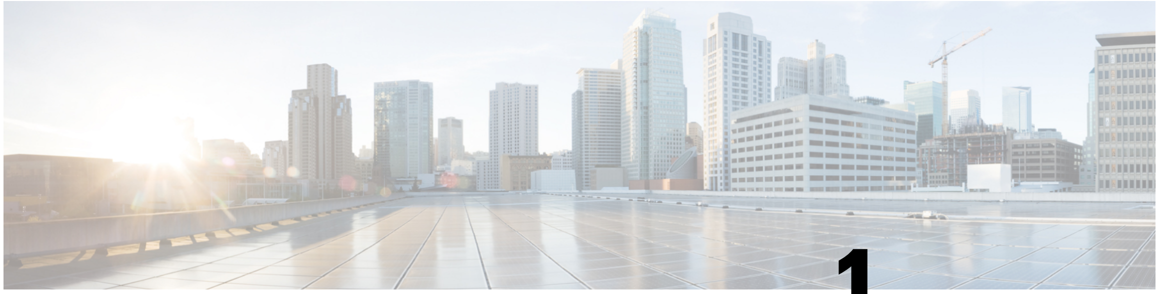
Cisco Cyber Vision Center Appliance Installation Guide, Release 5.4.x

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

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 5.4.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

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.

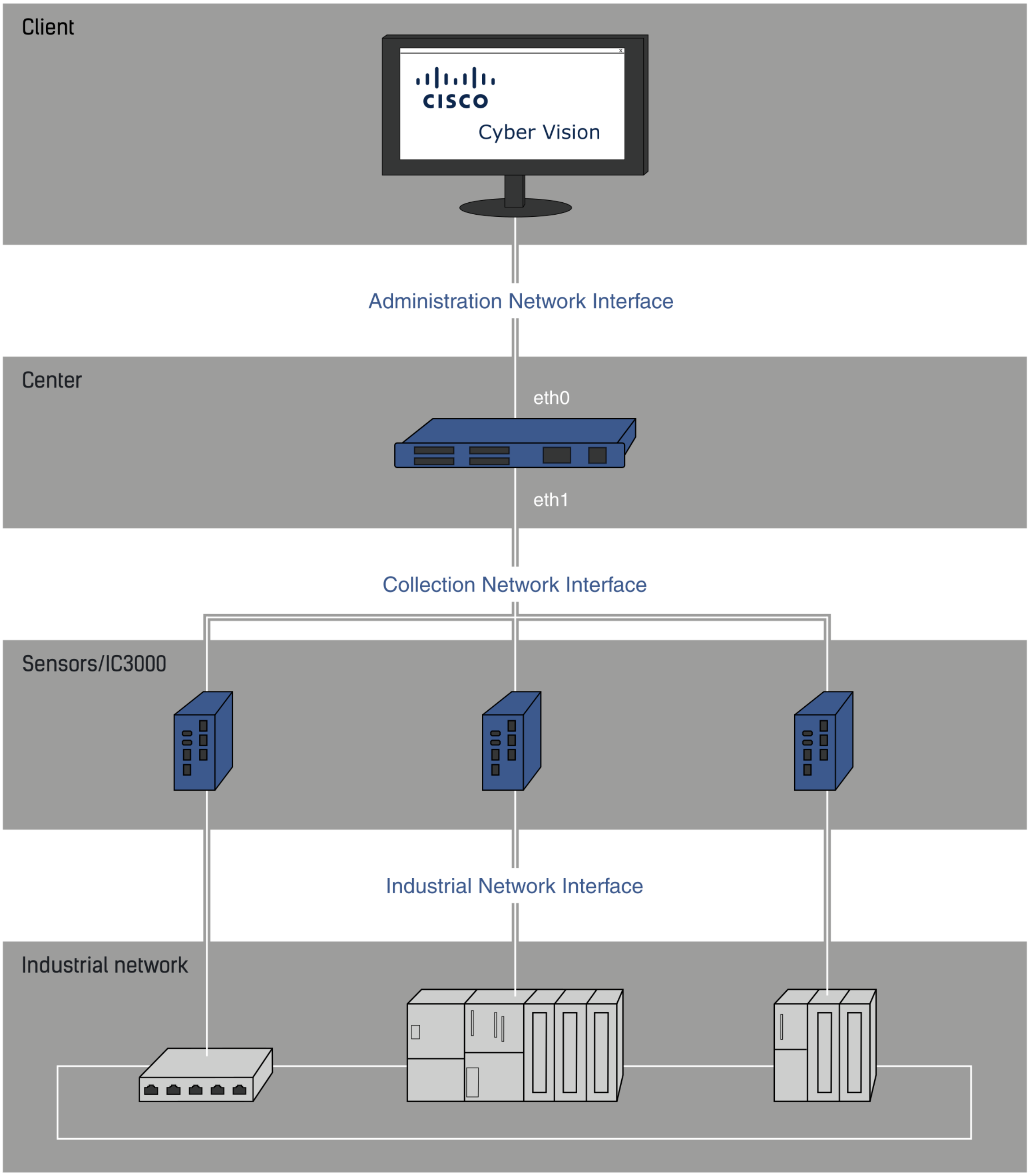
During the installation of the Center, you will have the opportunity to set up Center data synchronization to a Global Center. Although, if you choose to set up a global infrastructure, you must install the Global Center first, then the Centers, and finally, the sensors.

