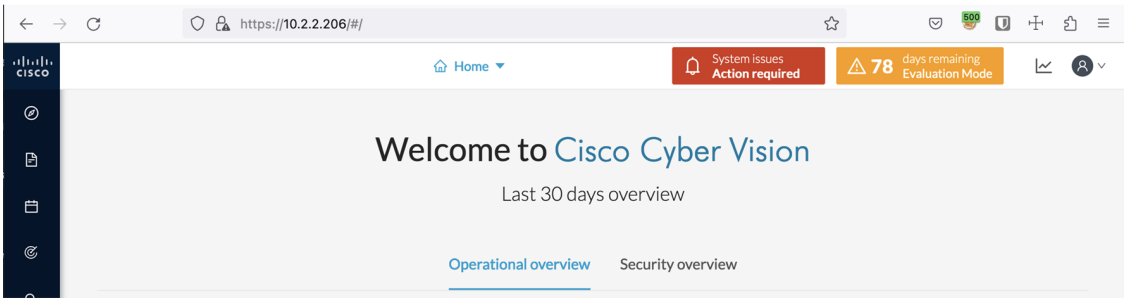
Step 3 Login to the Center.

An alert appears indicating that the Center is out of sync with the Global Center and the actions to take on the Global Center.

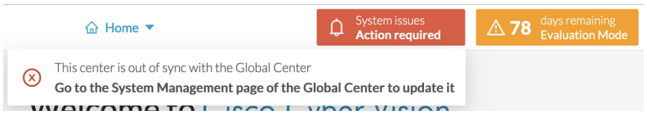


Step 4 Click **OK**.

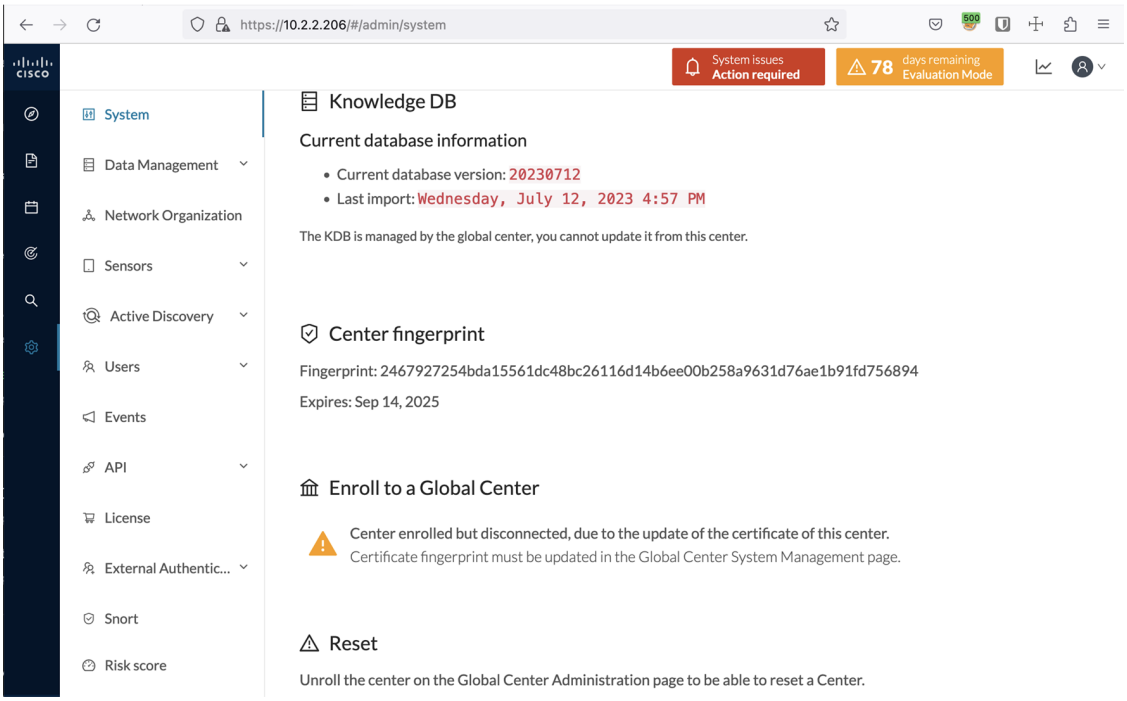
A red banner is displayed at the top of 's user interface.



