

Cisco Cyber Vision Center Appliance Installation Guide, Release 5.3.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

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **About this documentation** 1

Document purpose 1

Warnings and notices 1

CHAPTER 2 **Information and characteristics** 3

Information and characteristics 3

CHAPTER 3 **Connect the Center** 7

Connect an external device 7

Connect interfaces for communication 7

Power up the Center 8

CHAPTER 4 **Configure the Center** 9

Basic Center configuration 9

Access the basic Center configuration 10

Accept the End User License Agreement 10

Select the language to match your keyboard 11

Select the Center type 11

Center 12

Global Center 13

Configure the Center's Administration Network Interface 14

Set interfaces (dual or single) 16

Configure the Center's DNS 16

Synchronize the Center and the sensors to NTP servers 16

Give the Center a name 18

Set the Center's password 18

Configure the Center's Collection network interface 19
Authorize networks 19
Complete the basic Center configuration 20
configuration 21
Install the certificate in your browser 21
Install 27
Configure the user interface security 30
Upload a p12 31
Generate a CSR 33
Configure Center data synchronization 35

CHAPTER 5 Configure a Center DPI 39
Center DPI 39
Configure Center DPI 39

CHAPTER 6 Configure the Cisco Cyber Vision Center synchronization 41
Global Center Configuration 41
Center enrollment 41
Center unenrollment 44
Force the unenrollement of a Center 45

CHAPTER 7 Upgrade procedures 47
Architecture with a Global Center 47
Check the Global Center and Centers' health 47
Update the Global Center 48
Update the sensors 48
Update hardware sensors 48
Update IOx sensors 49
Architecture with a single Center 50
Update the Center 50
Update the sensors 50
Update hardware sensors 50
Update IOx sensors 51

CHAPTER 8 **Certificate renewal** 53

Renew the certificate of a Center 53

Update the Global Center fingerprint 54

Update a Center with sync fingerprint 58

CHAPTER 9 **Center Backup and Restore** 65

Backup and Restore Constraints 65

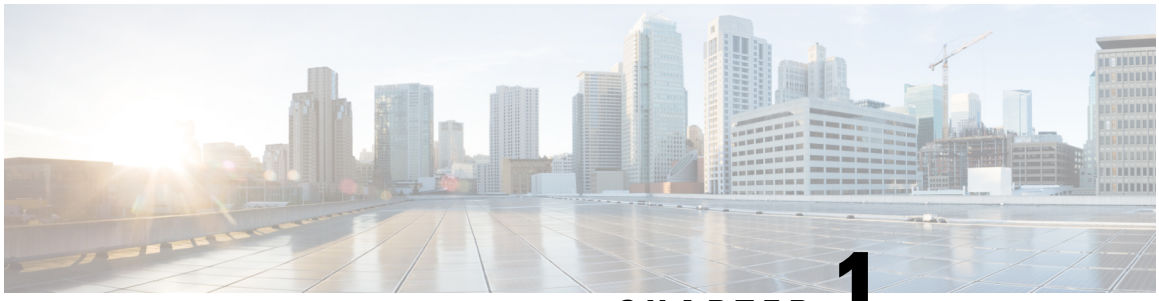
Backup Cyber Vision Center 66

Restore Cyber Vision Center 66

Automate the Backup of the Cyber Vision Center 67

Bash Script 68

Cron 68



CHAPTER 1

About this documentation

- Document purpose, on page 1
- Warnings and notices, on page 1

Document purpose

This installation guide shows how to connect, configure and install running on:

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

You will also find the upgrade procedures for an architecture with a Global Center and for an architecture with one Center only.

This documentation is applicable to **system version 5.3.x**.

Warnings and notices

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

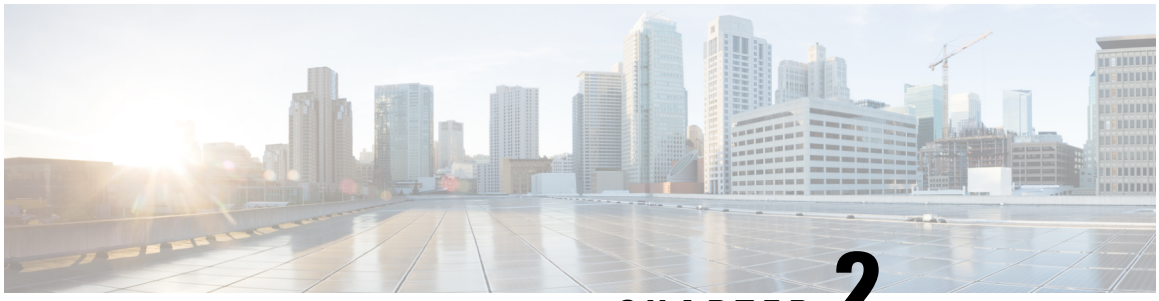
The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.

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, on page 3

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.

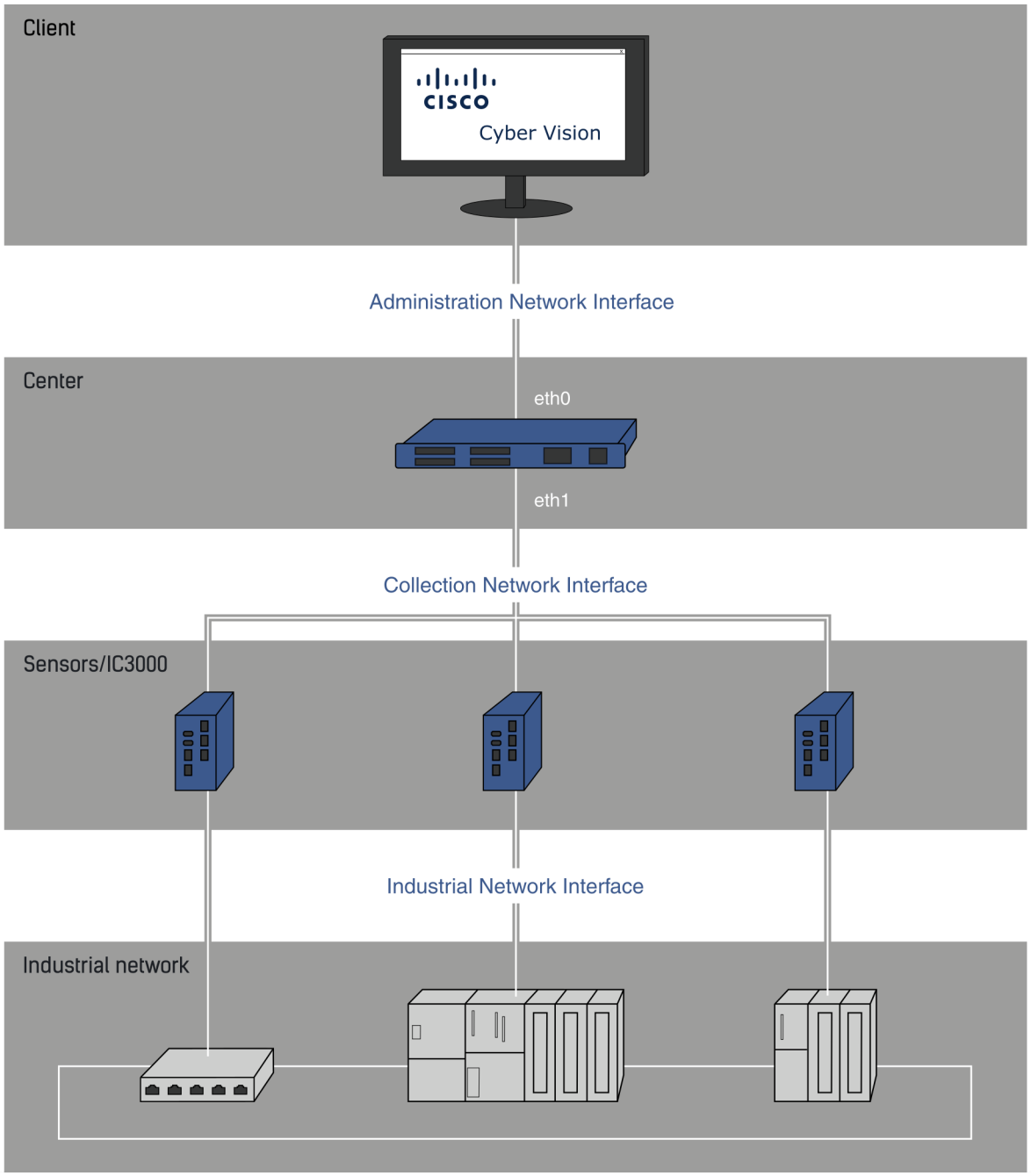
Networks or segments involved

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

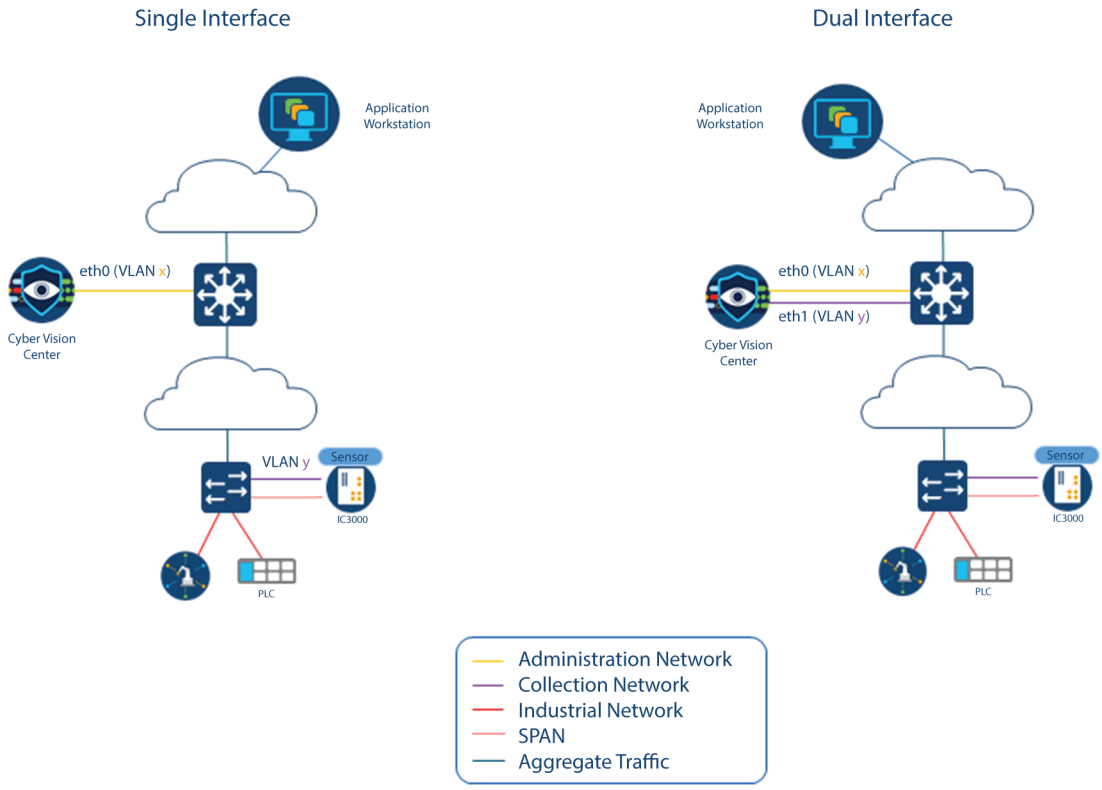


Configuring single or dual interface (not applicable to a Global Center)

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.

Information and characteristics

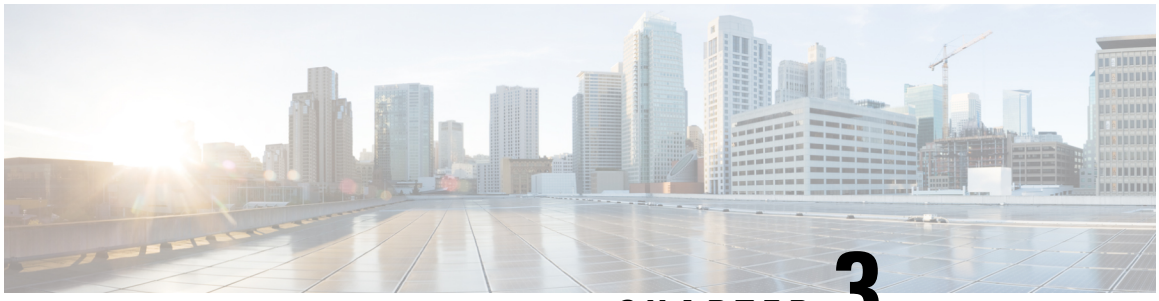


The Center provides two dedicated and separate 10 Gigabit Ethernet network ports to connect to these two networks.

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.

Information and characteristics



CHAPTER 3

Connect the Center

Before turning on the Center for the first time, you will need to connect the Center to a VGA display and a keyboard or a console so you can configure it, and to network interfaces to make it operational.

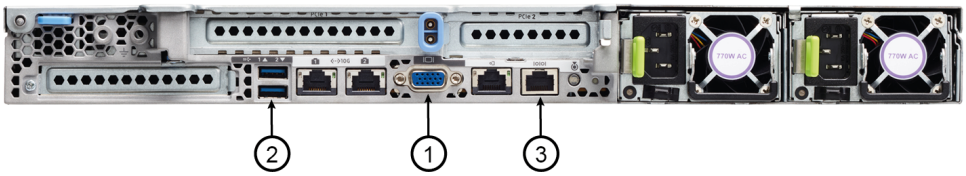
- Connect an external device, on page 7
- Connect interfaces for communication, on page 7
- Power up the Center, on page 8

Connect an external device

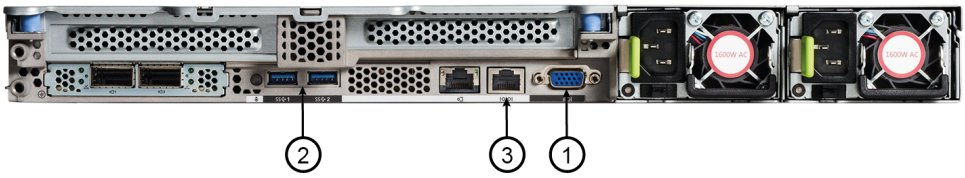
You need to connect an external device to access and configure the Center.

To do so, connect an external display to the VGA port **(1)** and a keyboard to any USB port **(2)** on the Center, or a console to the console serial port **(3)**.

Cisco Unified Computing C220 M5:



Cisco Unified Computing C225 M6:



Connect interfaces for communication

Cisco Unified Computing C220 M5:



Cisco Unified Computing C225 M6:



Global Center:

- Connect the eth0 interface to the network **(1)**.

Center with dual interfaces (two separate networks):

- Administration interface (eth0):

  Connect the administration network cable to the **Administration LAN port (1)** to connect the Center with the user interface or the Global Center.

- Collection interface (eth1):

  Connect the collection network cable to the **Collection LAN port (2)** to connect the Center with its sensors.

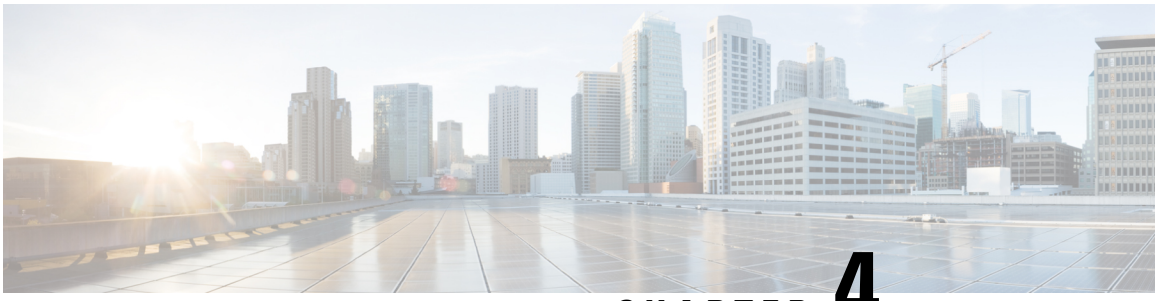
Center with single interface:

- Connect the eth0 interface to the network **(1)**.

  Administration and Collection will use the same interface.

Power up the Center

Connect the Center to the power supply and switch it ON from the Center front view.



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:

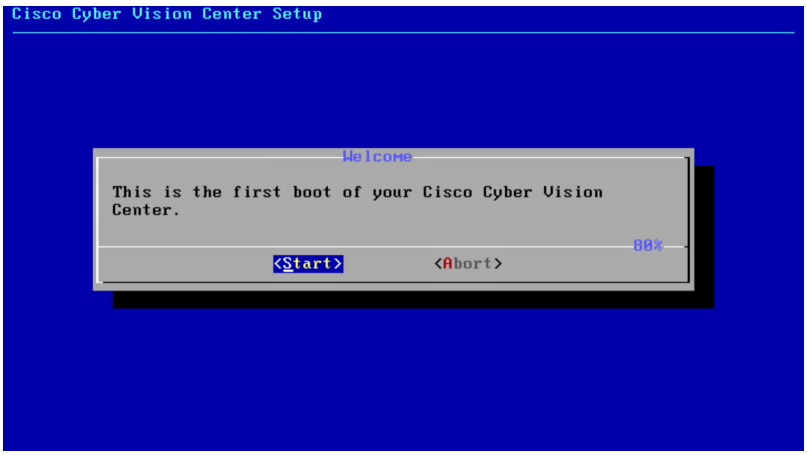
- Local NTP and DNS IP addresses.
- The Collection interface network address (n/a for a Global Center or a Center using a single interface).

In the case of manual Administration network interface configuration:

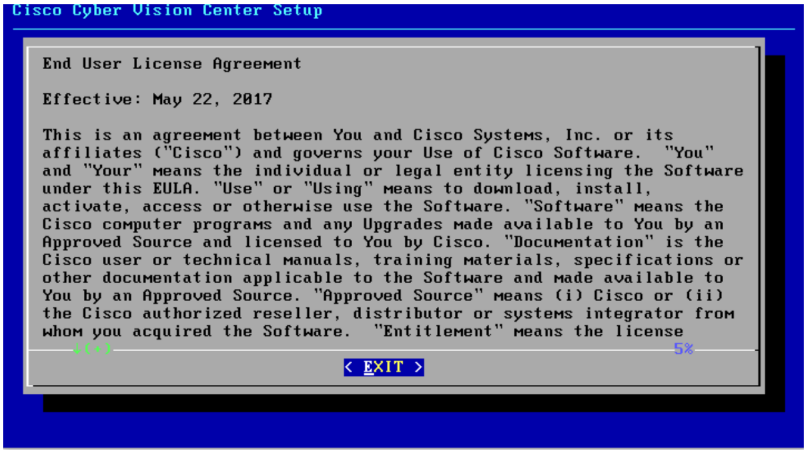
- Its IP address.
- Its netmask (in a two-number format, e.g. 192.168.1.0/24).
- Its default gateway (to reach devices located outside the local network).