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).

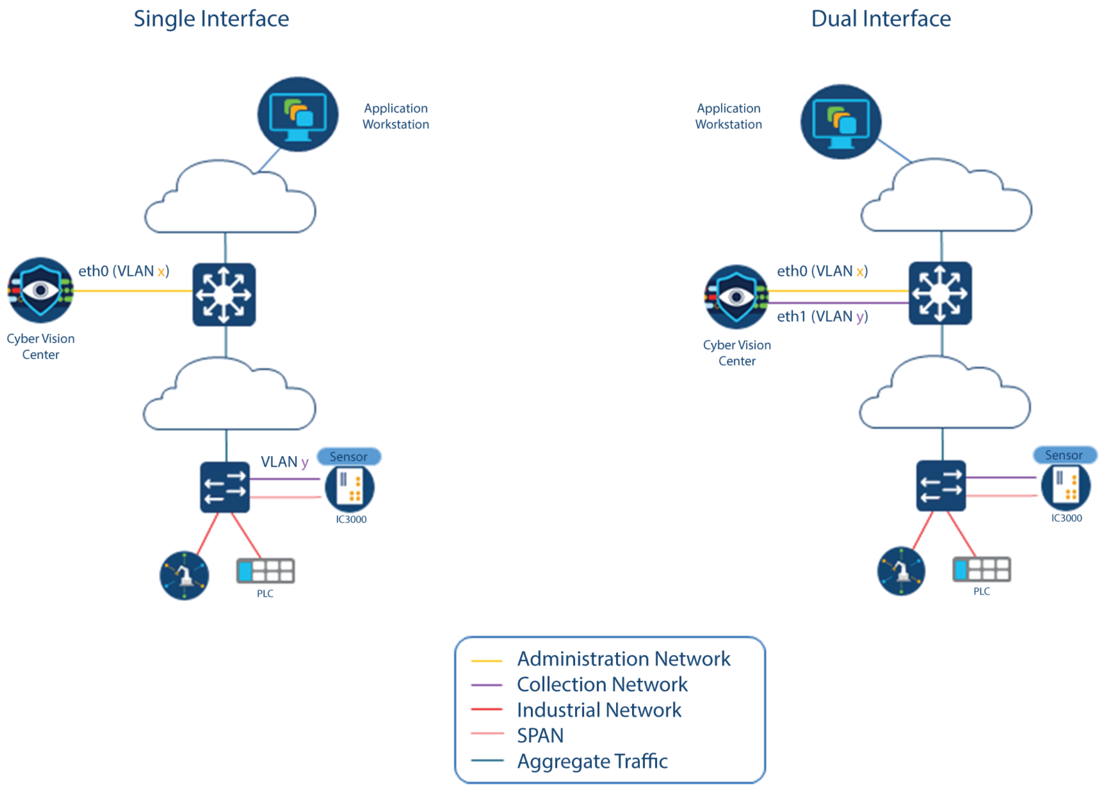
Example of a installation (without Global Center):


Client
cisco
Cyber Vision
Administration Network Interface
Center
eth0
eth1
Collection Network Interface
Sensors/IC3000
Industrial Network Interface
Industrial network

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 administration services in Cyber Vision.

You can use IPv6 on center eth0 for all your administration-related access, such as:

- Accessing the web UI.
- Integrating with third-party solutions such as syslog, ISE configurations, and LDAP.

Consider these limitations:

- License operations only work 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

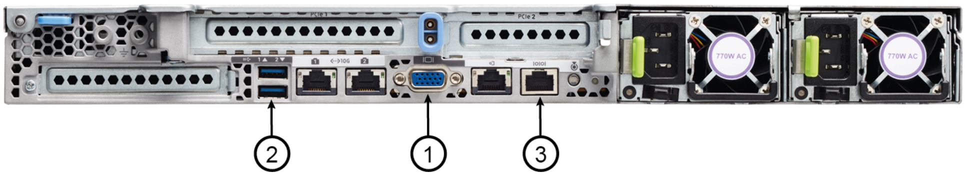
Before turning on the Center for the first time, you will need to connect the Center to a VGA display and a keyboard or a console so you can configure it, and to network interfaces to make it operational.