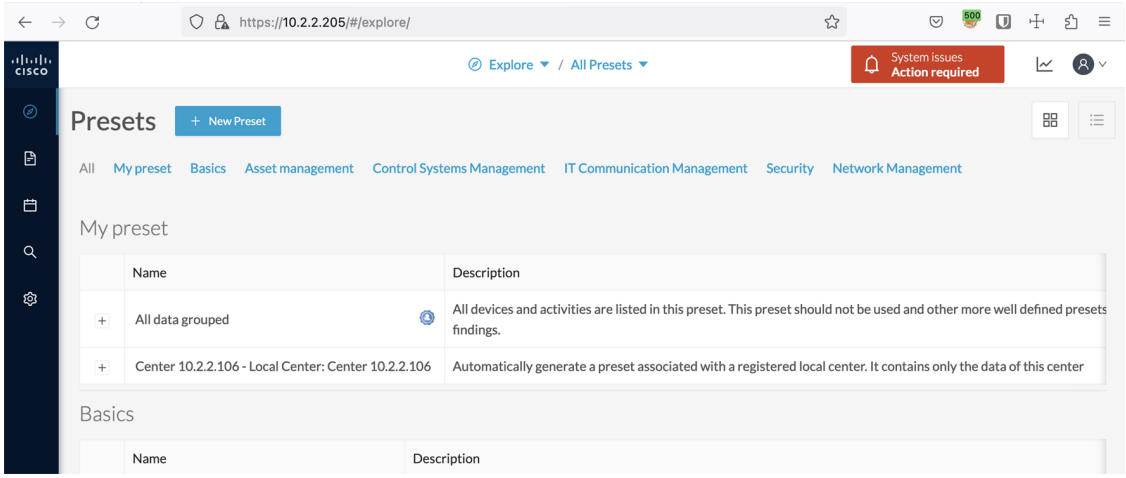
If you click the red banner, you will see the same message that appeared in the previous popup.



In the Center's administration system page, the Enroll to a Global Center state indicates that the Center is enrolled but disconnected.

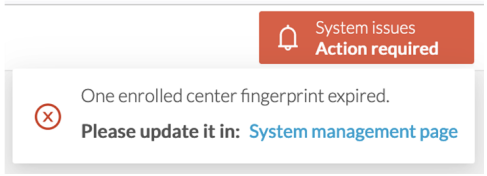


Step 5 Access the **Global Center**.

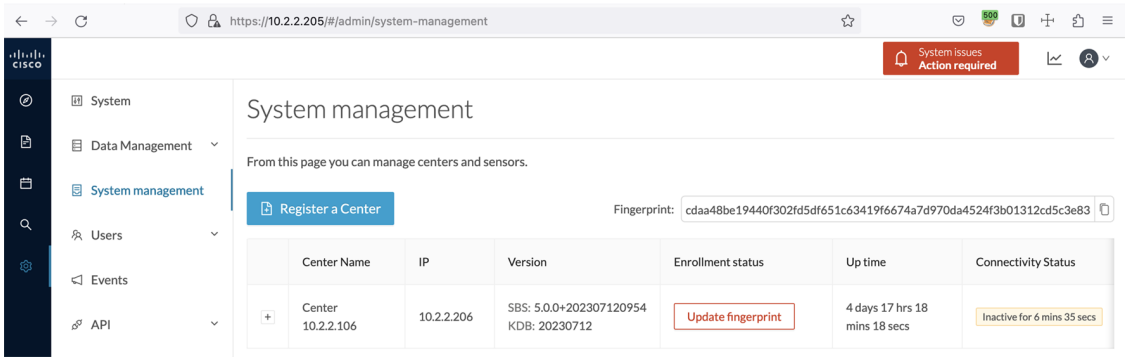


Step 6 Click the red banner.

A message indicating that a Center fingerprint is expired is displayed with a shortlink to access the administration system management page.

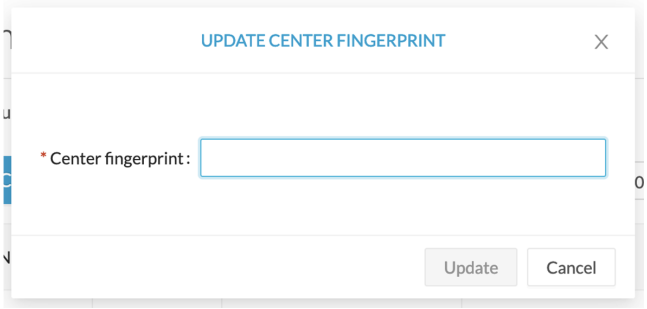


In the System management page you can see the Center with its enrollment status as Update fingerprint and Connectivity status as Inactive.