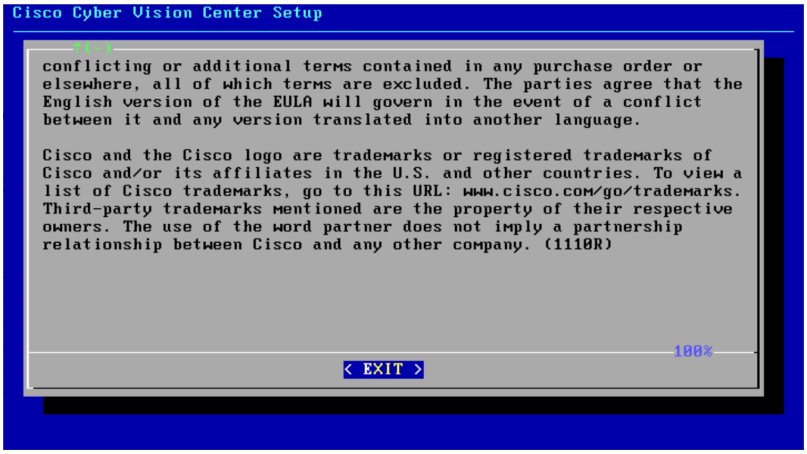
Access the basic Center configuration

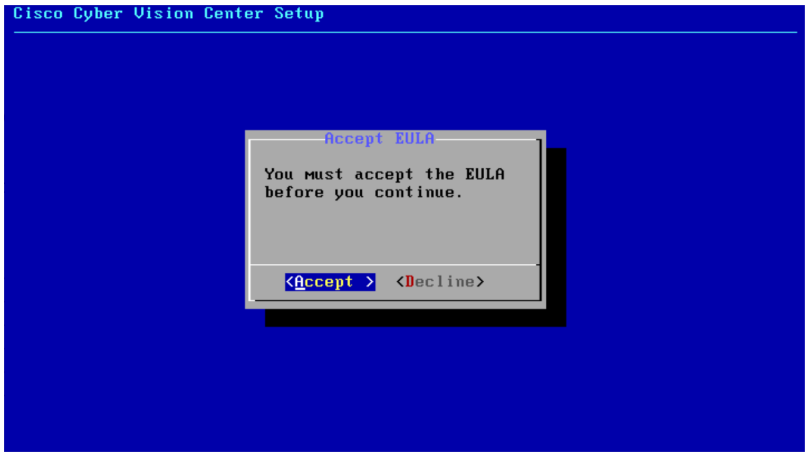
The Center wizard is displayed on your screen as you power on the Center. Enter Start to start configuring the Center.



Accept the End User License Agreement

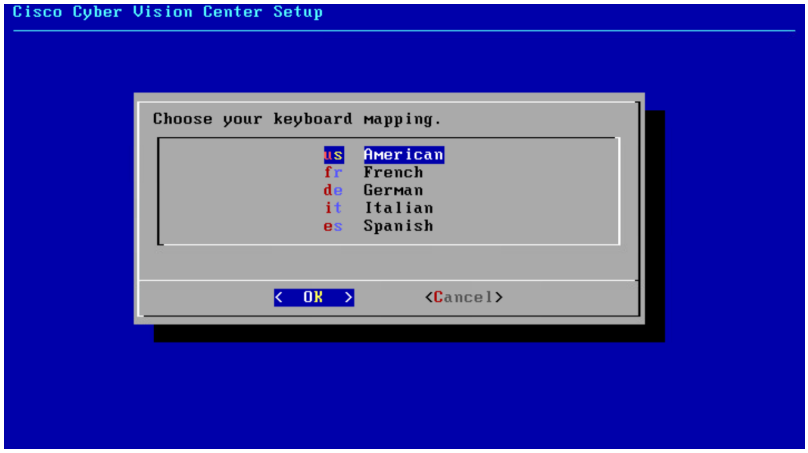






Select the language to match your keyboard

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

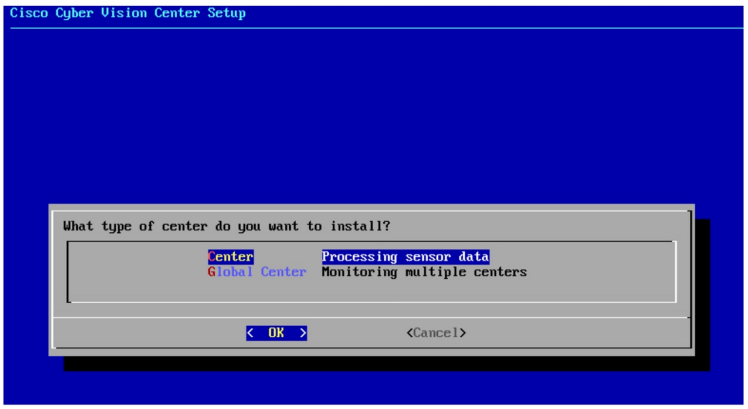


Select the Center type

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

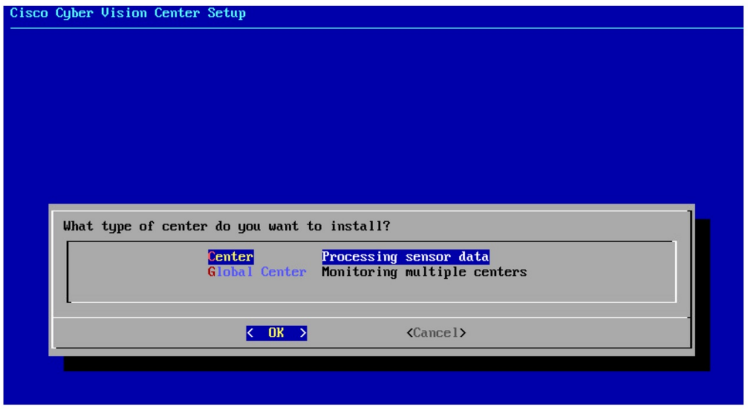
- A **Center** receives metadata from sensors and store them into an internal database (Postrgresql). It can be standalone or synchronized with a Global Center. A Center with sync is similar to a standalone Center from a functionality point of view, except for the link to a Global Center. You must install 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.



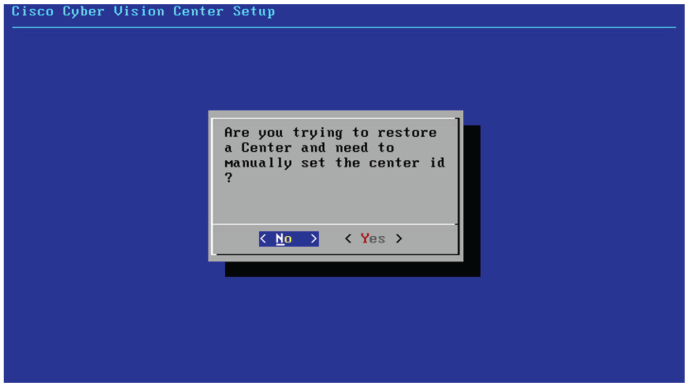
Center

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.



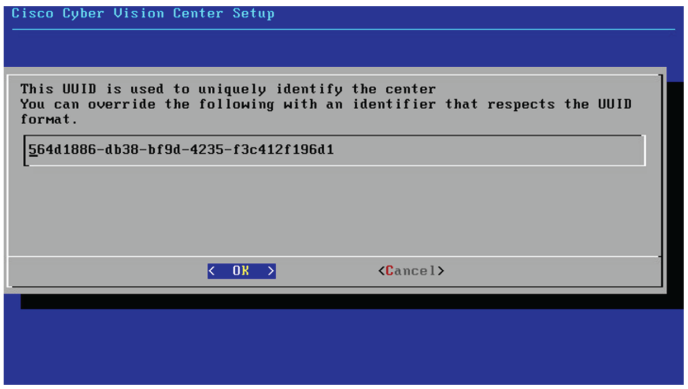
If you're reinstalling the Center and want to restore it, select Yes.