Connect an external device

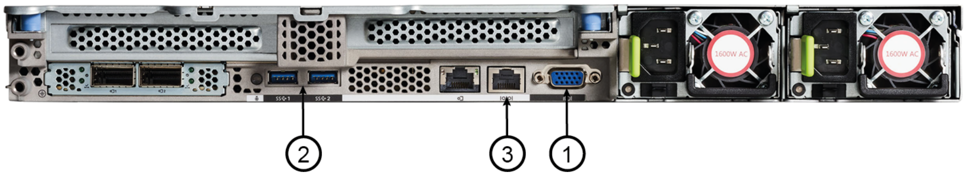
You need to connect an external device to access and configure the Center.

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:

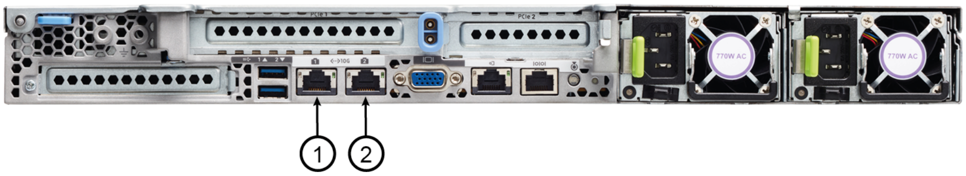


Cisco Unified Computing C225 M6:

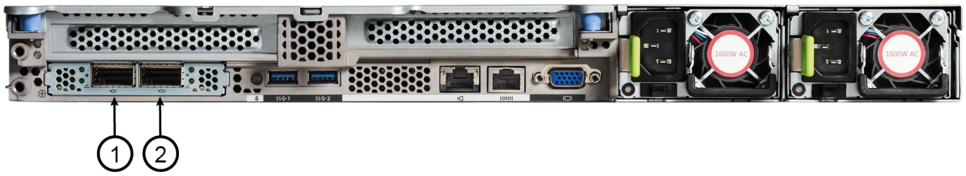


Connect interfaces for communication

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

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

Required information:

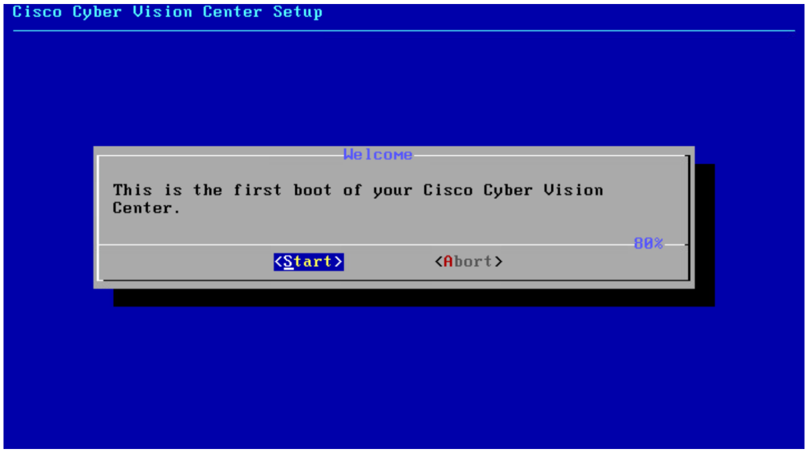
- Local NTP and DNS IP addresses.
- The Collection interface network address (n/a for a Global Center or a Center using a single interface).

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).