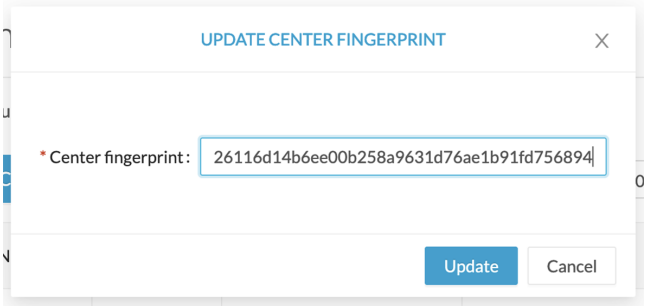


Step 7 Click the **Update fingerprint** status button.

An Update Center fingerprint window pops up.

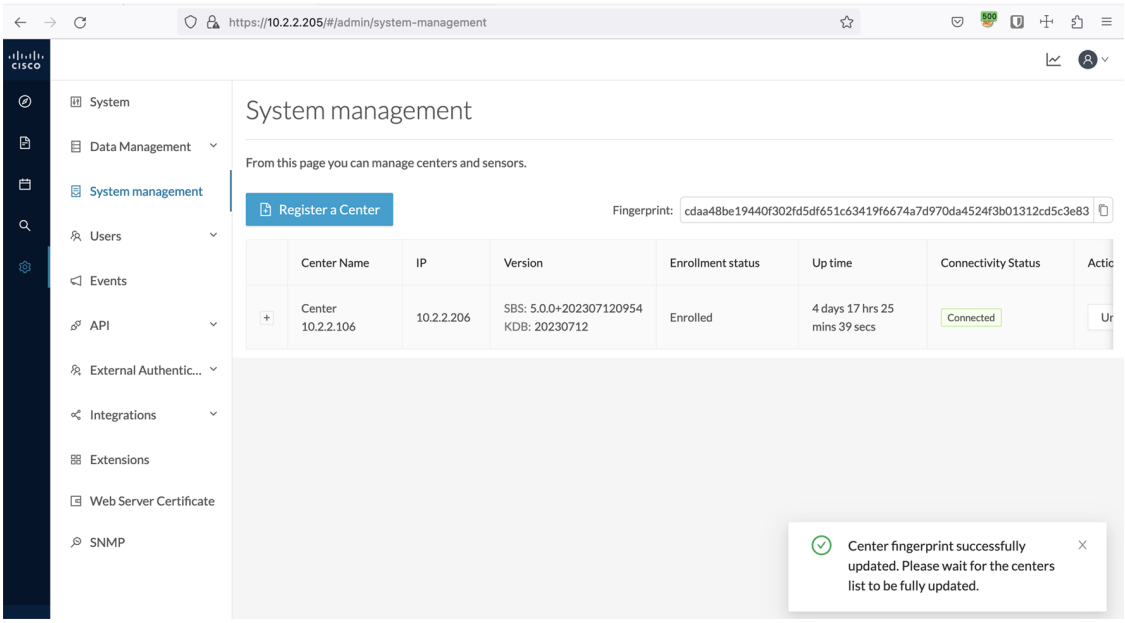


Step 8 Paste the Center fingerprint.