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"
```

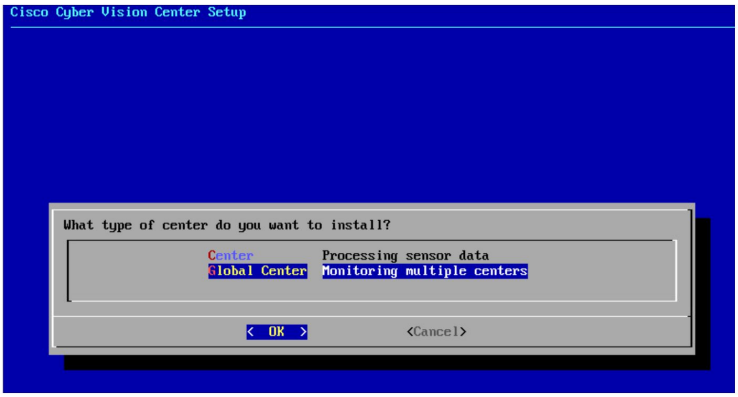
Type the id into the basic Center configuration UUID field.



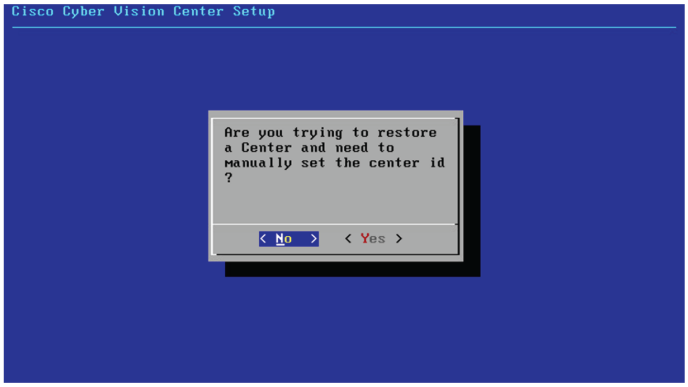
Click OK. You will be directed to the next step.

Global Center

If installing a Global Center, select the second option.



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



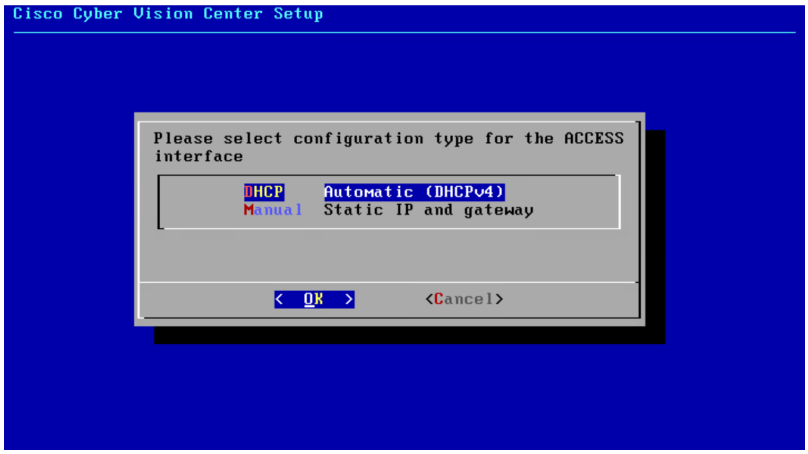
You will be directed to the next step.

Configure the Center's Administration Network Interface

The Center uses a dedicated sub-network on the Administration interface. It is possible to change it if the default one doesn't fit the environment on which the Center will be connected.

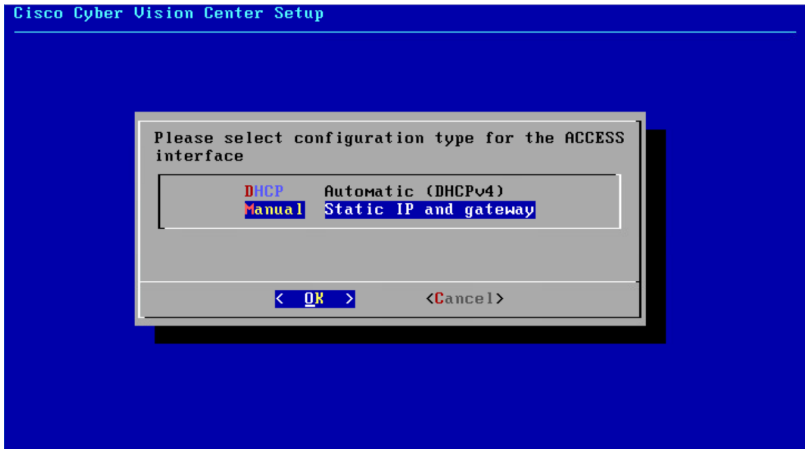
The Administration network interface configuration can be done either:

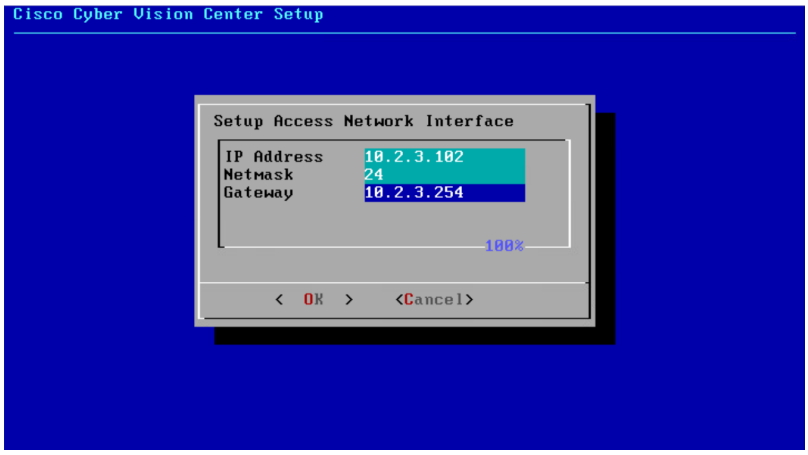
- Using a DHCP server, if there is one available on the network.



In this case, enter OK. Settings will be adjusted automatically, and you will be directed to the next step.

- Manually:





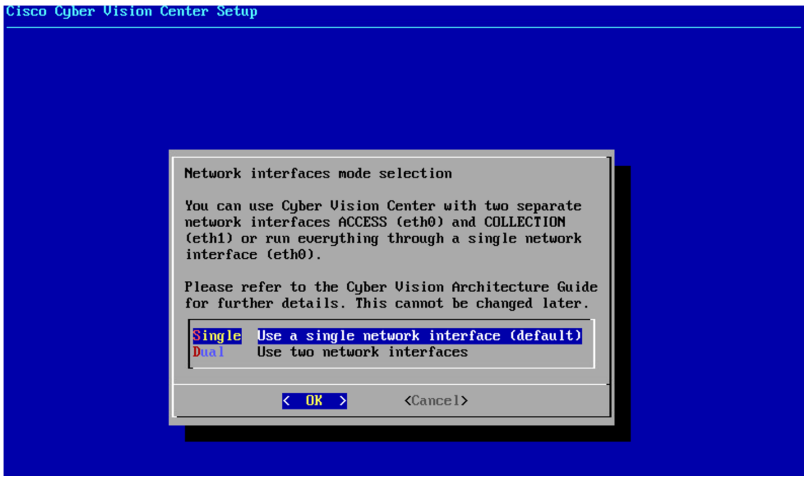
Enter the Administration network interface's IP address, netmask (in a two-number format), and gateway.

Set interfaces (dual or single)

This step is not applicable to a Global Center.

Regarding a Center, it is possible to:

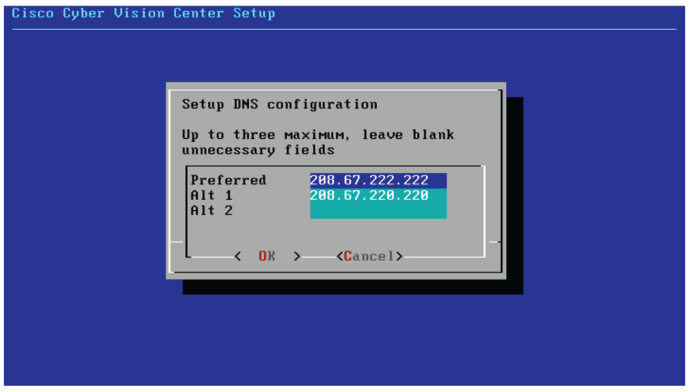
- Use a single interface. In this case, select the Single option.
- Set the Administration and Collection network interfaces on two distinct interfaces (recommended for security). In this case, select the Dual option.



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

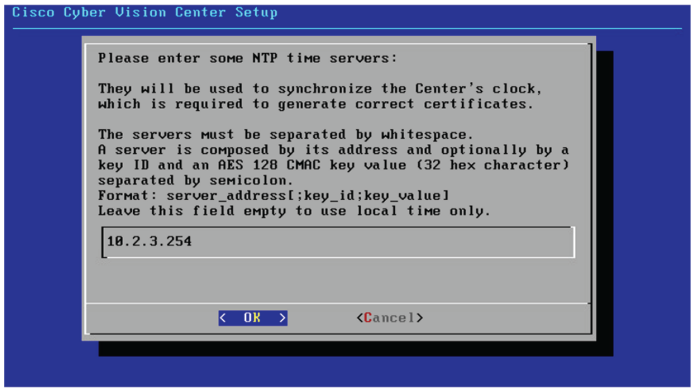
Configure the Center's DNS

Type a DNS server address and optional fallbacks.

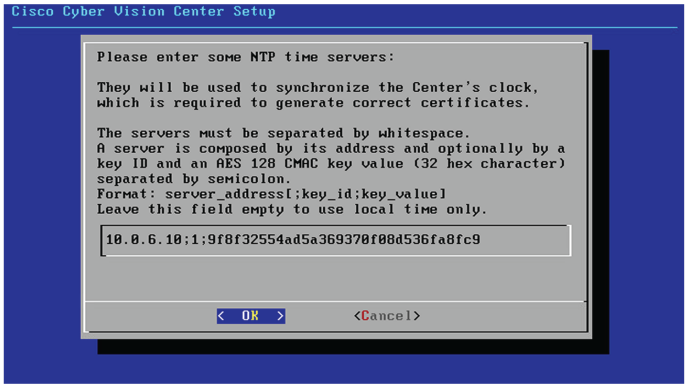


Synchronize the Center and the sensors to NTP servers

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.



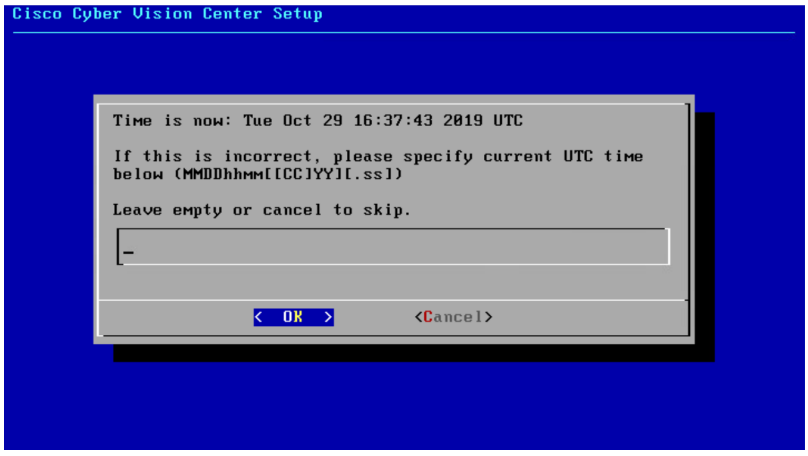
Optionally, add a key ID and an AES A28 CMAC key value separated by a semicolon with the corresponding NTP server.



The synchronization takes a few seconds.

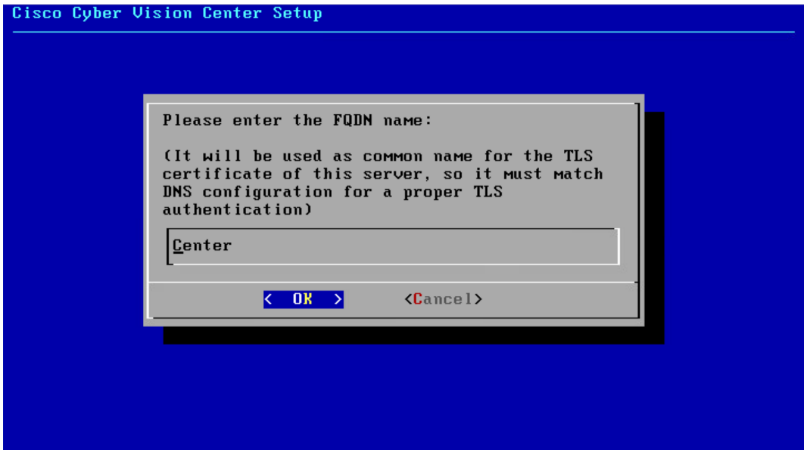
Check that the time is correct, or set the time manually.

Note The time is set in UTC standard.



Give the Center a name

Note This name will be used in the Center certificate.

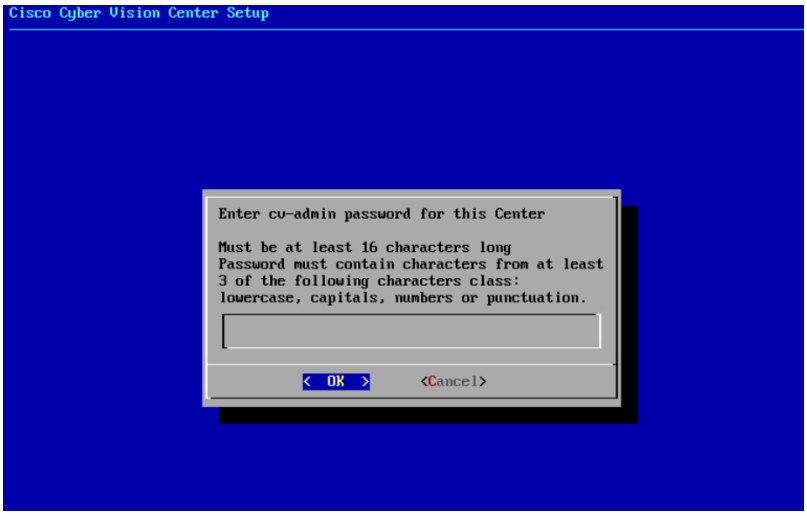


Enter the Center name provided by your administrator or type 'Default' which is a secure value.

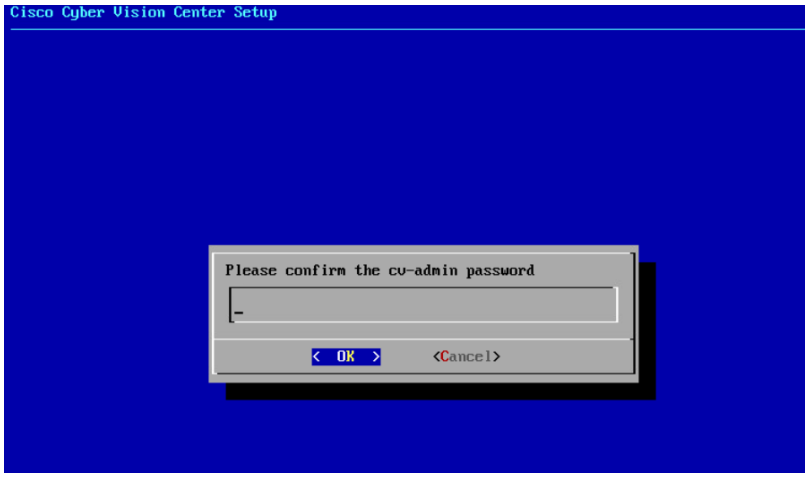
Note This name must match the DNS name you will use to access the Center through SSH or a browser.

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.

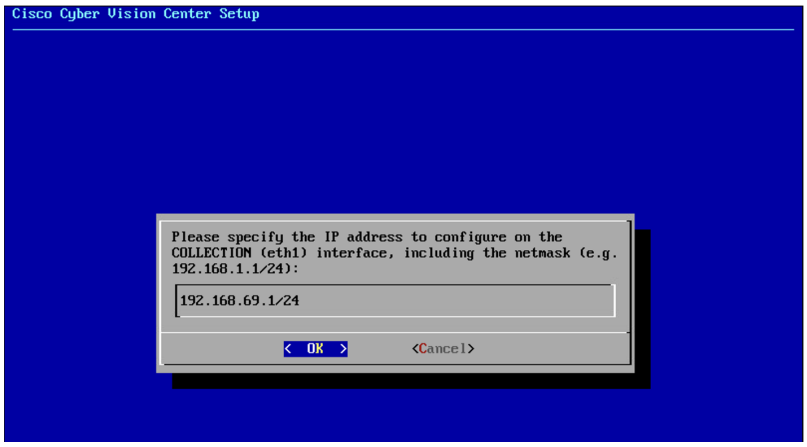


Configure the Center's Collection network interface

This step is not applicable to a Global Center.

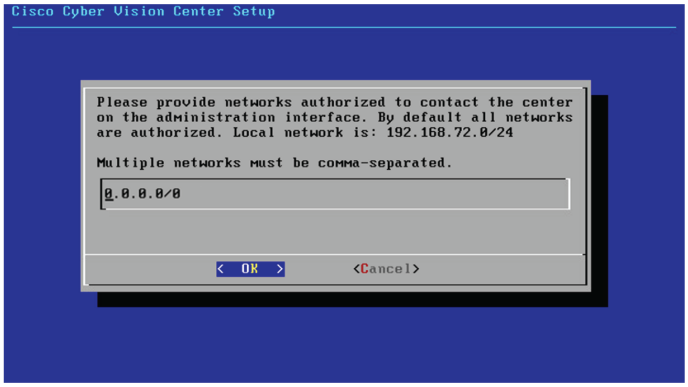
This step will only appear if the dual interface option has been selected during the Set interfaces (dual or single), on page 16 step.

Type the IP address of the Collection network interface:



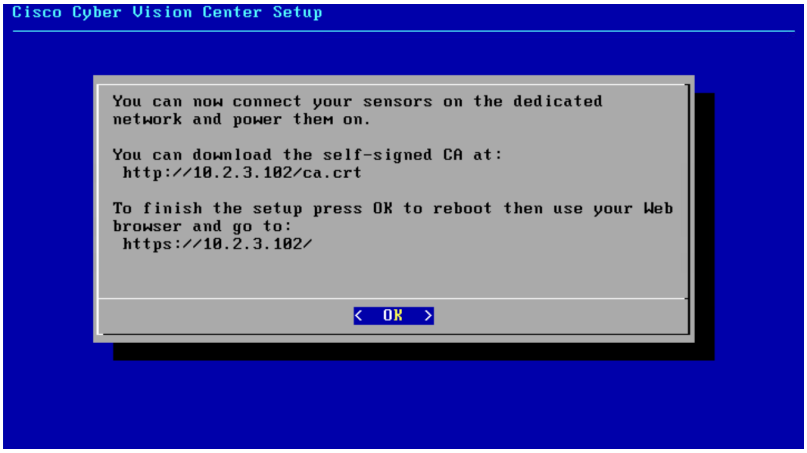
Authorize networks

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.

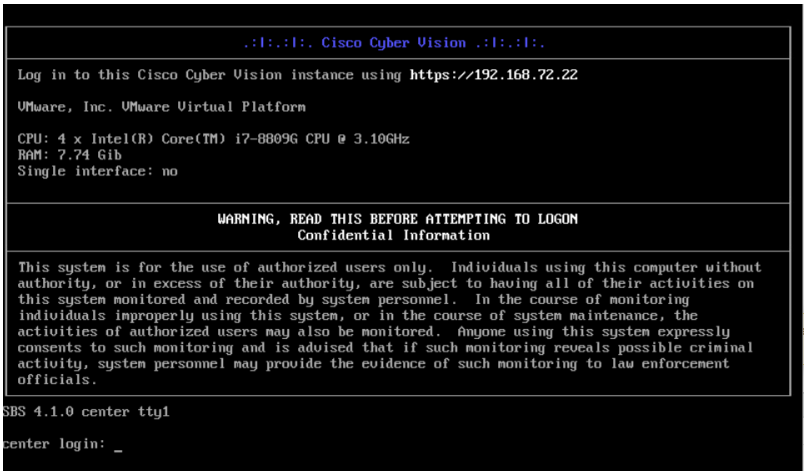


Complete the basic Center configuration

Next is the last screen of the basic Center configuration. It reminds you the addresses set to be used to download the CA certificate and access . Save these addresses somewhere, you will need them later to access the user interface.



Enter OK to finish the basic Center configuration.



Note To connect through CLI in serial consol or SSH you must use ‘cv-admin’ as user and the instance ID as password. This user has limited rights and many CLI commands will require permission elevation:

- prefix the command with "sudo".
- or open a root shell using "sudo -i" and enter the command.

Close the Center configuration window before proceeding with the next steps of configuration.

To proceed with the configuration, open your browser and go to the URL previously indicated to access the user interface.

Note Each Center includes its own PKI (Public Key Infrastructure), with a CA (Certification Authority), that will be used to establish the TLS connection with the sensors and to clients. The CA must be installed on each client browser (see the following chapters).

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 27.

Procedure

Step 1 Open your browser.

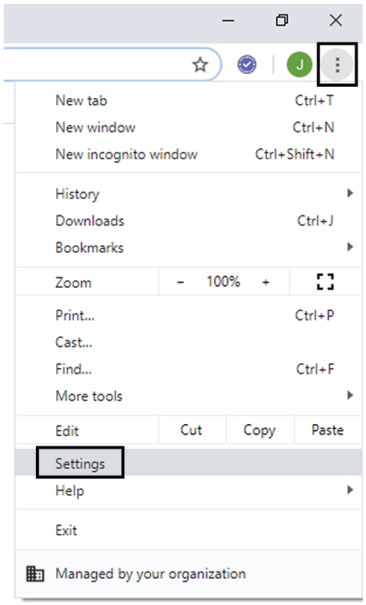
Step 2 Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.

The certificate is downloaded.

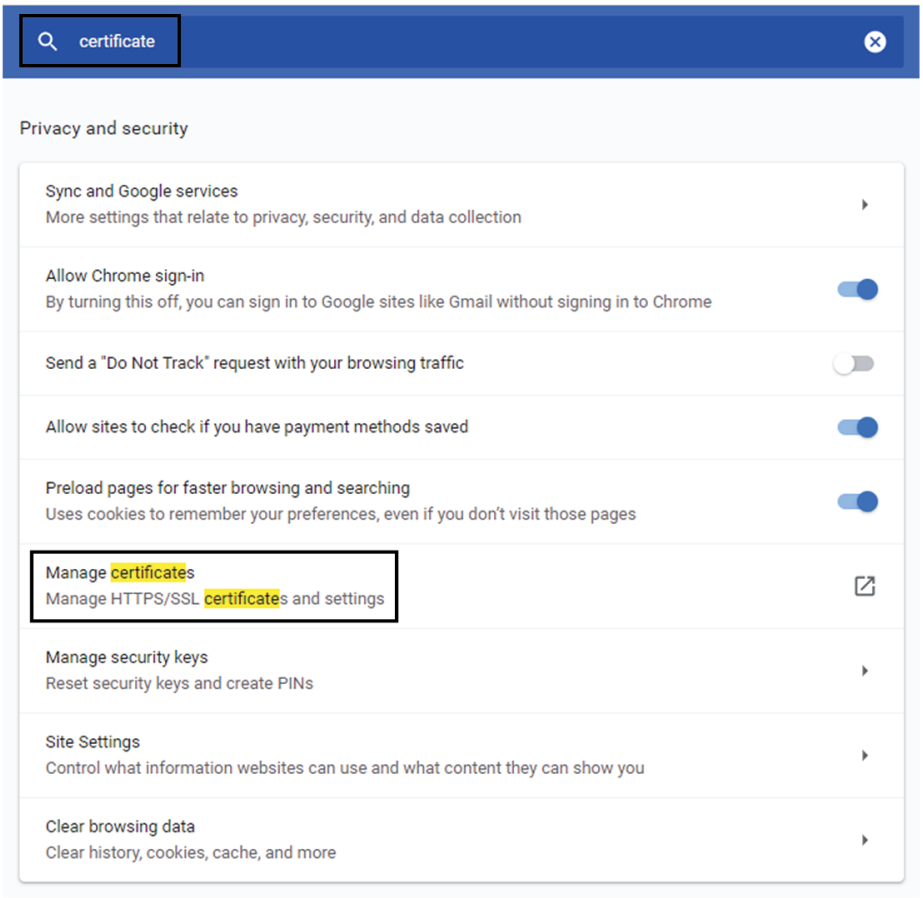
Step 3 Save the certificate on your computer.

Step 4 In the browser, access the settings.

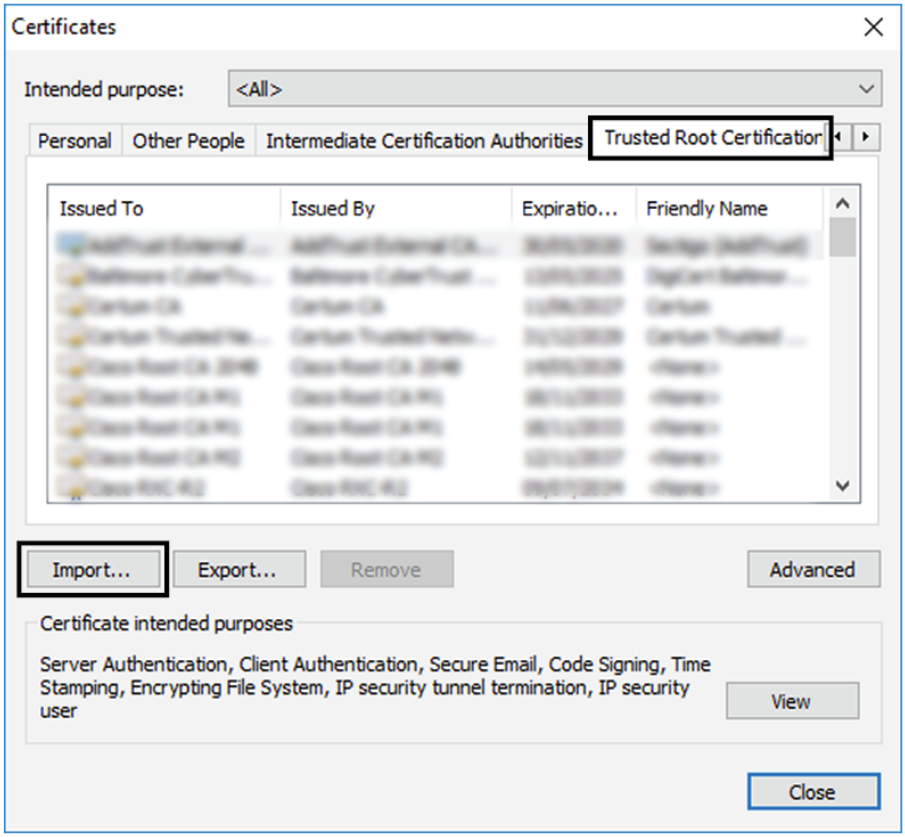
Example: Chrome



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

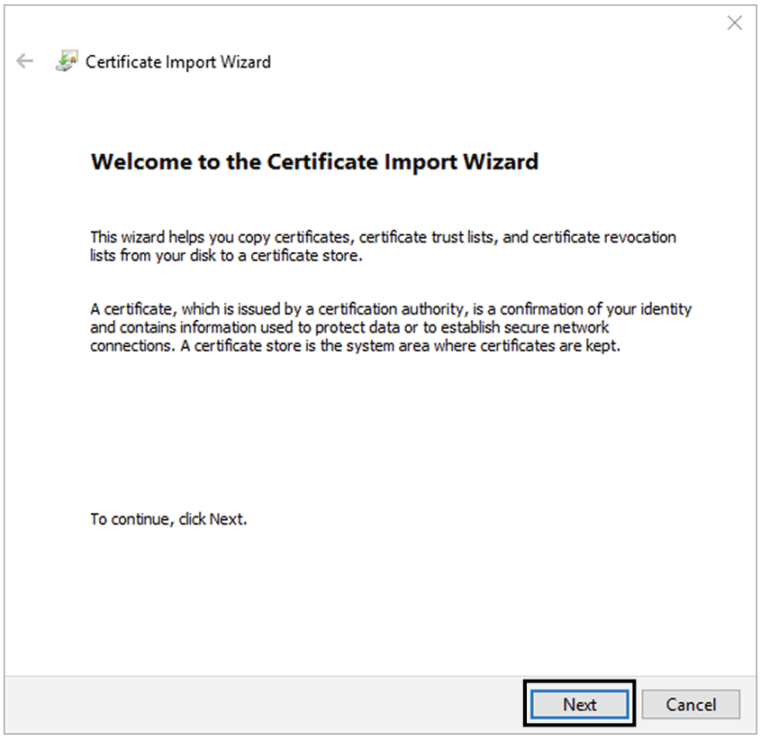


Step 6 Access the Trusted Root Certification tab and click Import.



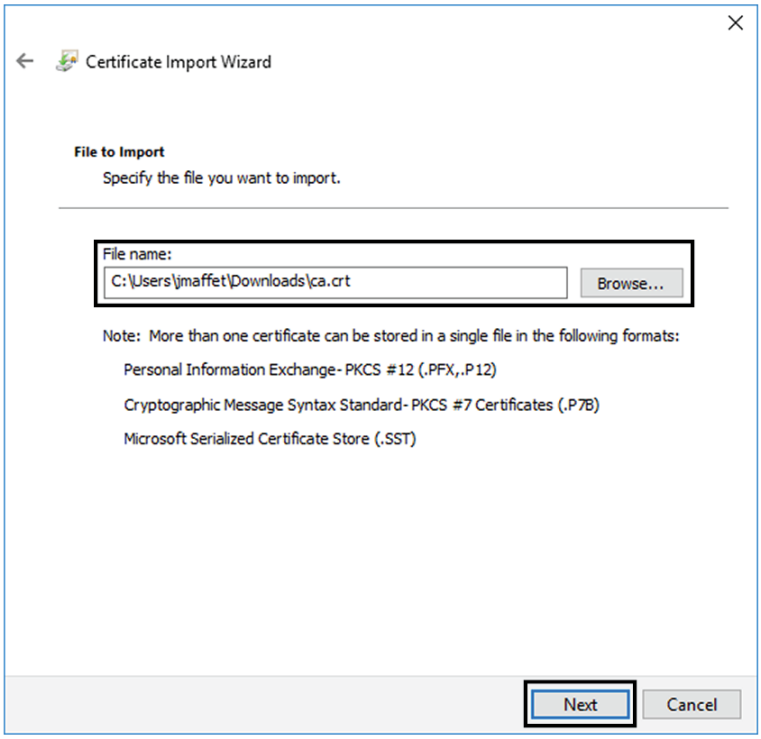
A certificate importation wizard opens.

Step 7 Go to the next step.

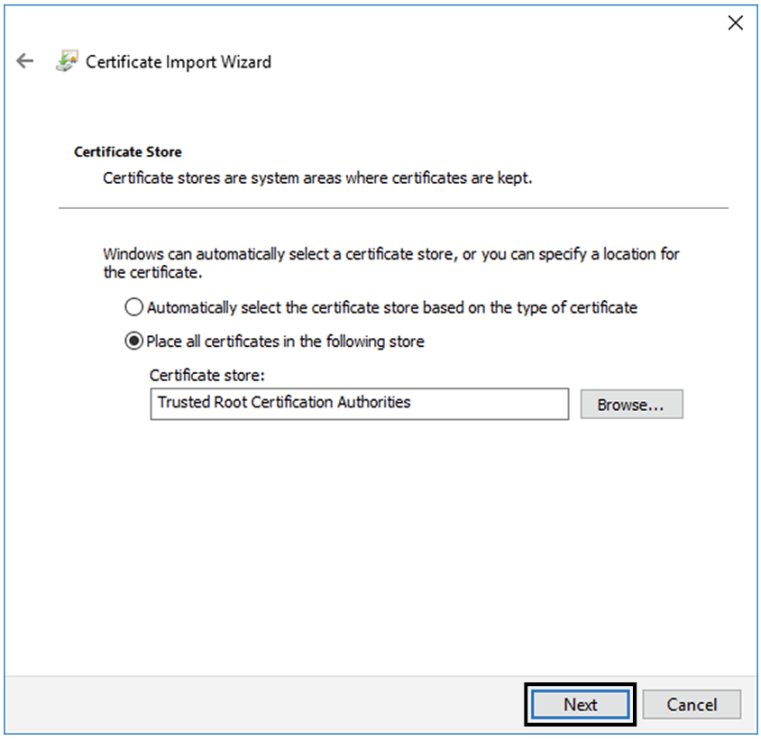


Step 8 Search for the certificate you downloaded earlier.

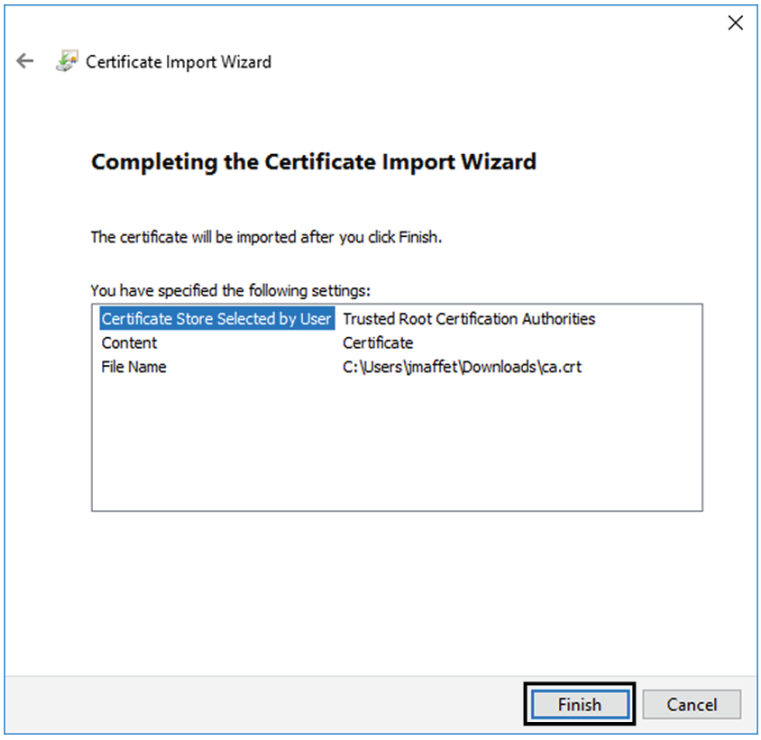
Step 9 Go to the next step.



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 27

Install

Access the installation wizard:

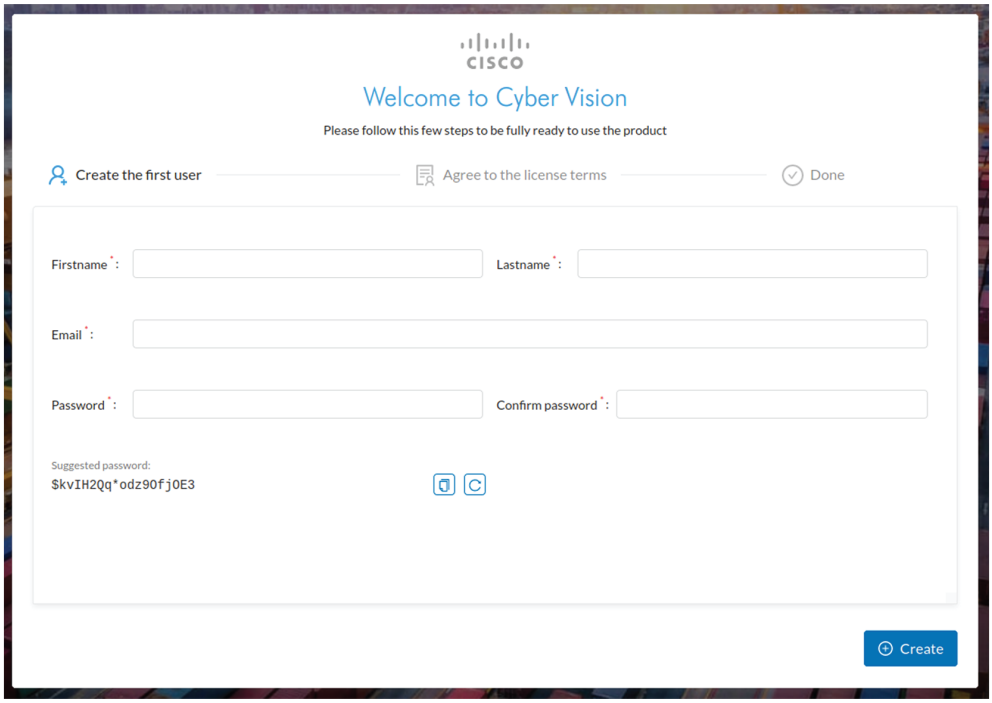
Procedure

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:**

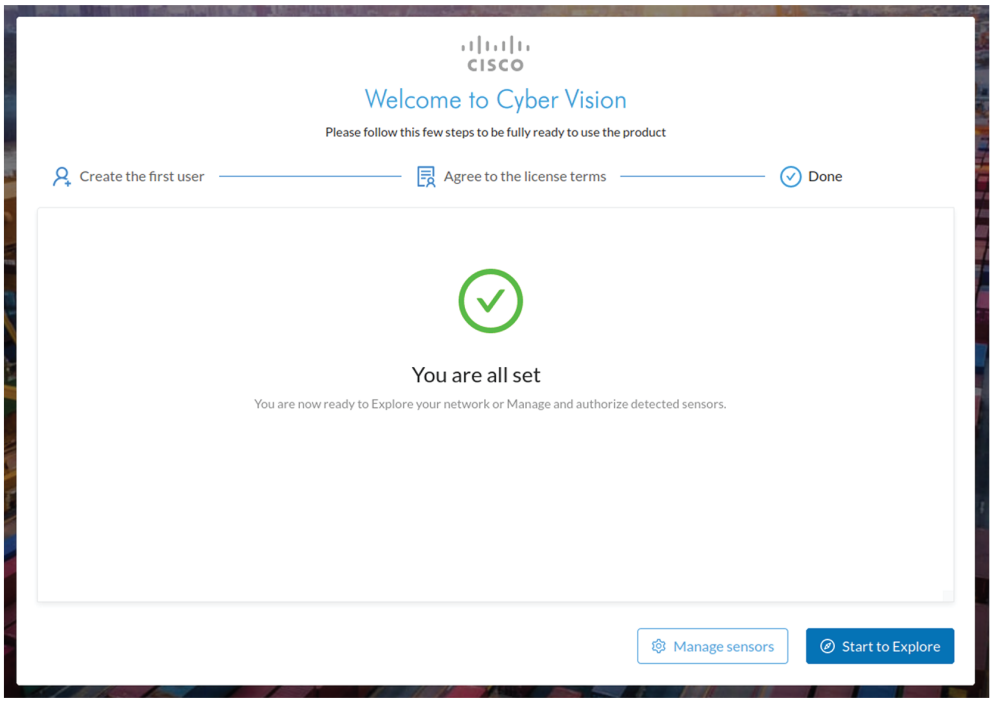


Step 7

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 30.

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 35.

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

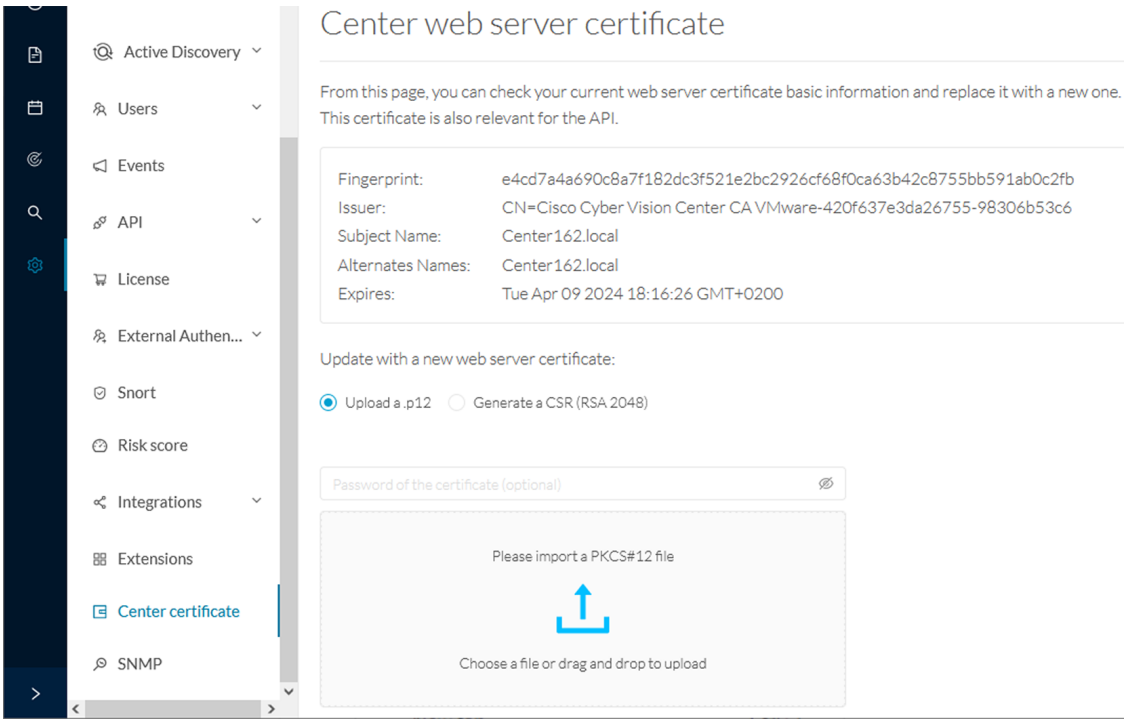
This section explains how to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

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.

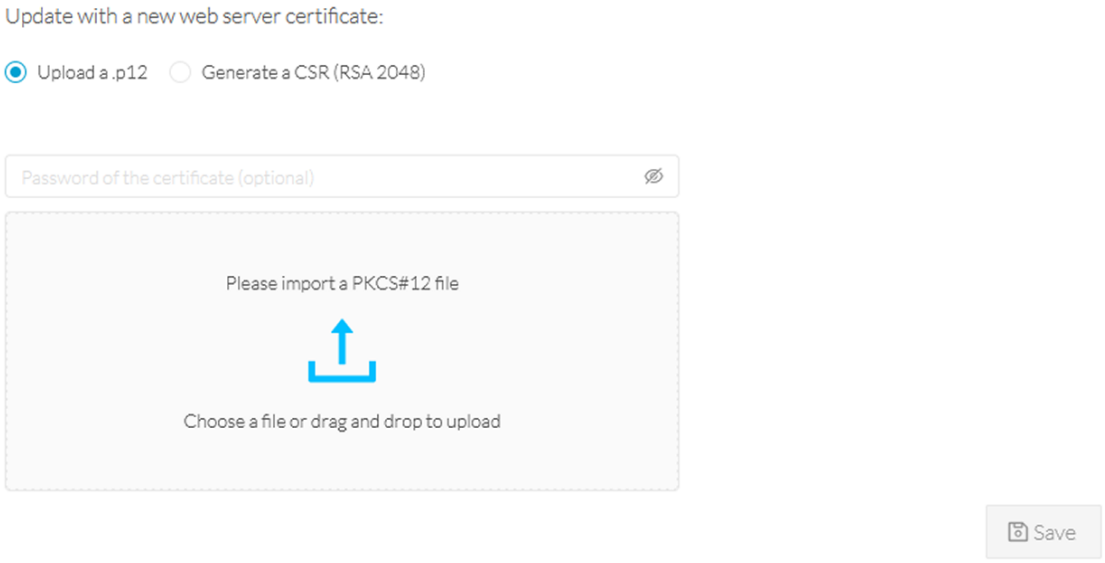
Upload a p12

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

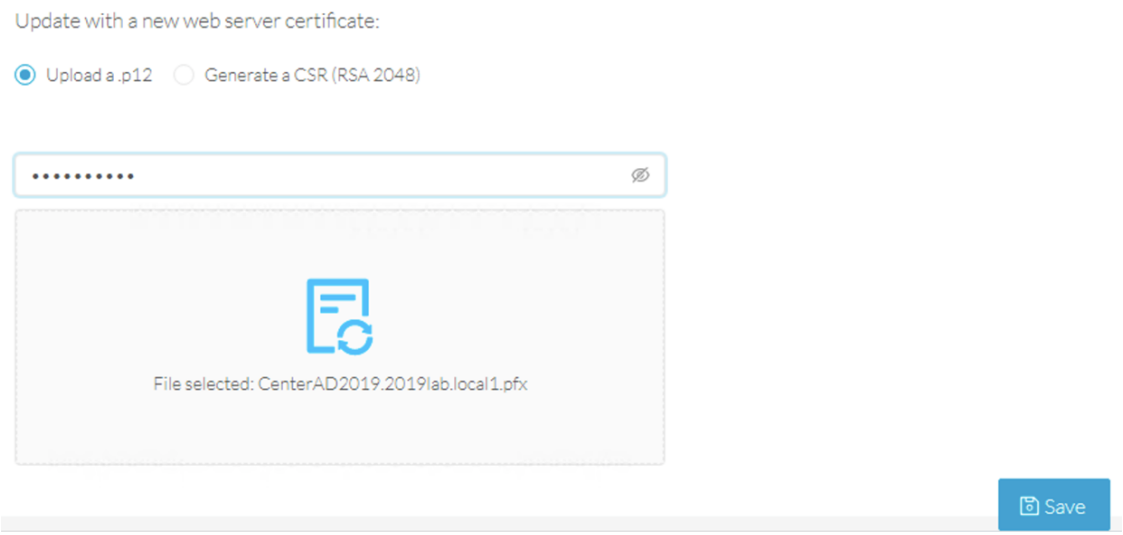
Step 1 Select Upload a .p12.



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

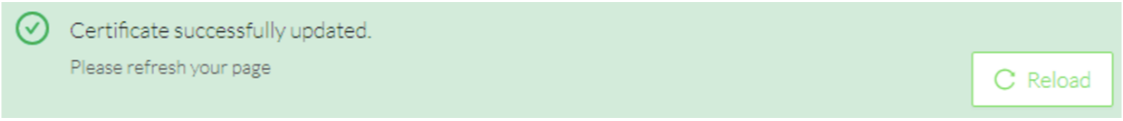
Step 2 Type the certificate password.

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



Step 4 Click Save.

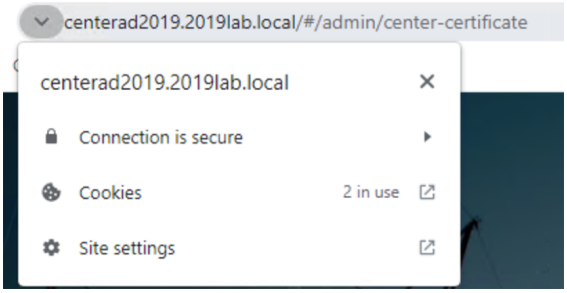
The following message appears:



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

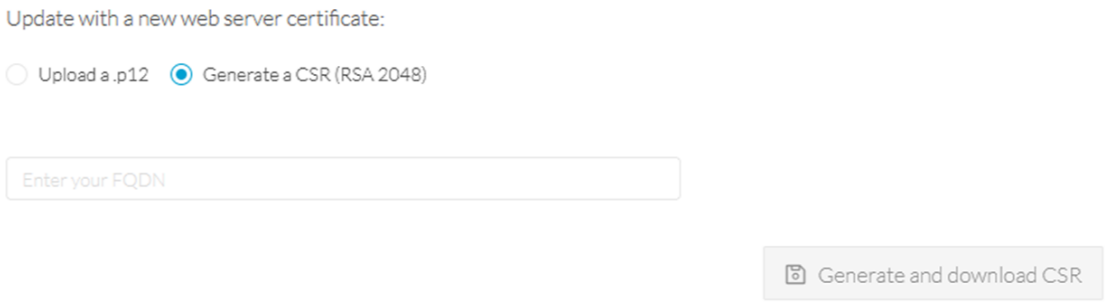
If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 35.

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.



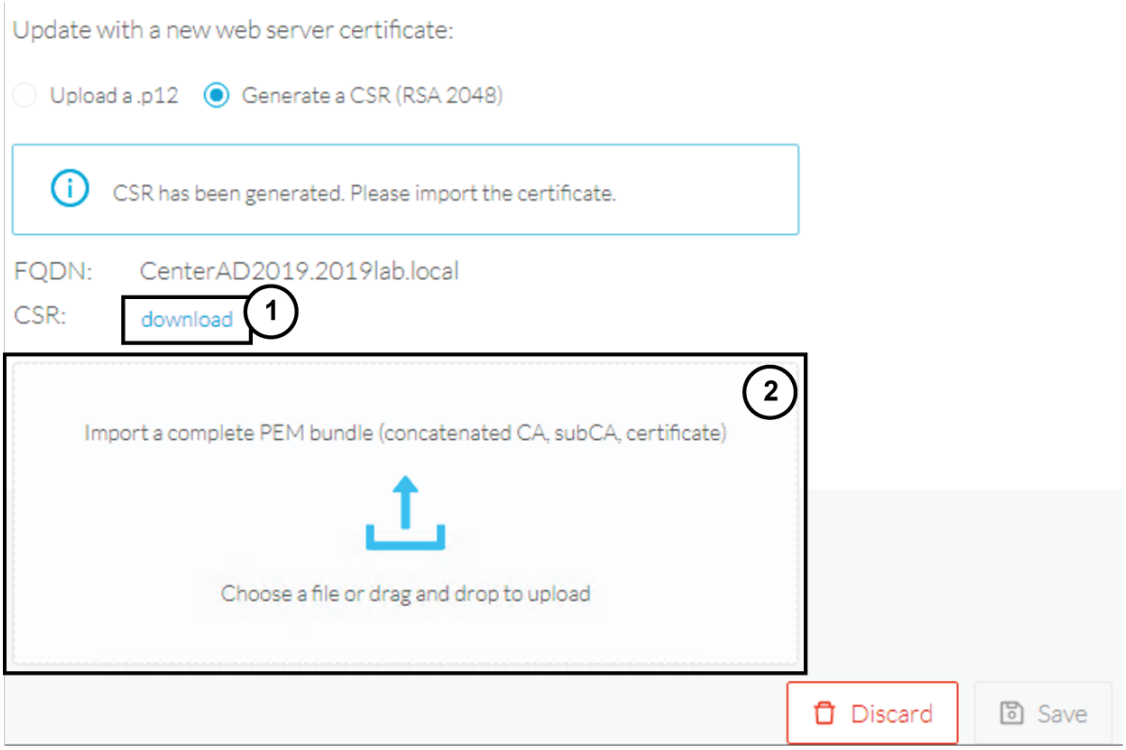
Step 2 Enter the Center FQDN as registered on your DNS server.

Step 3 Click the Generate and download CSR button.



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

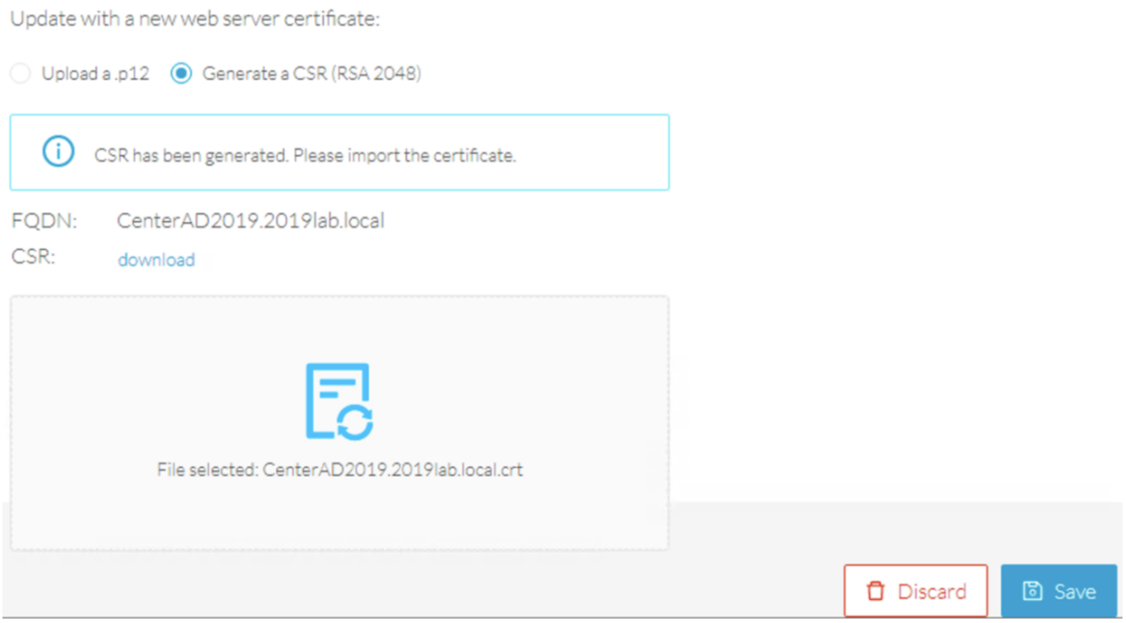
Step 4 Click the download button **(1)**.



A <FQDN>.csr file is downloaded.

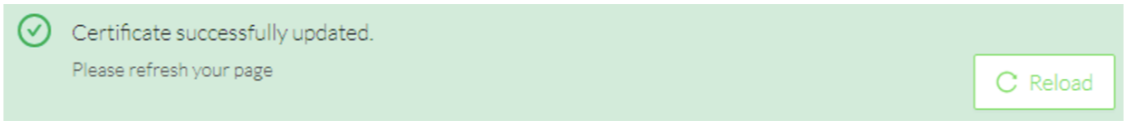
Step 5 Use the <FQDN>.csr file to generate a pem certificate from your enterprise Certification Authority.

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.

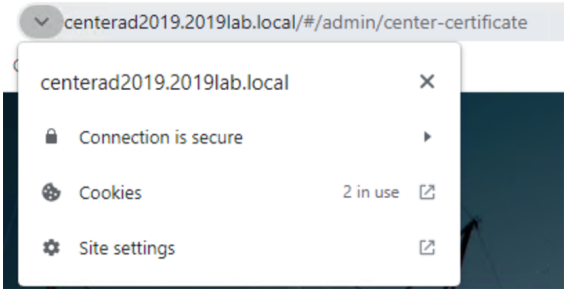
The following message appears:



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 35.

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.

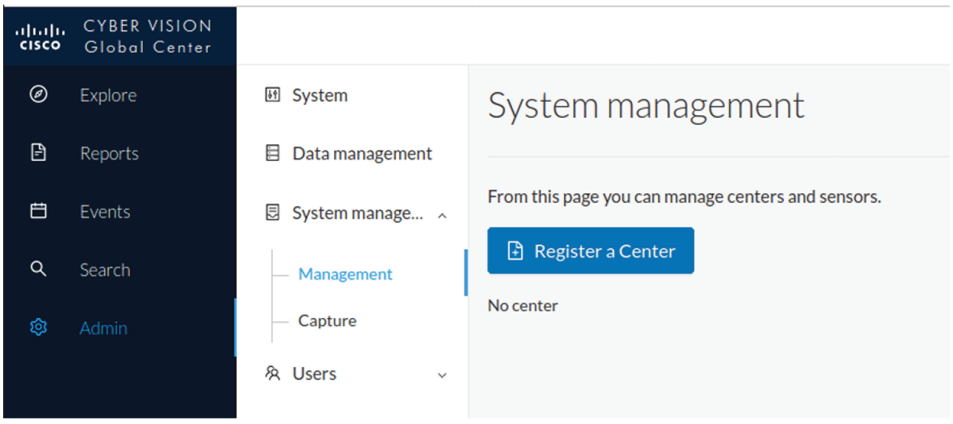
Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists of registering the Center in the Global Center and enrolling the Center to the Global Center. To do so, you need to open each's 's GUI.