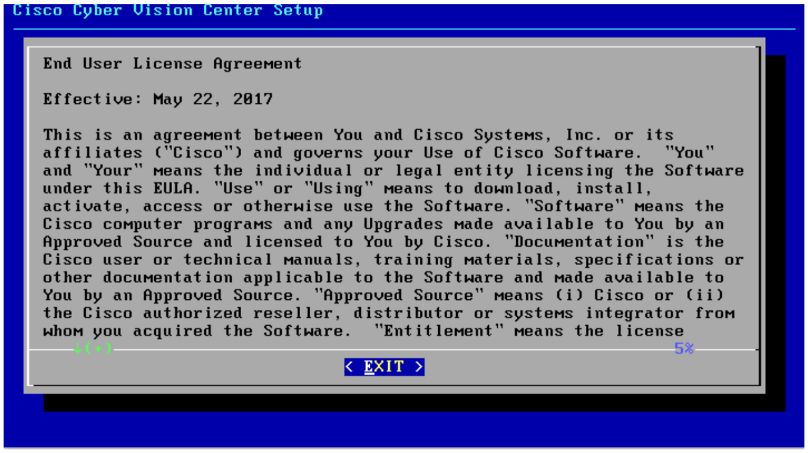
Access the basic Center configuration

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

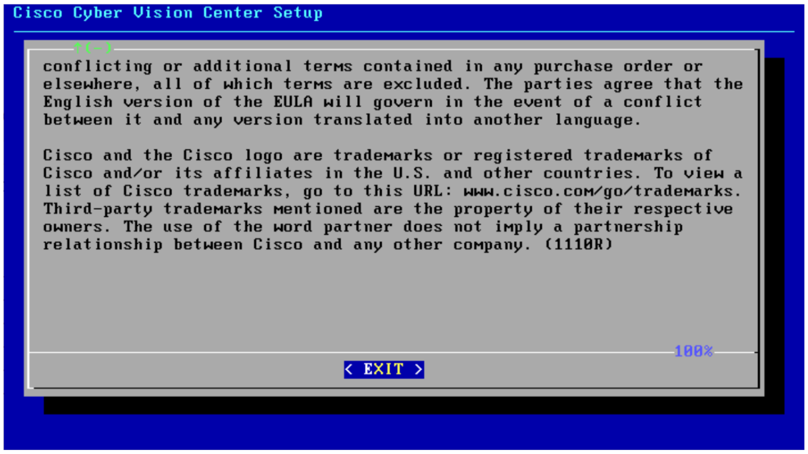


```
Cisco Cyber Vision Center Setup

Welcome

This is the first boot of your Cisco Cyber Vision
Center.
```

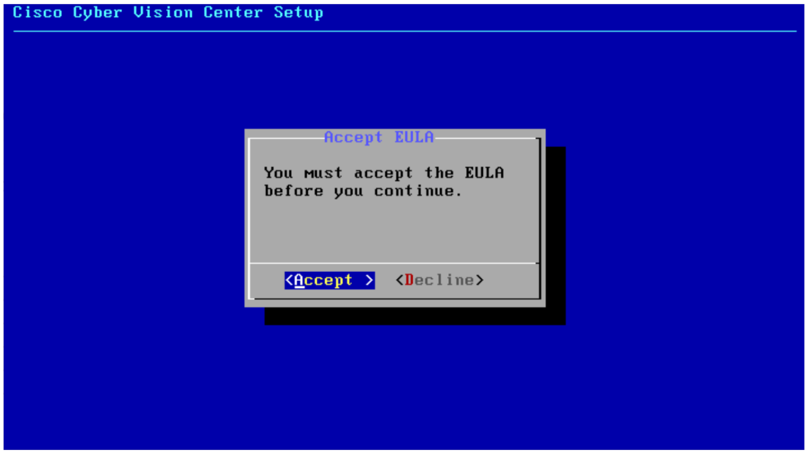
Accept the End User License Agreement



```
Cisco Cyber Vision Center Setup

End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its
affiliates ("Cisco") and governs your Use of Cisco Software.  "You"
and "Your" means the individual or legal entity licensing the Software
under this EULA. "Use" or "Using" means to download, install,
activate, access or otherwise use the Software. "Software" means the
Cisco computer programs and any Upgrades made available to You by an
Approved Source and licensed to You by Cisco. "Documentation" is the
Cisco user or technical manuals, training materials, specifications or
other documentation applicable to the Software and made available to
You by an Approved Source. "Approved Source" means (i) Cisco or (ii)
the Cisco authorized reseller, distributor or systems integrator from
whom you acquired the Software.  "Entitlement" means the license
```



```
Cisco Cyber Vision Center Setup

conflicting or additional terms contained in any purchase order or
elsewhere, all of which terms are excluded. The parties agree that the
English version of the EULA will govern in the event of a conflict
between it and any version translated into another language.

Cisco and the Cisco logo are trademarks or registered trademarks of
Cisco and/or its affiliates in the U.S. and other countries. To view a
list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.
Third-party trademarks mentioned are the property of their respective
owners. The use of the word partner does not imply a partnership
relationship between Cisco and any other company. (1110R)
```



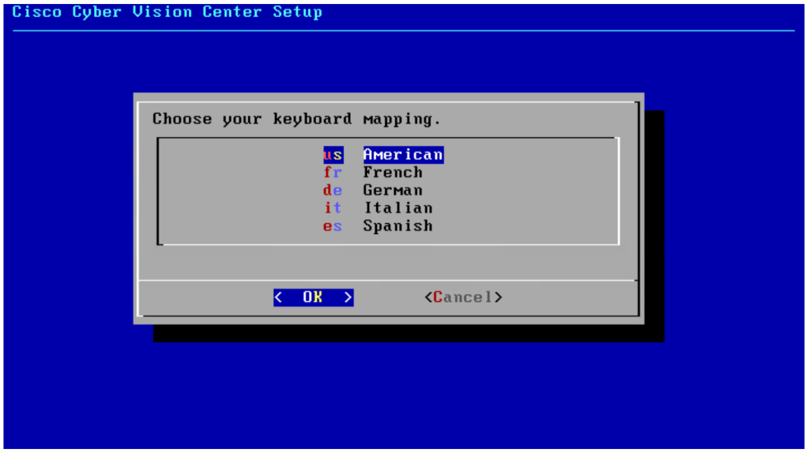
Cisco Cyber Vision Center Setup

Accept EULA

You must accept the EULA before you continue.