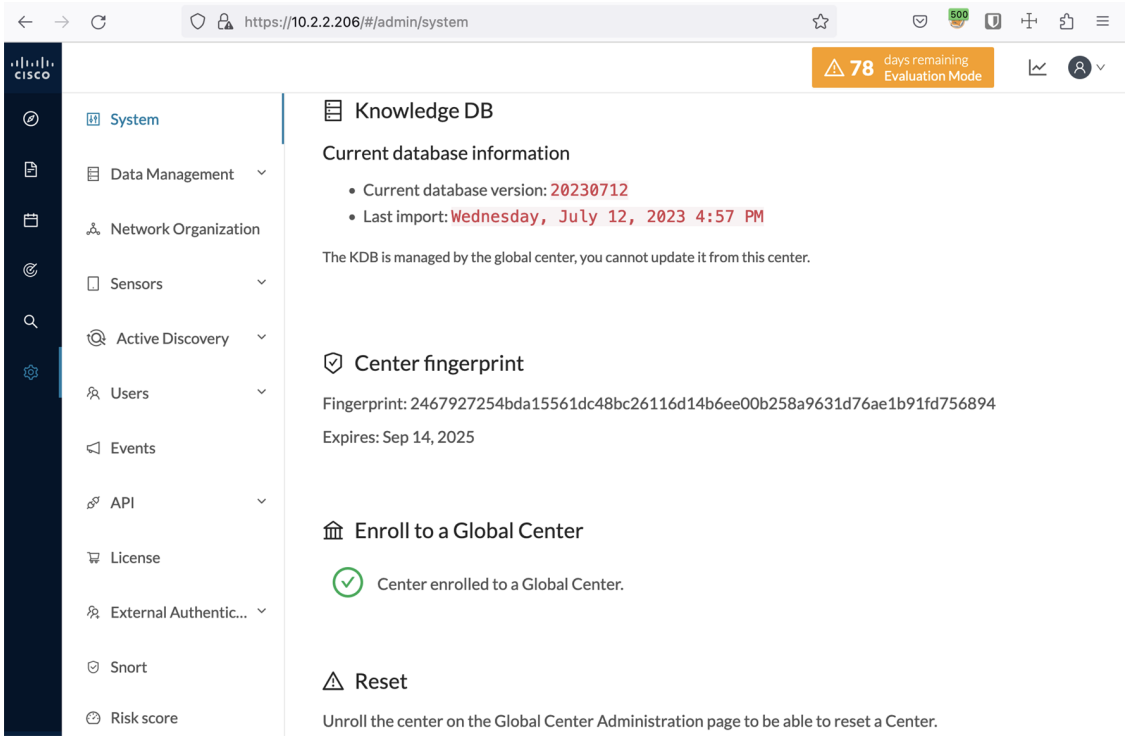


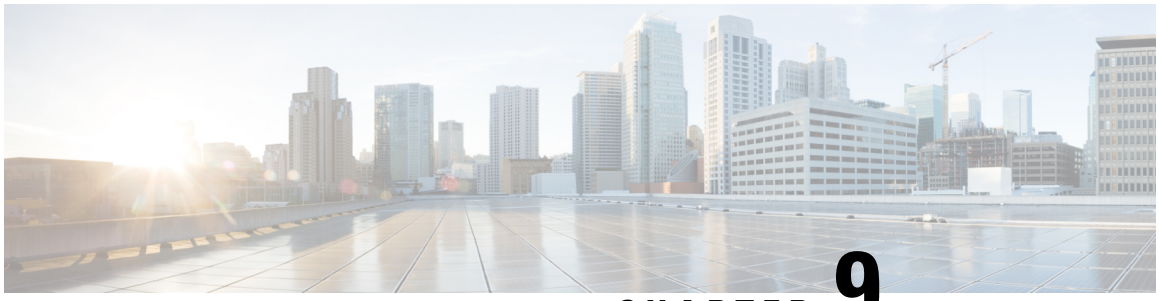
A message indicating that the Center fingerprint successfully updated appears.

Wait a few moments for the Center enrollment status to switch to Enrolled and the connectivity status to Connected.



In the **Global Center**'s administration system page the Center state is indicated as enrolled.


https://10.2.2.206/#/admin/system
78 days remaining
Evaluation Mode
System
Data Management
Network Organization
Sensors
Active Discovery
Users
Events
API
License
External Authentic...
Snort
Risk score
Knowledge DB
Current database information
Current database version: 20230712
Last import: Wednesday, July 12, 2023 4:57 PM
The KDB is managed by the global center, you cannot update it from this center.
Center fingerprint
Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894
Expires: Sep 14, 2025
Enroll to a Global Center
Center enrolled to a Global Center.
Reset
Unroll the center on the Global Center Administration page to be able to reset a Center.



CHAPTER 9

Center Backup and Restore

The Cisco Cyber Vision Center command-line interface (CLI) provides commands to back up and restore a Center. Use these commands to migrate a Center from one appliance or VM to another, such as from a cloud VM to a UCS appliance.

The backup archive includes the following information:

- Operating system settings, such as IP addresses, names, and certificates.
- Cisco Cyber Vision settings.
- Cisco Cyber Vision data.

After the restore is complete, the restored Center uses the network identity and data from the backed-up Center.