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.

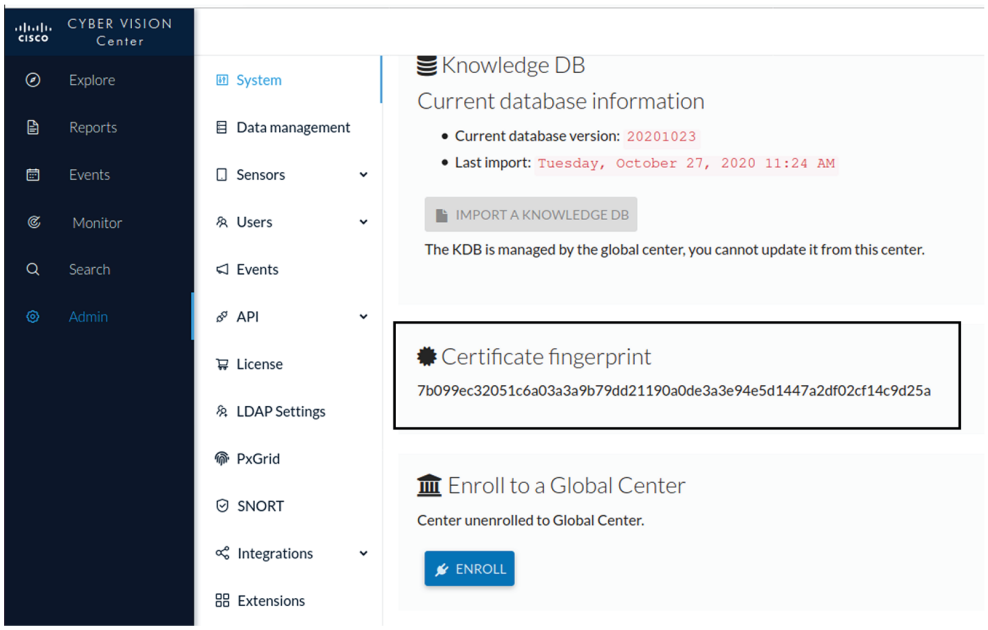
Step 2 Click the **Register a Center** button.



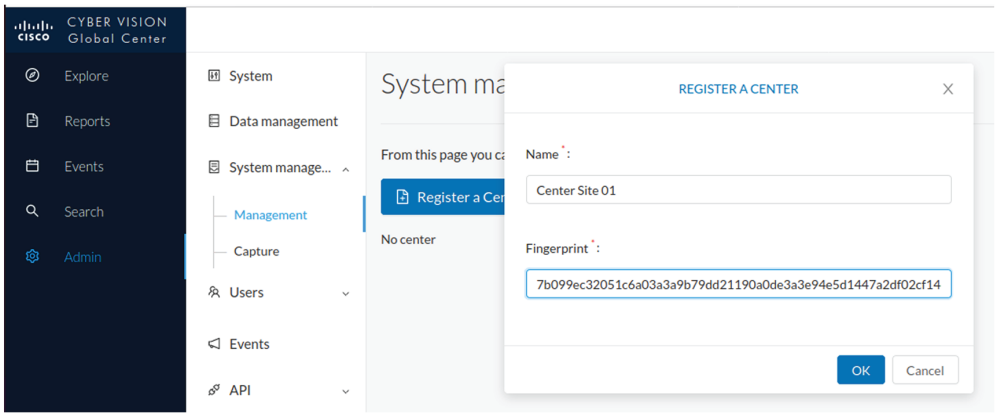
The window "Register a Center" pops up, ready to be filled. Now you must access the Center's GUI to retrieve its fingerprint.

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

Step 4 Scroll down to Certificate fingerprint and copy it.

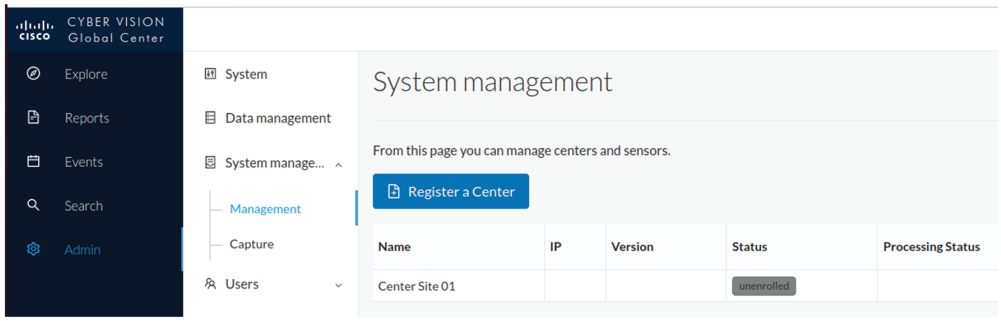


Step 5 In the Global Center's GUI, give a name to the Center, and paste the Center's fingerprint into the corresponding field



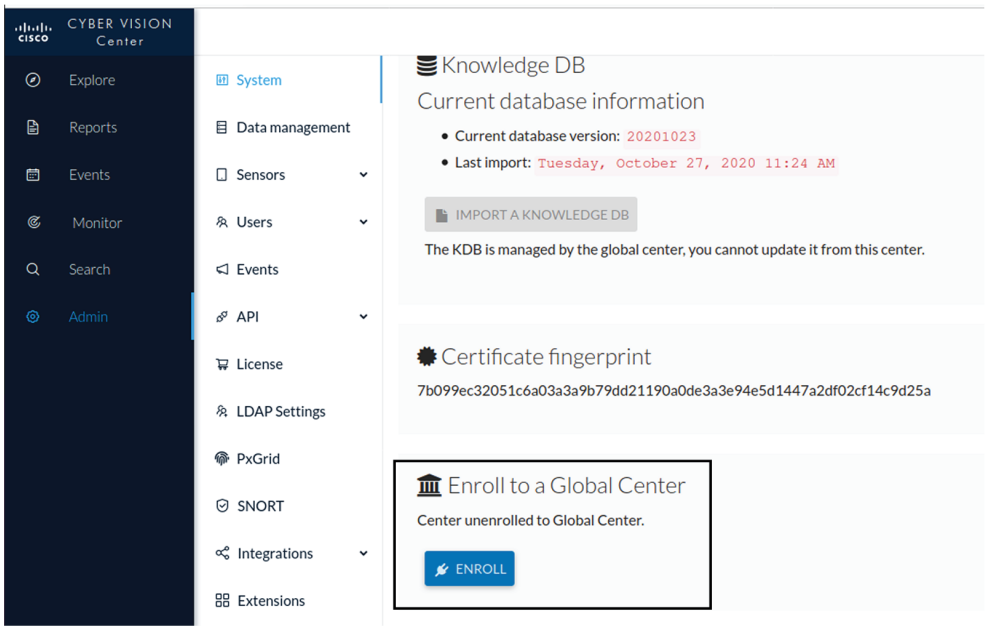
Step 6 Click **OK**.

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.

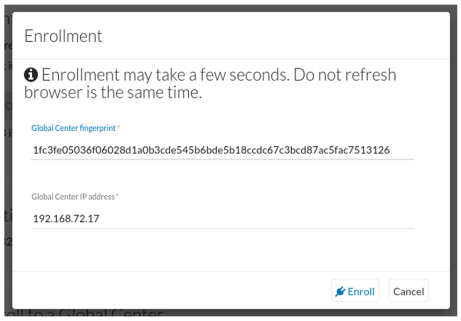
Step 7 In the Center's GUI, scroll down to Enroll a Global Center and click the **Enroll** button.



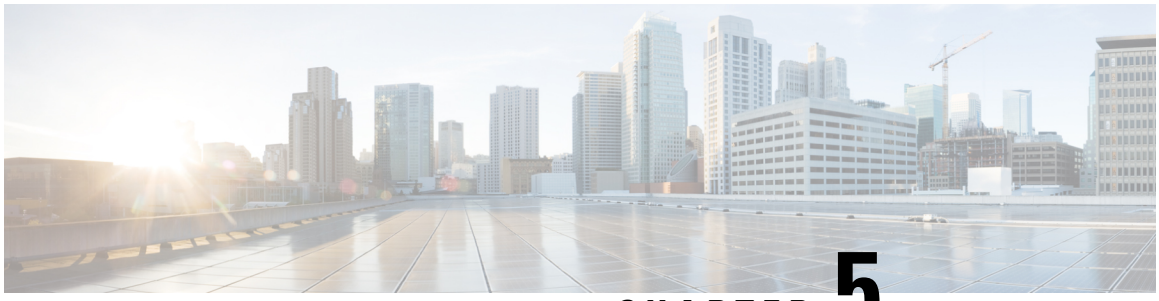
The Enrollment window pops up.

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

• Center DPI, on page 39

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.

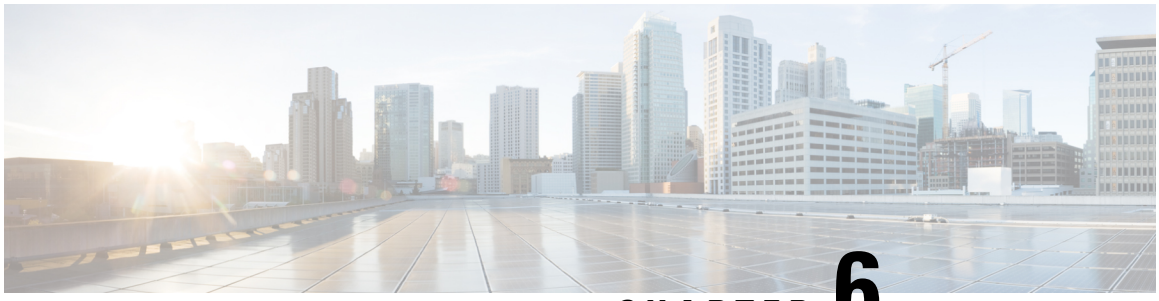
- **None** for SPAN configurations.
- **erspan2** for ERSPAN type 2 remote SPAN.
- **erspan3** for ERSPAN type 3 remote SPAN.

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 the Cisco Cyber Vision Center synchronization

• Global Center Configuration, on page 41

Global Center Configuration

Global Center feature will allow synchronization of several Centers within a single repository. The Global Center will aggregate Centers into a single application and will present a summary of several Center activities.

Once the setup of a Center and a Global Center is done, the Center synchronization could be initialized with a Global Center. This process consist of the enrollment of a Center with a Global Center. When the center is enrolled, it's data with be synchronized incrementally. Later on, if needed, the Center could be unenrolled. The Global Center will then remove all data form that particular Center. The Center will become unenrolled and will be ready for a future enrollment.

Enrollment and unenrollement will be described below.

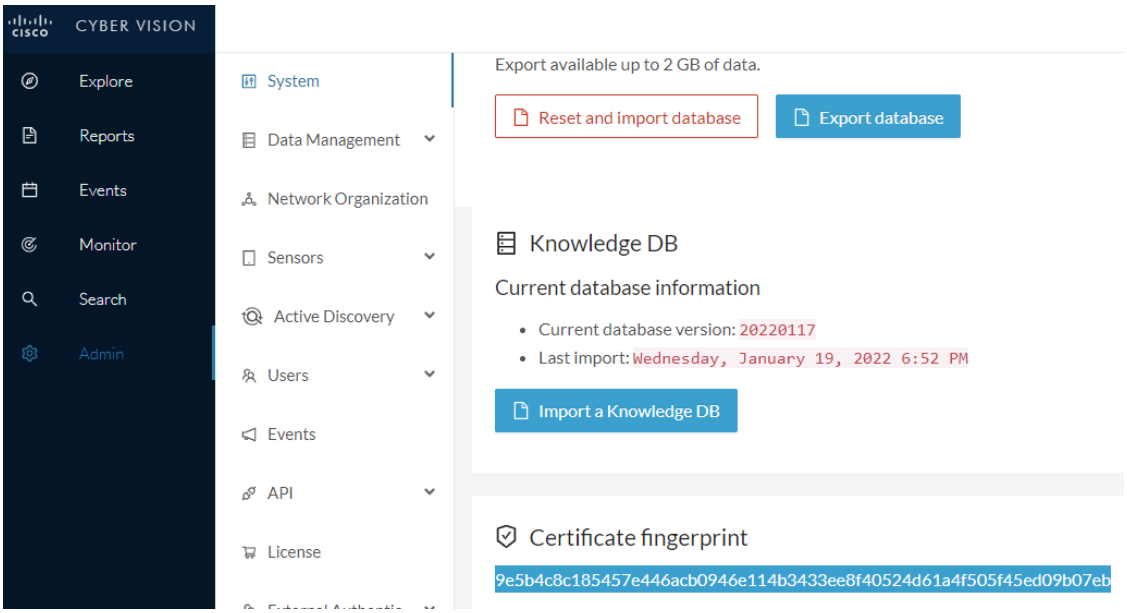
Center enrollment

Before you begin

A Global Center and its Centers need to be reachable in order to be enrolled.

Procedure

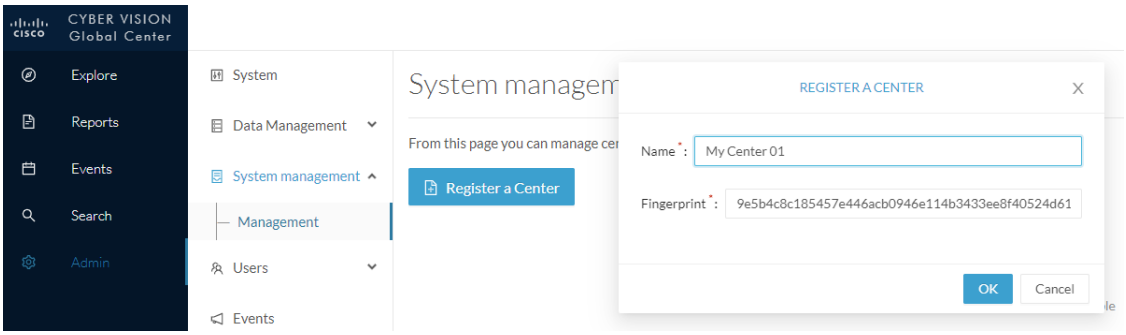
Step 1 Start the process in the Center to be synchronized user interface , navigate to the Admin menu, in the system page, you will find a **Certificate fingerprint**. Copy it, it will be needed.



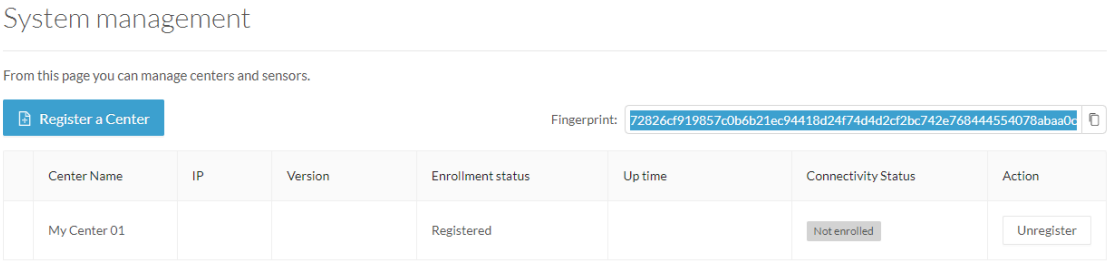
Step 2 Move to the Global Center user interface, Admin menu, in the **System management**, navigate to the **Management** menu. Click on the button **Register a Center** and:

a) Fill the **Name** field with the name you would like to have for this center

b) Paste the **Certificate fingerprint** copied above



Step 3 Stay in the Global Center, on the same menu (Admin - System management - Management) and copy the **Fingerprint** of the Global Center.

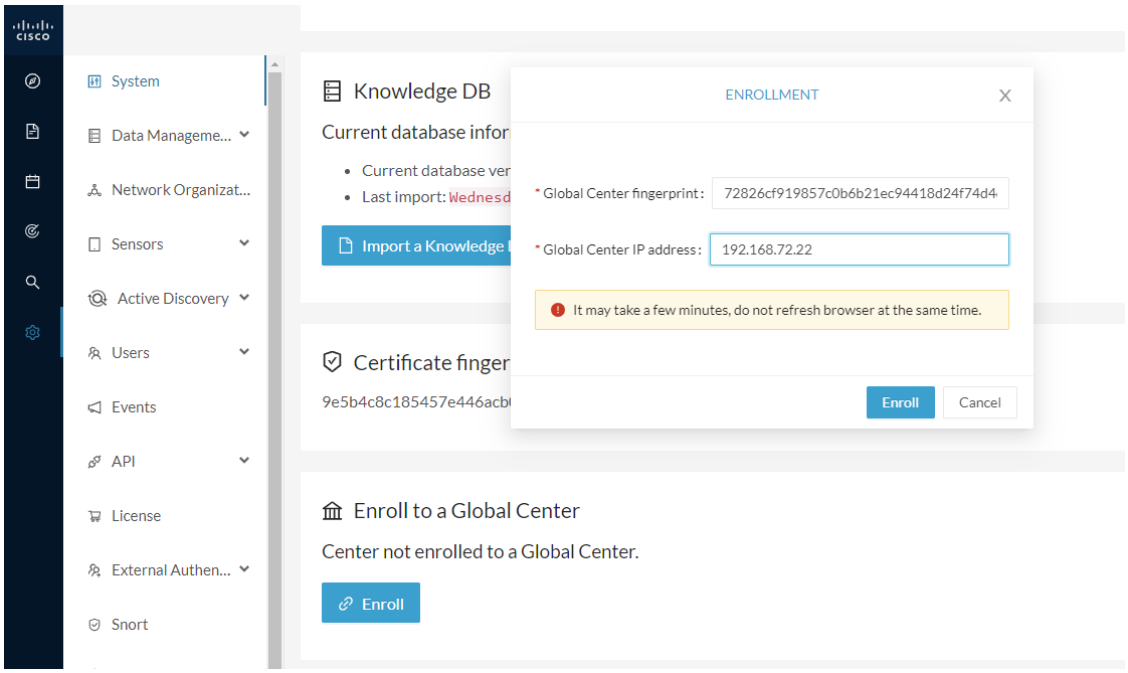


Step 4 On the Center, in the Admin menu, System page, click on the button **Enroll** and:

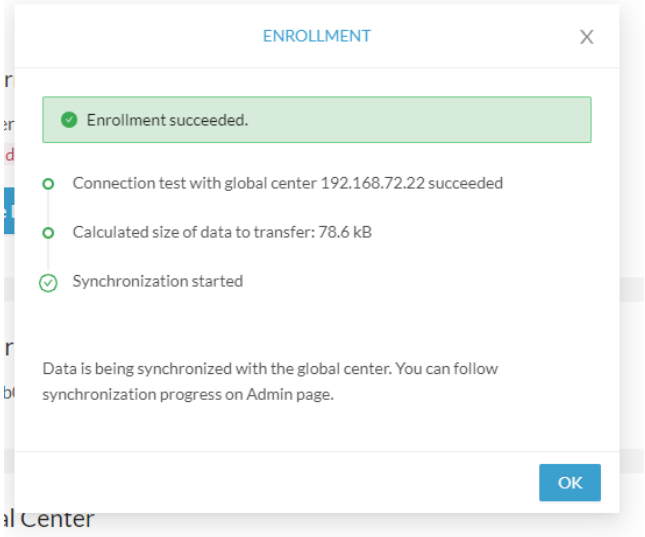
a) add the **Global Center fingerprint** (paste it with the value copied above in the Global Center)

b) add the **Global Center IP address**

c) press on **Enroll**

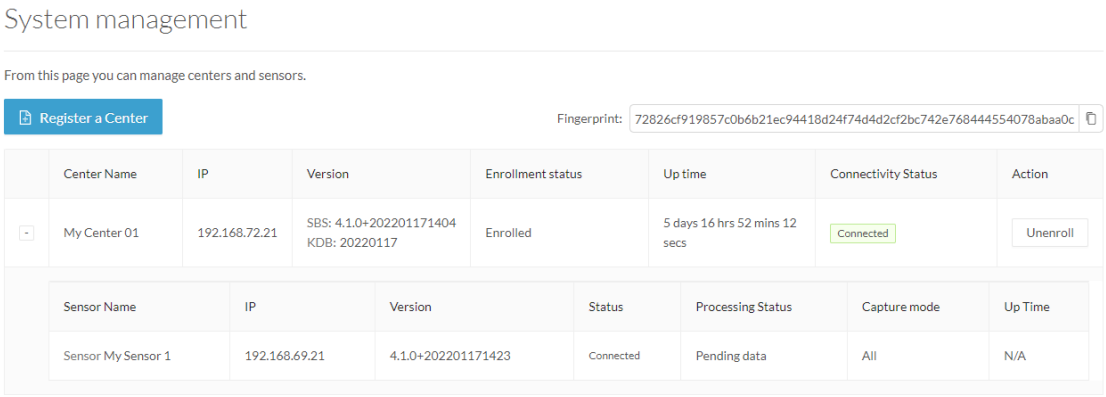


Step 5 The first synchronization will occur. The Center will send all the needed historical information. Once done, a green message is displayed: **Enrollment succeeded**.



What to do next