Select the language to match your keyboard

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



Cisco Cyber Vision Center Setup

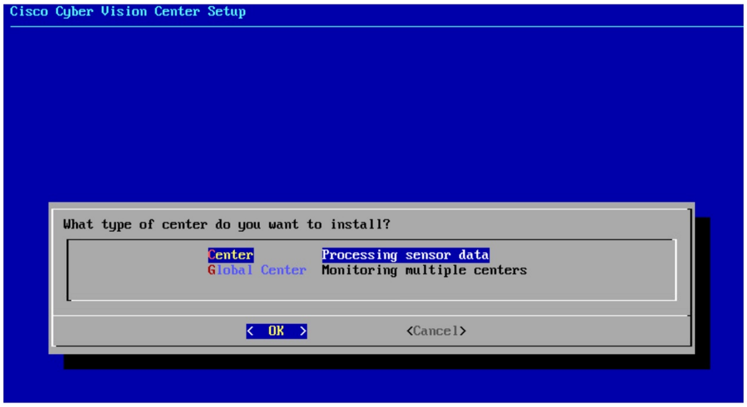
Choose your keyboard mapping.

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.

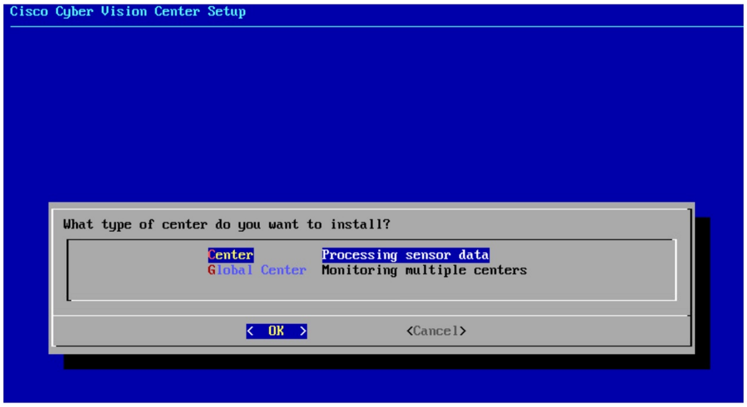
Select the type of Center you want to install.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

              Center         Processing sensor data
              Global Center  Monitoring multiple centers
```

Center

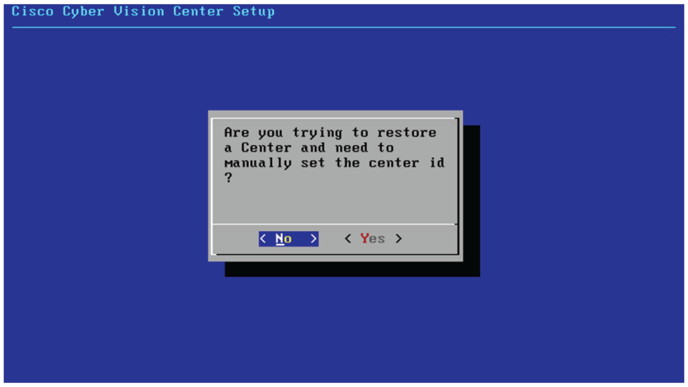
If installing a Center, select the first option.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

              Center         Processing sensor data
              Global Center  Monitoring multiple centers
```

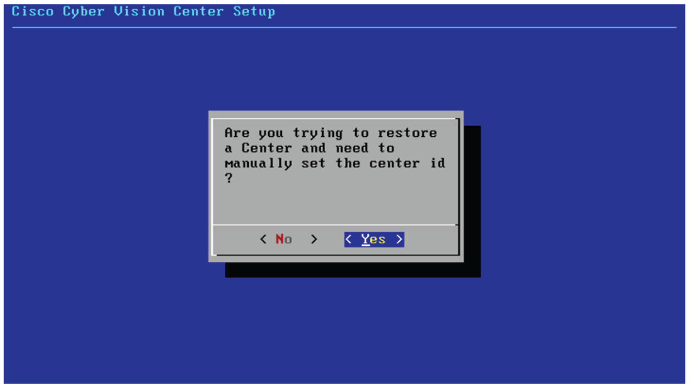
Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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.



```
Cisco Cyber Vision Center Setup

Are you trying to restore
a Center and need to
manually set the center id
?
```