Backup and restore requirements and limitations

Before restoring a backup archive, make sure that the target Center meets the following requirements:

- The target appliance or VM has the same number of network interfaces as the backed-up Center.
- The target Center has the required base network configuration before the archive is transferred. At minimum, configure the `eth0` IP address.
- The target Center interface mode, such as single-interface or dual-interface mode, matches the backed-up Center.

Observe the following limitations when restoring a backup archive:

- If the restored Center reuses the network identity of the original Center, power off the original appliance before bringing the restored Center online.
- The Cisco Cyber Vision license is not included in the backup archive. Return the license from the original Center to the Smart Account server if required, and install a license on the restored Center.

- Report extension packages are not restored automatically. Install the report extension on the restored Center if your deployment requires it.

Back up the Cisco Cyber Vision Center

Use this procedure to create a backup archive of the Cisco Cyber Vision Center before migration, appliance replacement, or recovery operations.

Use this procedure to create a backup archive from an existing Cisco Cyber Vision Center. The backup is generated locally on the Center and can then be copied to another appliance for restore or to another storage location for safekeeping.

Before you begin

- Ensure that the Cisco Cyber Vision Center is running and accessible.
- Ensure that you have CLI access to the Center through SSH or console access.
- Verify that sufficient free space is available on the Center to generate the backup archive.
- If you plan to copy the backup file off the Center, ensure that a secure transfer method and target location are available.

Procedure

Step 1 Connect to the Center through SSH.

Step 2 Run the following command:

```
sbs-backup export
```

A backup file is generated in the `/data/tmp/ccv-center-backup/` directory.

In the following example, the generated file is named `ccv-center-backup-Center224433labautomccvlocal-5.4.0-20240405112443.tar.gz` .

Step 3 Copy the backup file to the target appliance or to a secure storage location for restore.

A backup archive of the Cisco Cyber Vision Center is available in `/data/tmp/ccv-center-backup/` and is ready to be transferred or used during a restore procedure.

What to do next

Use the backup archive during the restore procedure or transfer it to a secure storage location for retention according to your operational policy.

Restore the Cisco Cyber Vision Center

Use this procedure to restore Cisco Cyber Vision Center configuration and data from an existing backup archive.

Before you start the restore procedure, copy the Center backup archive to the new Center in the `/data/tmp/` directory.

Before you begin

- Ensure that the backup archive is already copied to the `/data/tmp/` directory on the target Center.
- Ensure that you have CLI access to the Center through SSH or console access.
- If the restored Center will reuse the previous Center network identity, ensure that the old appliance is powered off.

Procedure

Step 1 Connect to the Center through SSH.

Step 2 Run the following command:

```
sudo -i sbs-backup import <path to the center backup>
```

Step 3 Type `reboot` to restart the Center.

Step 4 Install the report management extension if your deployment requires it.

Step 5 Install a license on the restored Center.

The Cisco Cyber Vision Center is restored from the backup archive and is ready for any required post-restore tasks, such as report extension installation and licensing.

Automate Cisco Cyber Vision Center backups

You can use file-transfer tools to automate Cisco Cyber Vision Center backup export and transfer.

`rclone` is a command-line program for managing files across local and remote storage systems. You can use it to move or synchronize Center backup files with a remote location.

Procedure

Step 1 Configure `rclone` for the remote storage system.

```
sudo -i
rclone config
```

For configuration options, see rclone documentation.

Step 2 Use the `rclone` command to move the backup directory to the remote location.

Syntax:

```
rclone [options] subcommand <parameters> <parameters...>
```

For example:

```
rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
```

In this example, `rclone` moves the backup files stored in `/data/tmp/ccv-center-backup/` to the remote location `lab_sftp:/srv/pub/`.

Automate backup export and transfer with a Bash script

You can use a Bash script to run the commands that generate the backup archive and transfer it to a remote location.

- Generate the backup archive.
- Transfer the backup archive to a remote location.

For example:

```
#!/bin/bash
sbs-backup export
rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
```

Schedule the backup script with cron

You can schedule a Bash script with `cron` to back up Cisco Cyber Vision data and send the backup file to a remote location.

Use the following commands to create the schedule:

1. Edit the crontab file:

   ```
   crontab -e
   ```

2. Add the cron entry. The following example runs `/data/tmp/backup.sh` every Saturday at 1:00 a.m.:

   ```
   00 01 * * 6 bash /data/tmp/backup.sh
   ```