After the enrollment, the Center is synchronized regularly with the Global Center. In the Global Center, in the Admin menu, the System Management page gives a status of all Centers Synchronized and their Sensors.



Center unenrollment

Before you begin

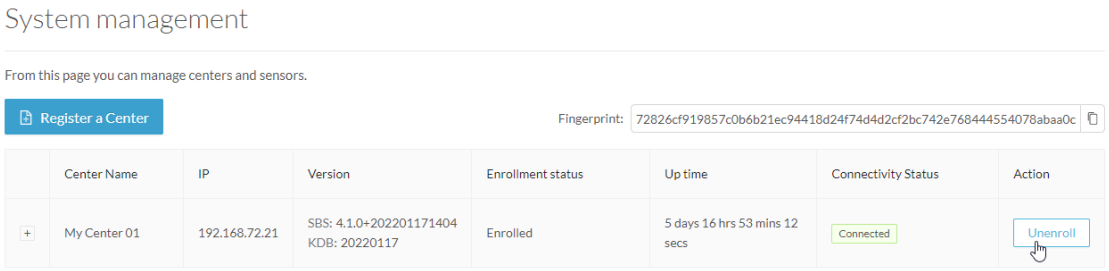
A Center can be unenrolled whenever it is needed, for example as a maintenance operation to replace the Center or the Global Center. This will delete all the Center's data in the Global Center.

Procedure

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

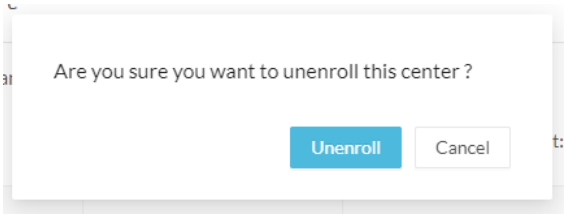
All Centers of the Global Center are listed.

Step 2 Click Unenroll on the Center required.



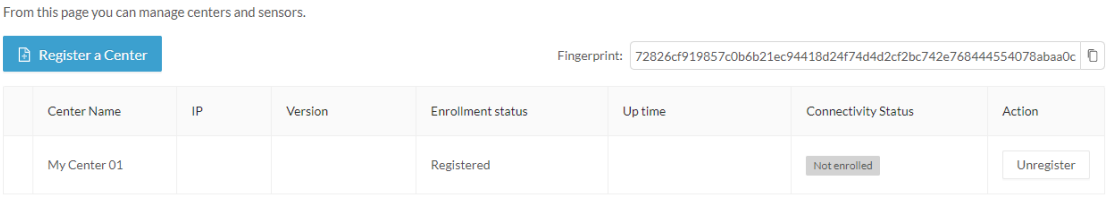
In case of a Global Center replacement, you need to unenroll all its synchronized Centers.

Step 3 A popup asking for confirmation appears. Click **Unenroll** to start the process.



All Center's data are deleted from the Global Center. The Center is then ready to be enrolled again in the Global Center or in another Global Center.

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



Force the unenrollement of a Center

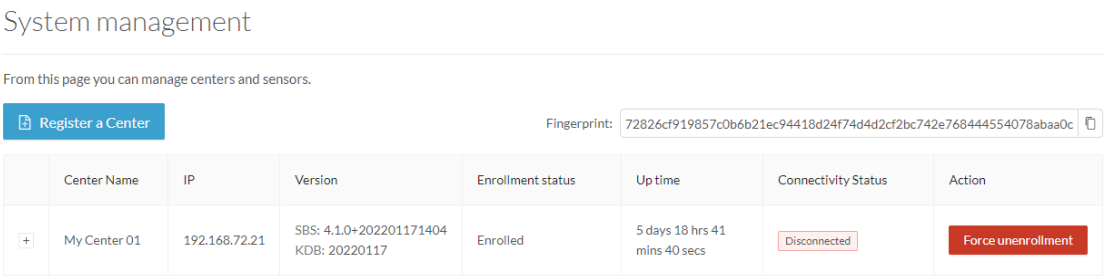
When a Center with sync has been disconnected for a very long time, for example because of a hardware failure, it is possible to unenroll it from the Global Center. This will allow you to delete all Center's data and to replace it.

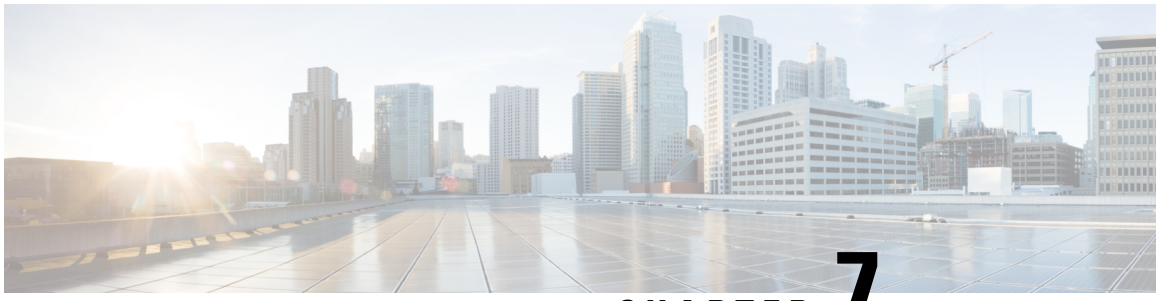


Important Make sure the Center with sync is definitely lost before performing this action. As all the Center's data will be deleted from the Global Center, the Center trying to send data to the Global Center would cause significant data syncronization issues.

In Cisco Cyber Vision, navigate to Admin > System management > Management. All Centers of the Global Center are listed.

Whenever a Center has been disconnected for a long time, the red button **Force unenrollment** appears in the Action column. Use this button to delete all the Center's data from the Global Center. The Center will be removed from the list.





CHAPTER 7

Upgrade procedures

- Architecture with a Global Center, on page 47
- Architecture with a single Center, on page 50

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:

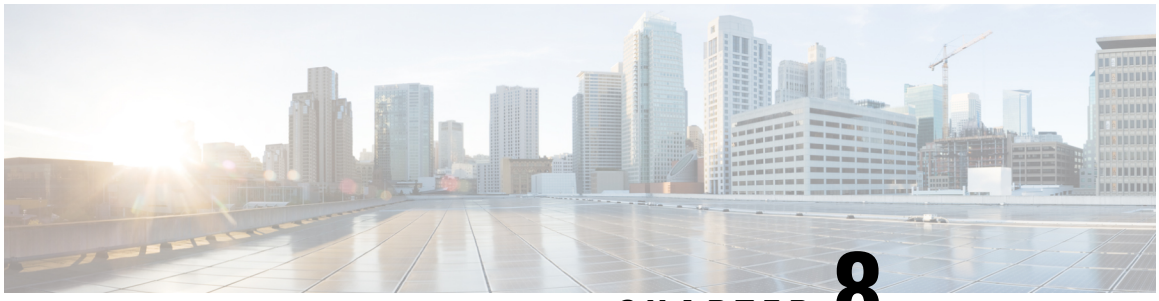
Step 4 Navigate to Admin > Sensors > Sensor Explorer.

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 53

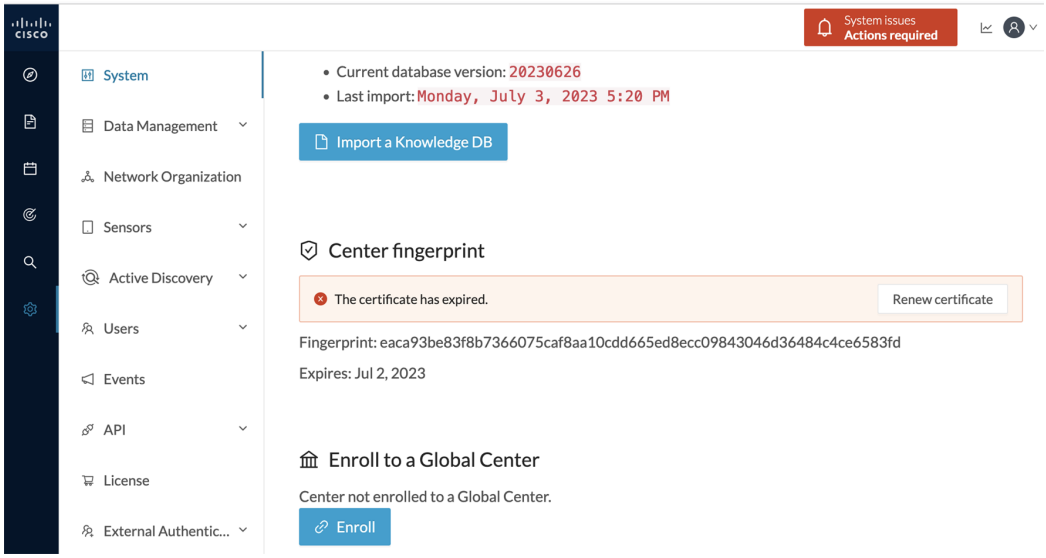
Renew the certificate of a Center

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

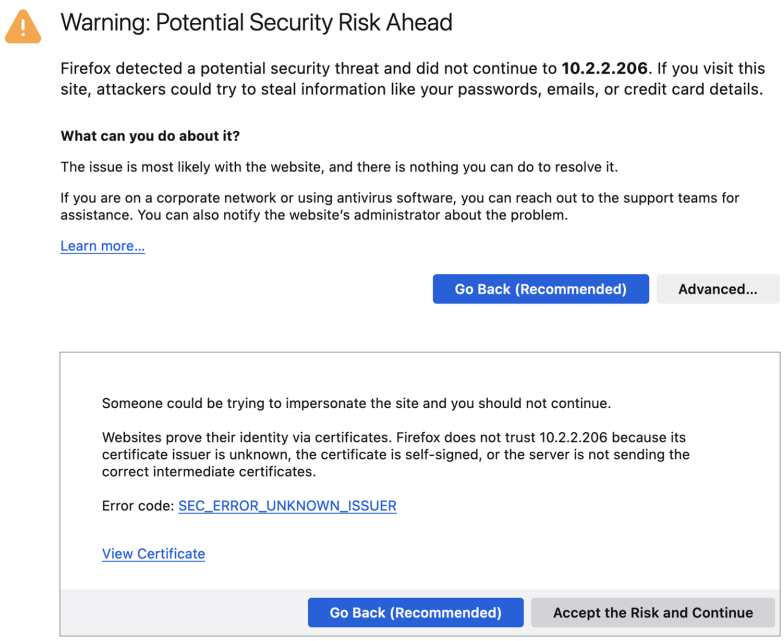
Before you begin

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

Procedure

Step 1 Access the **Global Center**.

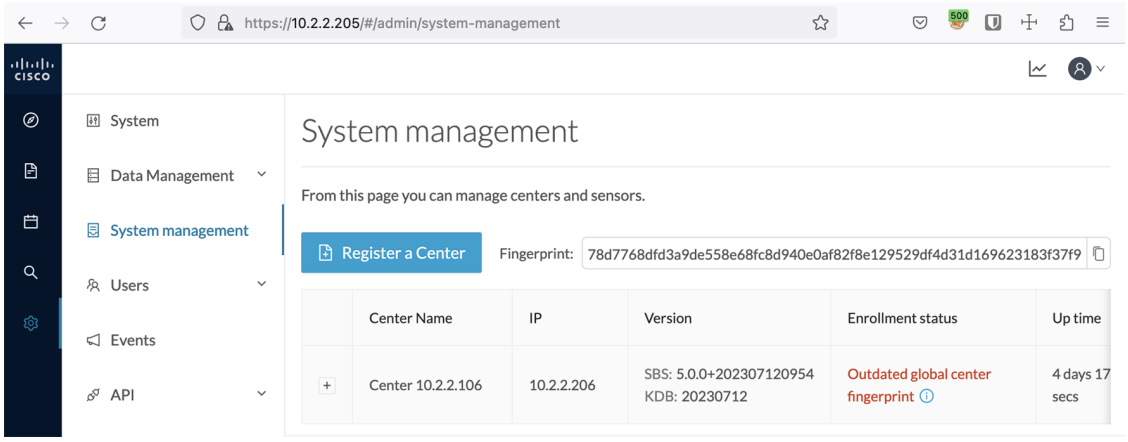
This warning page indicates that the certificate has been renewed.



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

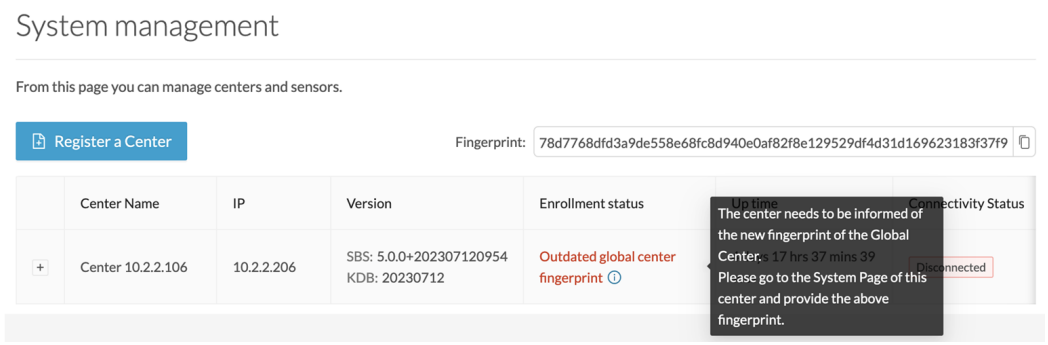
Step 3 Login to the Global Center.

Step 4 Navigate to the System management page.



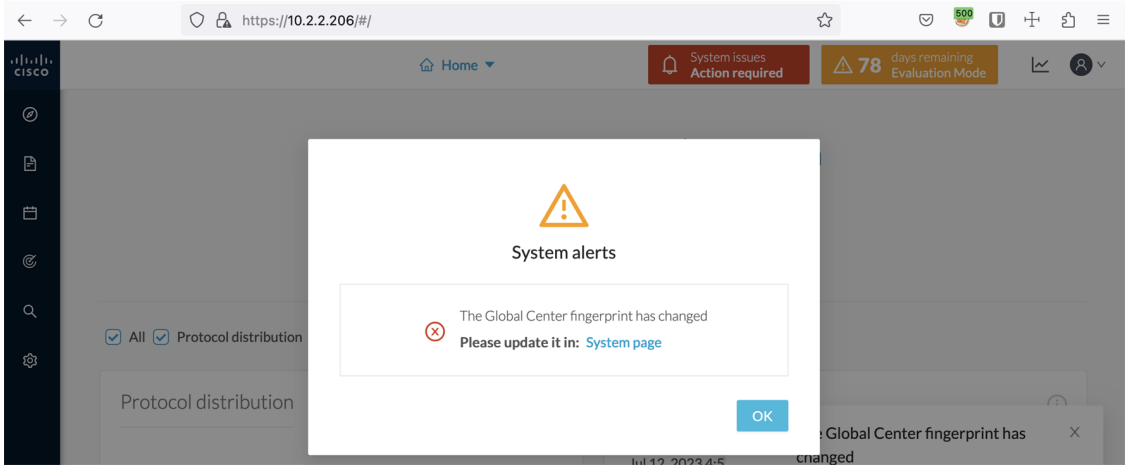
In the Center list, you can see the Center with sync which must be updated with the Global Center's fingerprint.

Step 5 Copy the Global Center fingerprint.



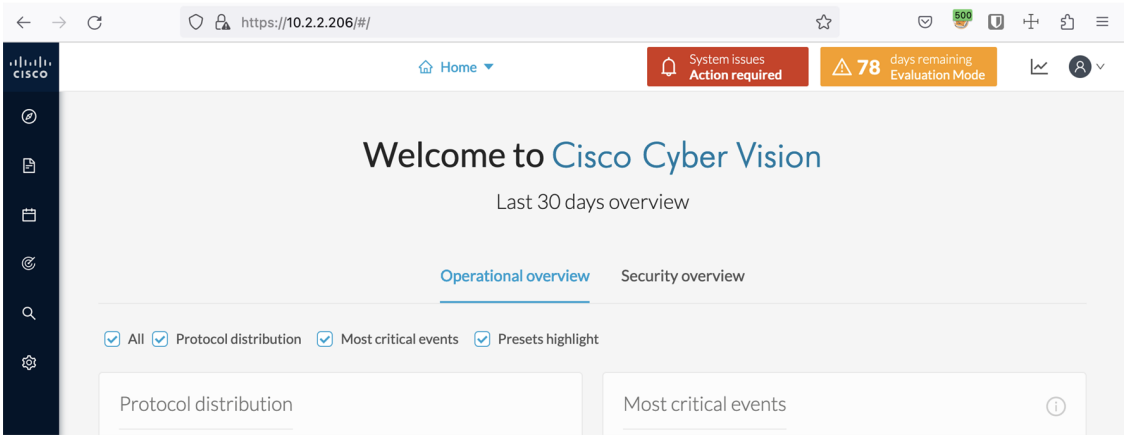
Step 6 Login to the **Center with sync**.

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.

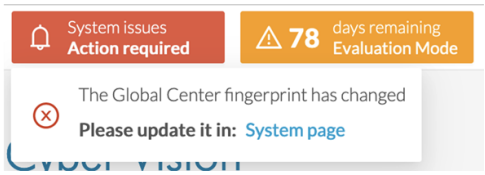


Step 7 Click **OK**.

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



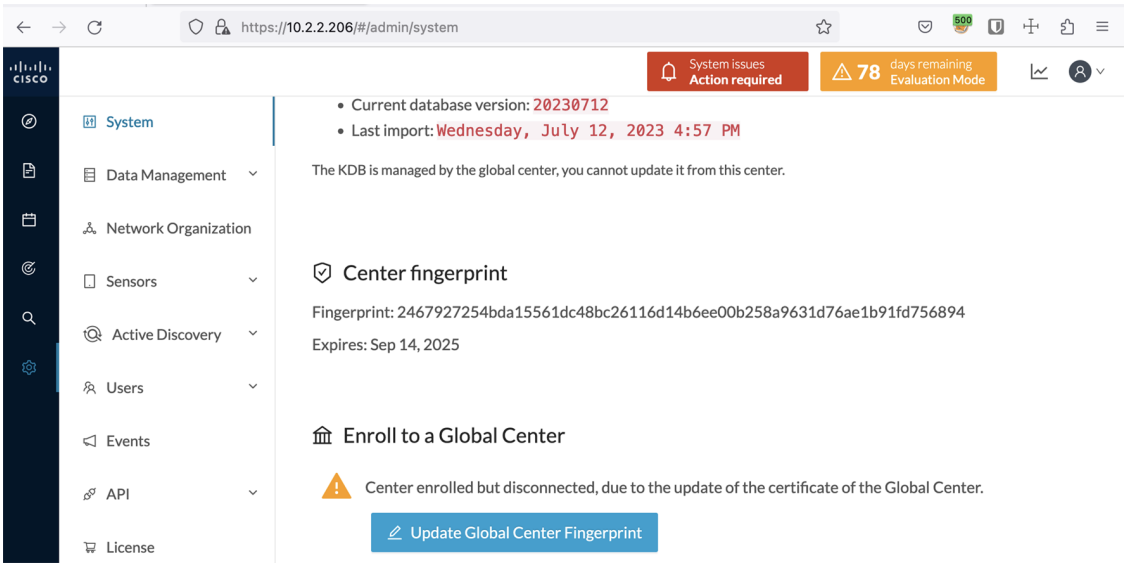
If you click the red banner, you will see the same message that appeared in the previous popup, with a link to the System page to update the Global Center fingerprint.



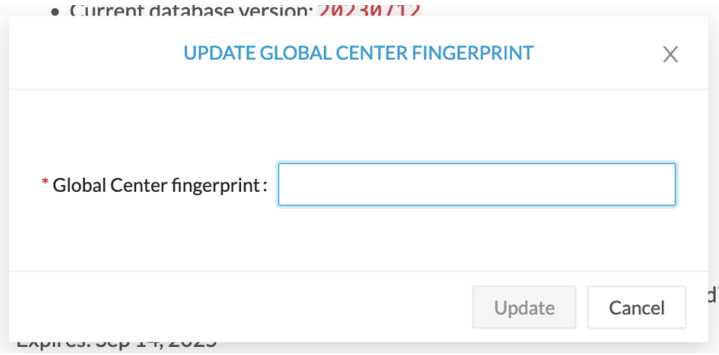
Step 8 In the System page, slide down to Enroll to a Global Center.