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

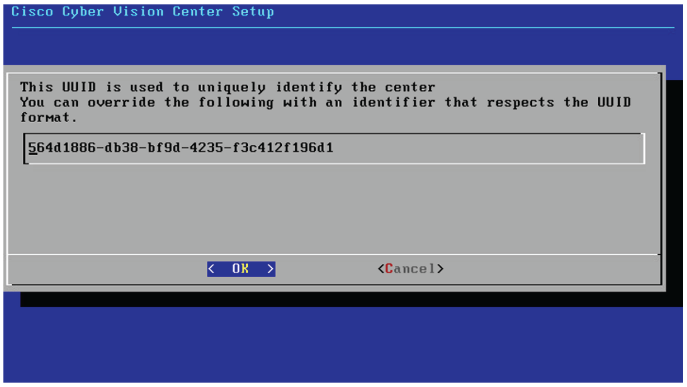


```
Cisco Cyber Vision Center Setup

Are you trying to restore
a Center and need to
manually set the center id
?
```

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.

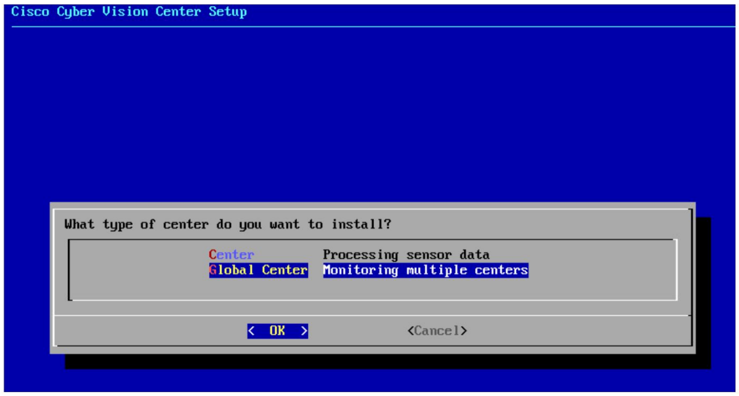


```
Cisco Cyber Vision Center Setup

This UUID is used to uniquely identify the center
You can override the following with an identifier that respects the UUID
format.

564d1886-db38-bf9d-4235-f3c412f196d1
```

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

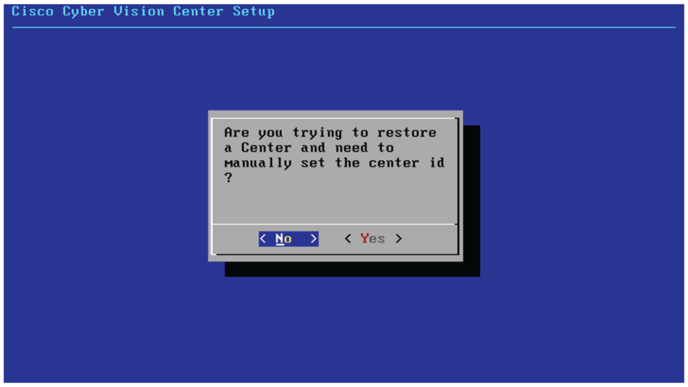
Global Center

If installing a Global Center, select the second option.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

Center          Processing sensor data
Global Center   Monitoring multiple centers
```

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



```
Cisco Cyber Vision Center Setup

Are you trying to restore
a Center and need to
manually set the center id
?
```

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.

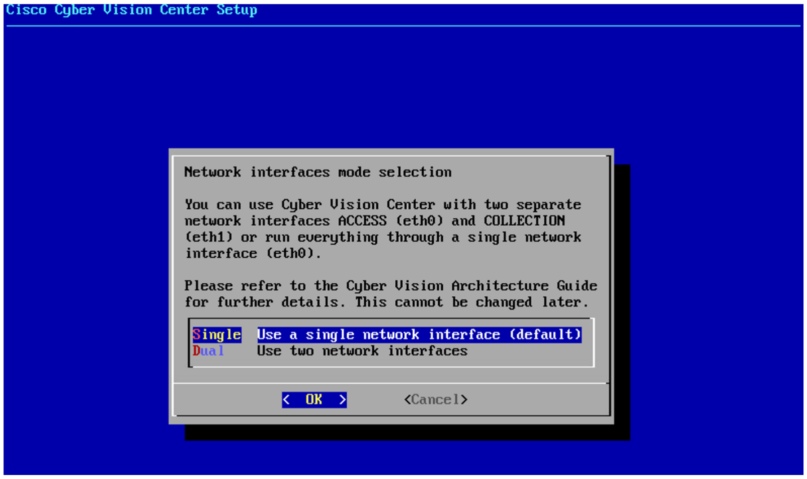
The administration network interface is configured using your chosen addressing and assignment method.

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.

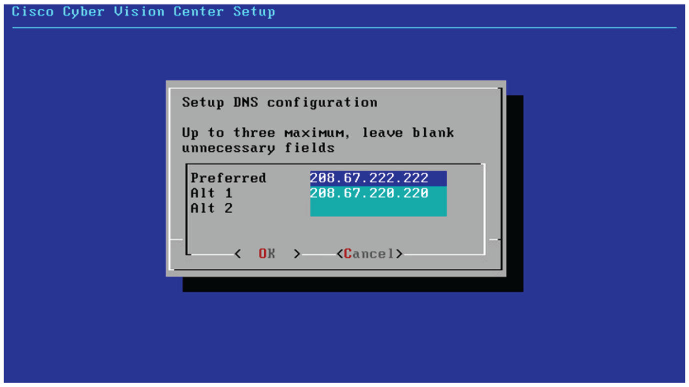


```
Cisco Cyber Vision Center Setup

Network interfaces mode selection

You can use Cyber Vision Center with two separate
network interfaces ACCESS (eth0) and COLLECTION
(eth1) or run everything through a single network
interface (eth0).

Please refer to the Cyber Vision Architecture Guide
for further details. This cannot be changed later.

Single   Use a single network interface (default)
Dual     Use two network interfaces

< OK >          <Cancel>
```

If you choose the Dual option, you will later be directed to: Configure the Center's Collection network interface, on page 18.

Configure the Center's DNS

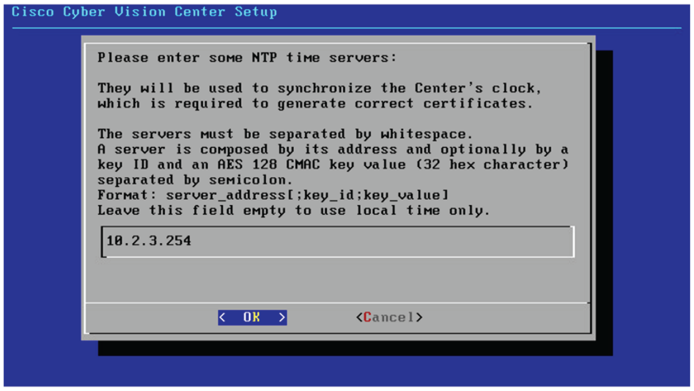
Type a DNS server address and optional fallbacks.



```
Cisco Cyber Vision Center Setup

Setup DNS configuration

Up to three maximum, leave blank
unnecessary fields

Preferred      208.67.222.222
Alt 1          208.67.220.220
Alt 2

        <  OK  >      <Cancel>
```

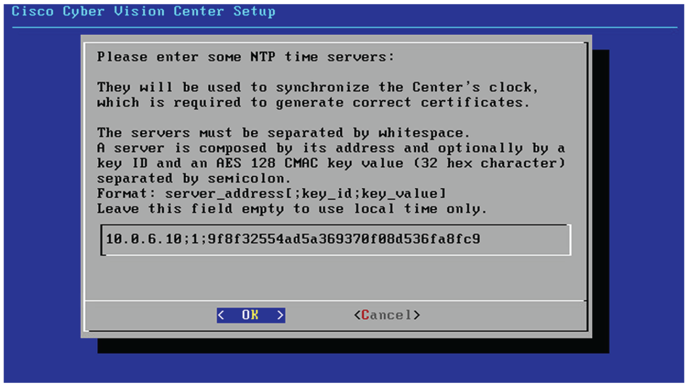
Synchronize the Center and the sensors to NTP servers

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.



```
Cisco Cyber Vision Center Setup

Please enter some NTP time servers:

They will be used to synchronize the Center's clock,
which is required to generate correct certificates.

The servers must be separated by whitespace.
A server is composed by its address and optionally by a
key ID and an AES 128 CMAC key value (32 hex character)
separated by semicolon.
Format: server_address[;key_id;key_value]
Leave this field empty to use local time only.