It is indicated that the Center is enrolled but disconnected.

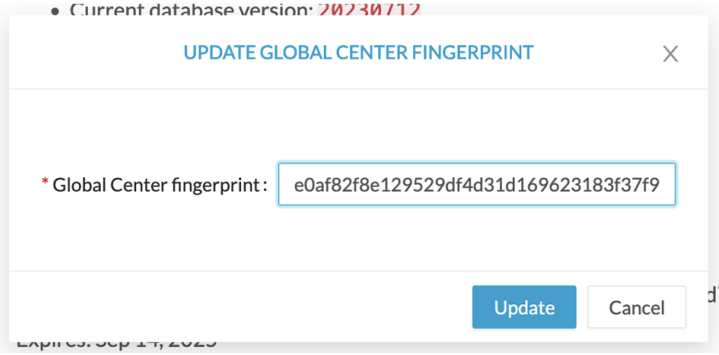
Step 9 Click **Update Global Center Fingerprint**.



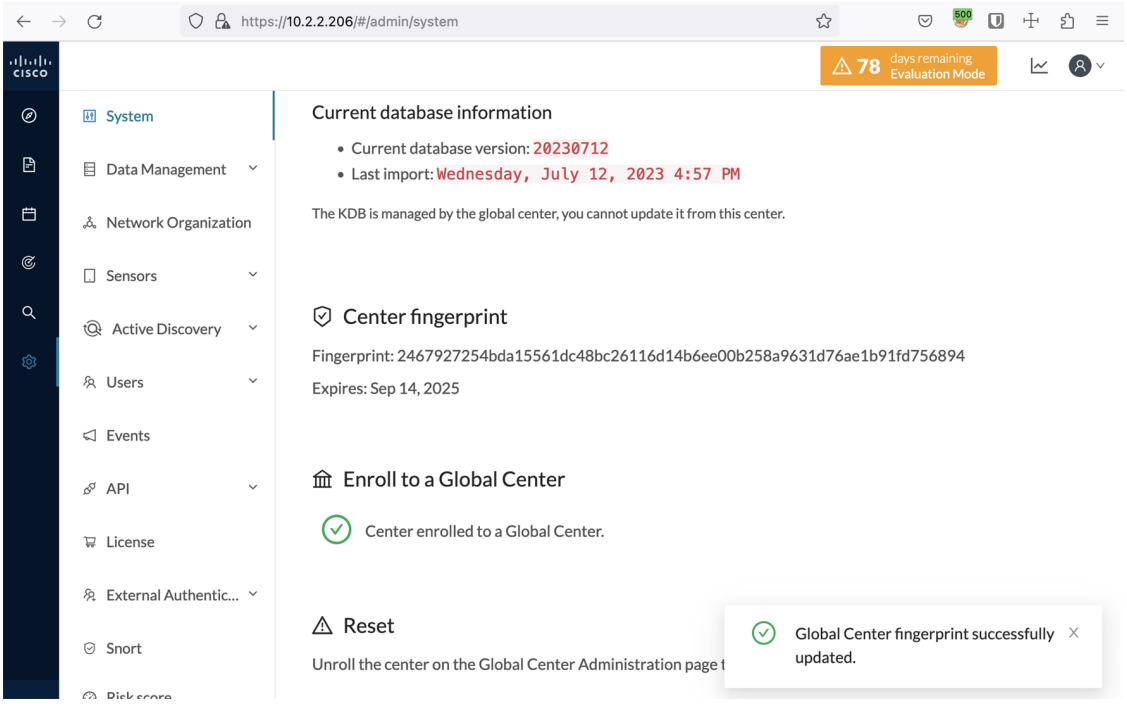
The Update Global Center fingerprint window pops up.



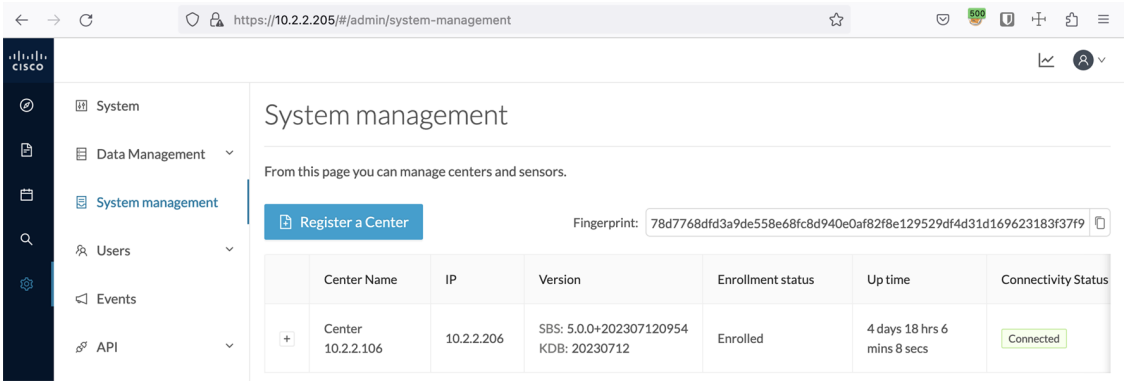
Step 10 Paste the Global Center fingerprint and click **Update**.



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

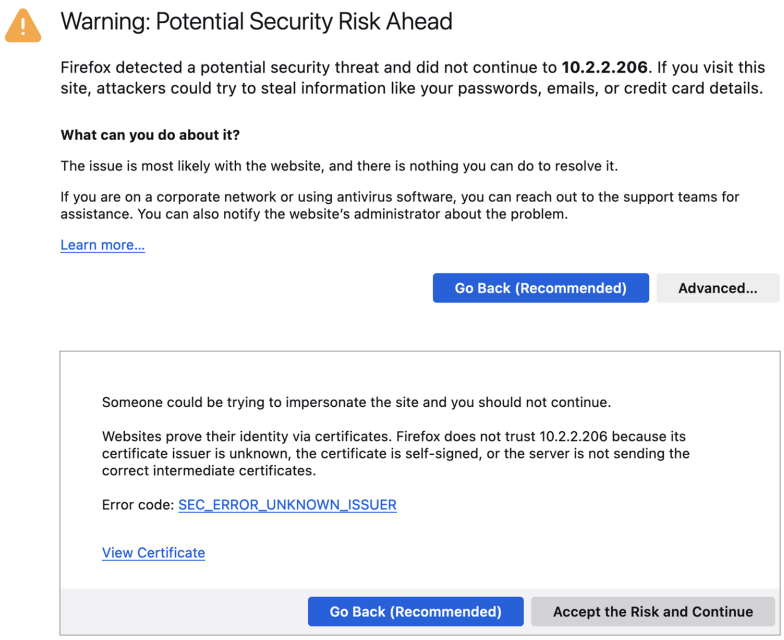
Before you begin

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

Procedure

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

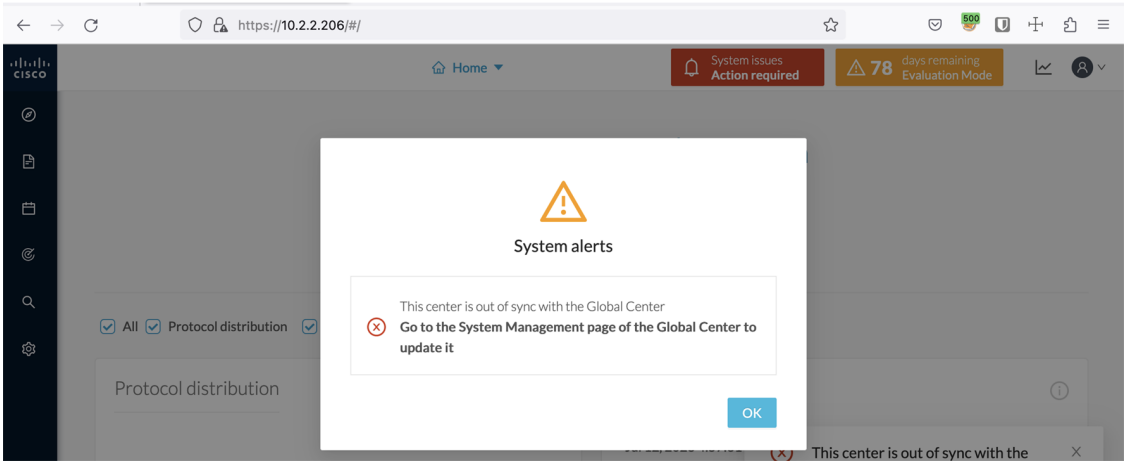
This warning page indicates that the certificate has been renewed.



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

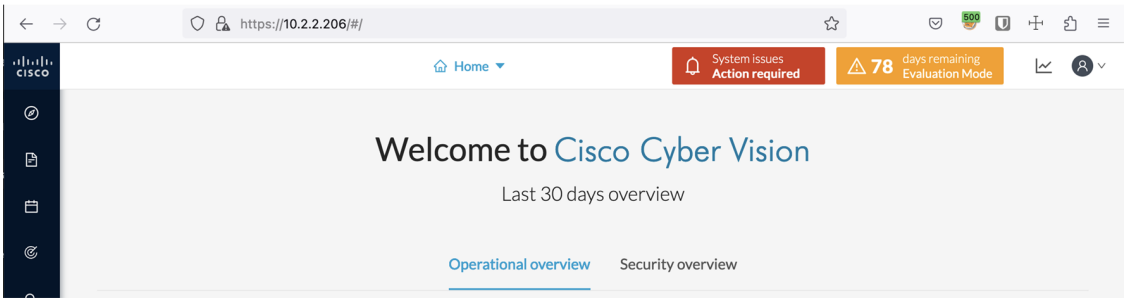
Step 3 Login to the Center.

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

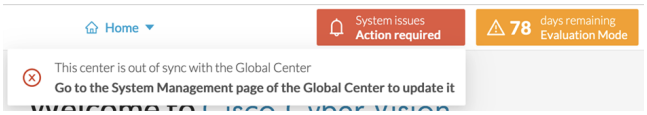


Step 4 Click **OK**.

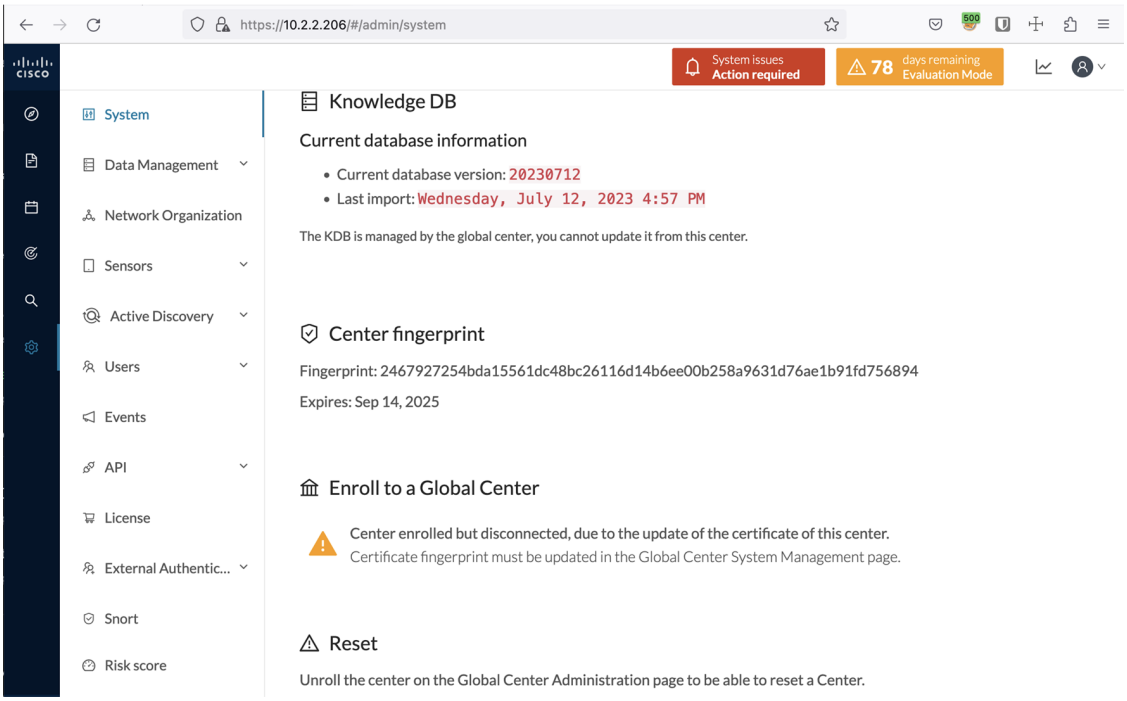
A red banner is displayed at the top of 's user interface.



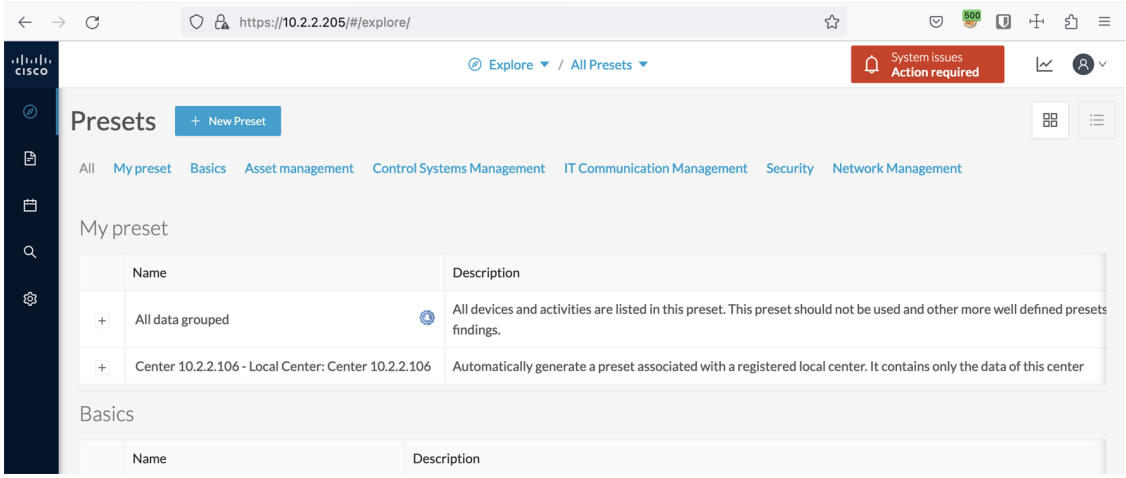
If you click the red banner, you will see the same message that appeared in the previous popup.



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

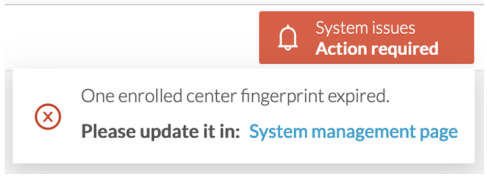


Step 5 Access the **Global Center**.

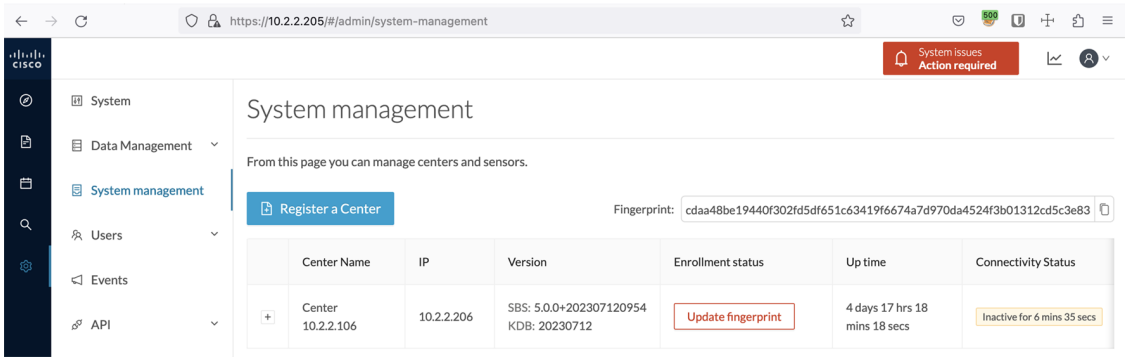


Step 6 Click the red banner.

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

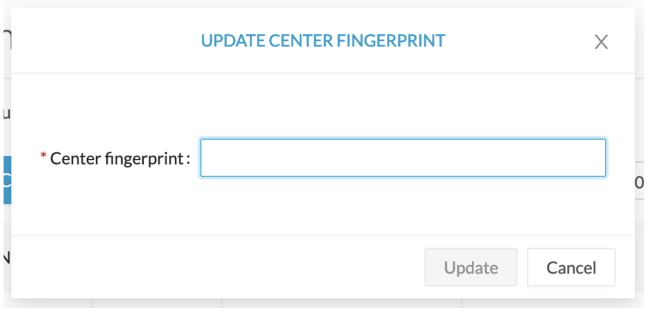


In the System management page you can see the Center with its enrollment status as Update fingerprint and Connectivity status as Inactive.

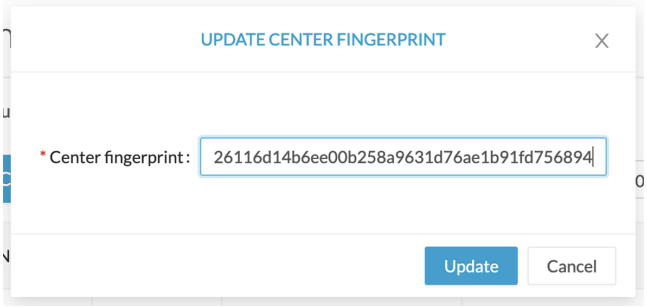


Step 7 Click the **Update fingerprint** status button.

An Update Center fingerprint window pops up.

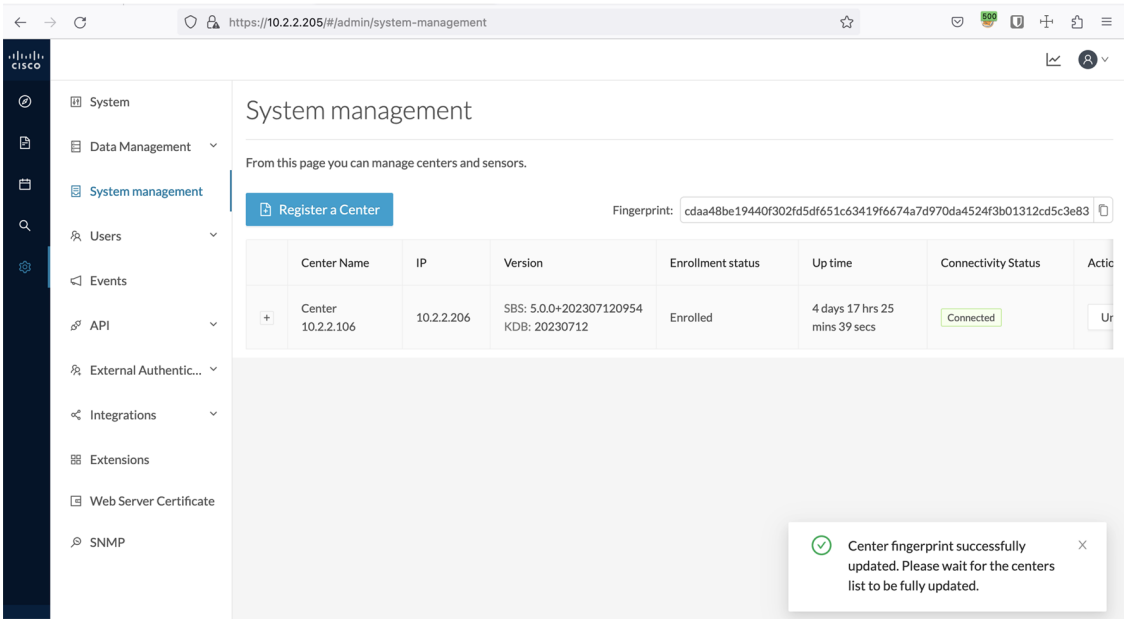


Step 8 Paste the Center fingerprint.

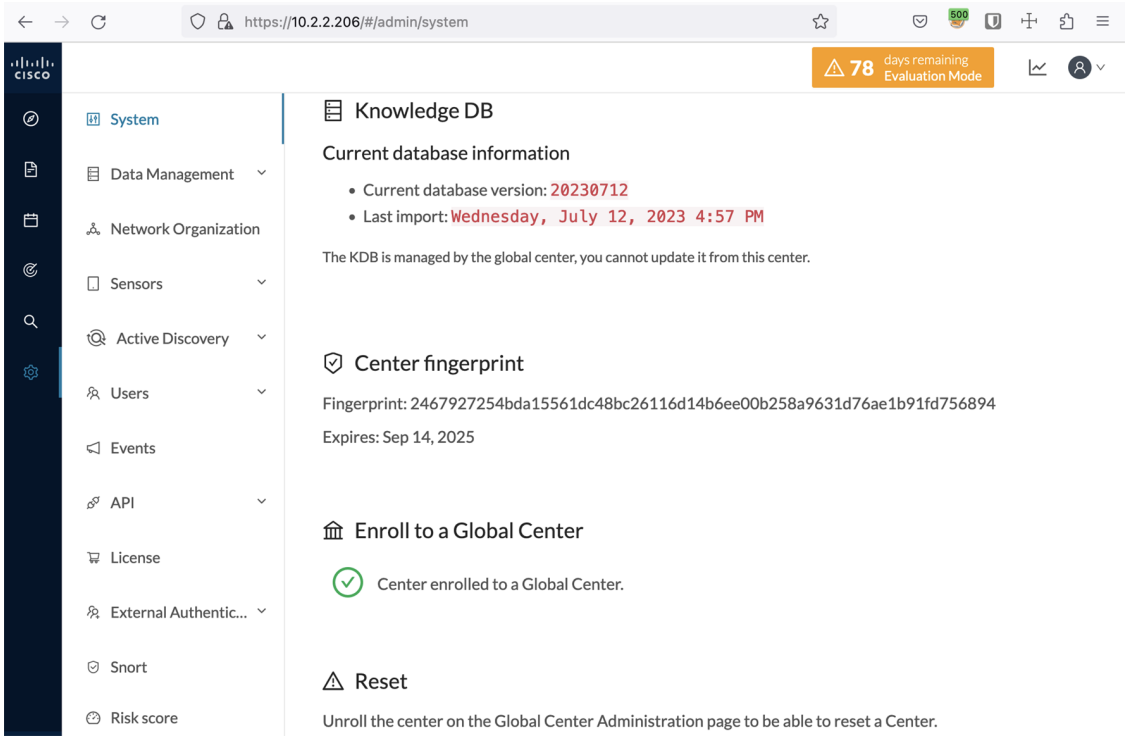


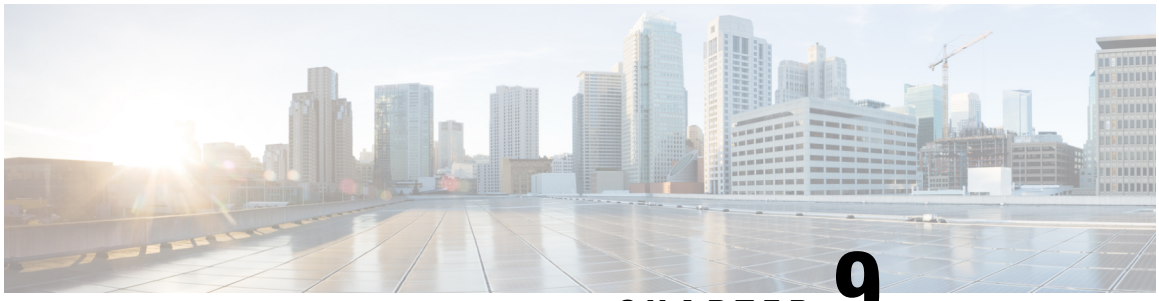
A message indicating that the Center fingerprint successfully updated appears.

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

A new Command Line Interface (CLI) command is available to back up and restore a center. It will help the user to migrate a center from one appliance to another. For example, migrating a center from a virtual machine to a UCS appliance. The feature is designed to backup all settings and data, including:

- Operating system settings (such as IP addresses, names, certificates, etc.)
- Cyber Vision Settings
- Cyber Vision Data

After restoration, the new center will function on the network just like the old center.

- Backup and Restore Constraints, on page 65
- Backup Cyber Vision Center, on page 66
- Restore Cyber Vision Center, on page 66
- Automate the Backup of the Cyber Vision Center, on page 67
- Bash Script, on page 68
- Cron, on page 68

Backup and Restore Constraints

list of the constraints:

- The new appliance requires an equal number of network interfaces as the center backed up.
- Set up the new appliance with Cyber Vision configuration. (Achieve the center setup, at least for the eth0 IP address, which needs to be configured to transfer the center archive.
- The new center interface configuration (single or dual) needs to match the backed-up center.
- As the new center adopts all old center settings like the IP address, the old appliance needs to be powered off.
- The Cyber Vision License cannot be copied.
  1. Return the license to the smart account server.
  2. After restoring, the new center needs to be licensed.
- Install the report extension on the restored center.

1. Report configuration and old report versions are copied.

Backup Cyber Vision Center

Procedure

Step 1 Connect to the center in SSH.

Step 2 Type the following command:

```
sbs-backup export
```

A file will be generated in the folder: `'/data/tmp/ccv-center-backup'`

```
root@Center224433:~# sbs-backup export
Please note that license information is also backed up and will be restored if you restore the backup on the same system from whi
ch the backup was taken.
If you restore the backup on a different system, first return the license reservation to Cisco Smart Software Licensing so you ca
n set it up again after the restoration on the new system.
***************** Taking backup of file system     *****************
***************** Taking backup of database        *****************
***************** Taking backup of RMQ definitions *****************
***************** Taking backup of center version  *****************
***************** Taking backup of symlinks        *****************
***************** Taking backup of extension       *****************
Created center archive at /data/tmp/ccv-center-backup/ccv-center-backup-Center224433labautomccvlocal-4.4.0-20240405112443.tar.gz
```

In the above given example, the created file is called::

```
ccv-center-backup-Center224433labautomccvlocal-4.4.0-20240405112443.tar.gz
```

Step 3 Copy the file to the new appliance for the restore.

Restore Cyber Vision Center

Copy the center backup file to the new center's **/data/tmp/ folder**.

Procedure

Step 1 Connect to the center in SSH.

Step 2 Type the following command:

```
sudo -i
```

```
sbs-backup import path-to center-backup
```

```
root@Center224433:~# sbs-backup import /data/tmp/ccv-center-backup/ccv-center-backup-Center224433labautomccvlocal-4.4.
0-20240405112443.tar.gz
********** Restoring file system     **********
********** Restoring database        **********
********** Restoring RMQ definitions **********
********** Restoring symlinks        **********
********** Restoring extension       **********
Restore completed, please reboot to finalise the system configuration. After reboot, please install the Reports extens
ion compatible with the center version.
root@Center224433:~#
```

Step 3 Type reboot to restart the sensor.

Step 4 Install the report management extension if necessary.

Step 5 Install a license on your center.

Automate the Backup of the Cyber Vision Center

Many tools are available to automate the Cyber Vision center backup.

rclone: It is a command line program to manage files. You can use it to synchronize your center backup with a remote drive.

Procedure

Step 1 To handle the complex authentication of object storage systems, rclone requires configuration due to the information being stored in a config file. The simplest way to create this config is by running rclone with the config option:

```
sudo -i
```

```
rclone config
```

Various options are available, as mentioned here: https://rclone.org/docs/

Example of config file:

```
root@Center224433:~# rclone config show
[lab_sftp]
type = sftp
host = 10.2.3.172
user = user
pass = ZcQlawWIsn3NprBf0mFEb4cwElMYHXcJ-2k
md5sum_command = md5sum
sha1sum_command = sha1sum

root@Center224433:~#
```

Step 2 Rclone syncs a directory tree between storage systems. Here's the syntax:

```
Syntax: [options] subcommand <parameters> <parameters...>:
```

For example:

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

With the example above, rclone will move the backup file stored in '`/data/tmp/ccv-center-backup/`' to the `remote drive 'lab_sftp'`.

Bash Script

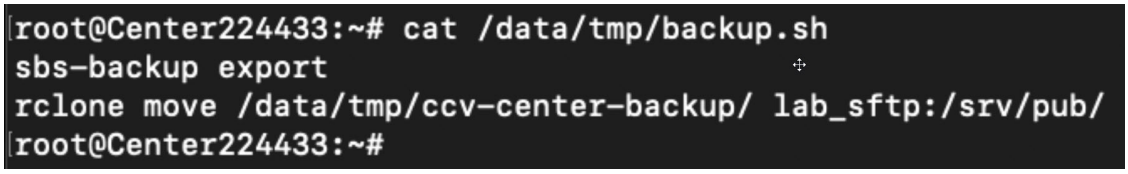
You can use bash script to execute the two necessary commands mentioned below:

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

For example:

```
sbs-backup export

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



Cron

You can schedule a bash script using cron to back up Cyber Vision data and send the backup file to a remote drive.

Usages are as follows:

1. Edit crontab launching the command:
   - `crontab -e`

     : It allows you to edit the crontab file using the vi editor, enabling you to make modifications.
2. Add the command mentioned bellow::
   - `00 01 * * 6 bash /data/tmp/backup.sh`

```
# ┌──────────── minute (0 - 59)
# │ ┌──────────── hour (0 - 23)
# │ │ ┌──────────── day of the month (1 - 31)
# │ │ │ ┌──────────── month (1 - 12)
# │ │ │ │ ┌──────────── day of the week (0 - 6) (Sunday to Saturday;
# │ │ │ │ │                                     7 is also Sunday on some systems)
# │ │ │ │ │
# │ │ │ │ │
# * * * * * <command to execute>
```