10.2.3.254

            <  OK  >          <Cancel>
```

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

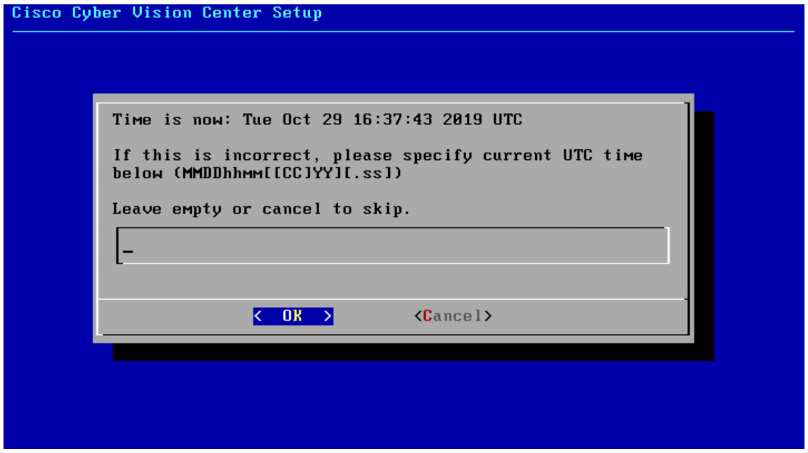


```
Cisco Cyber Vision Center Setup

Please enter some NTP time servers:

They will be used to synchronize the Center's clock,
which is required to generate correct certificates.

The servers must be separated by whitespace.
A server is composed by its address and optionally by a
key ID and an AES 128 CMAC key value (32 hex character)
separated by semicolon.
Format: server_address[;key_id;key_value]
Leave this field empty to use local time only.

10.0.6.10;1;9f8f32554ad5a369370f08d536fa8fc9

            <  OK  >          <Cancel>
```

The synchronization takes a few seconds.

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

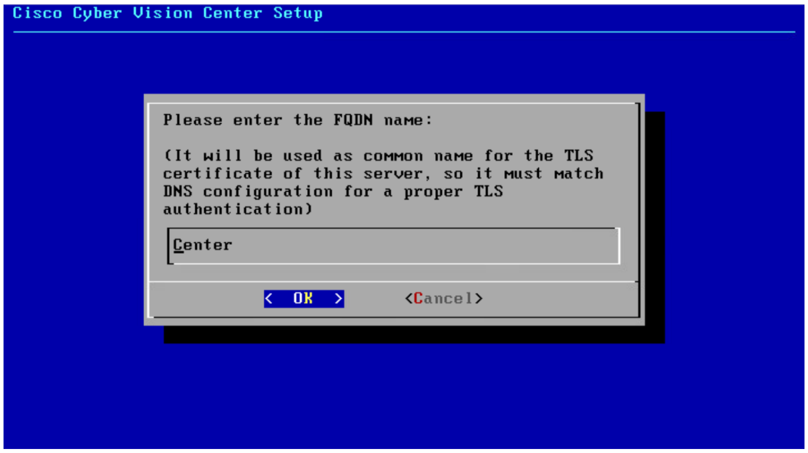
Note The time is set in UTC standard.



```
Cisco Cyber Vision Center Setup

Time is now: Tue Oct 29 16:37:43 2019 UTC

If this is incorrect, please specify current UTC time
below (MMDDhhmm[[CC]YY][.ss])

Leave empty or cancel to skip.

_

<  OK  >          <Cancel>
```

Give the Center a name

Note This name will be used in the Center certificate.



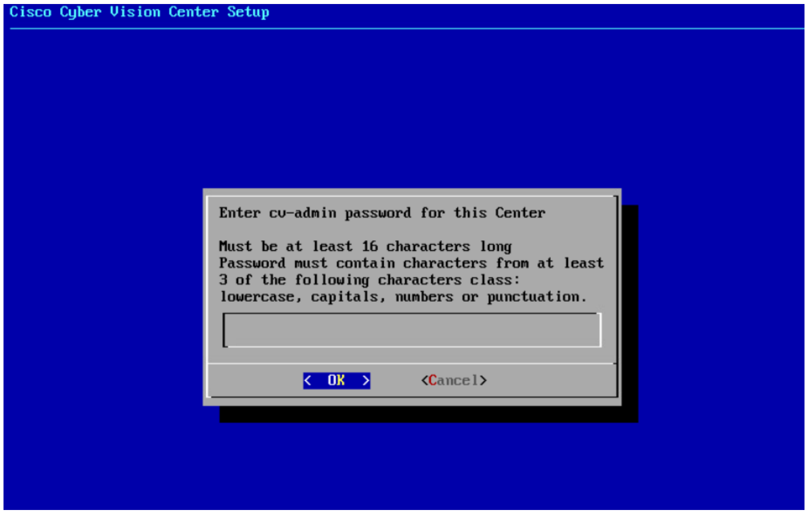
```
Cisco Cyber Vision Center Setup

Please enter the FQDN name:

(It will be used as common name for the TLS
certificate of this server, so it must match
DNS configuration for a proper TLS
authentication)

Center

<  OK  >          <Cancel>
```

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.

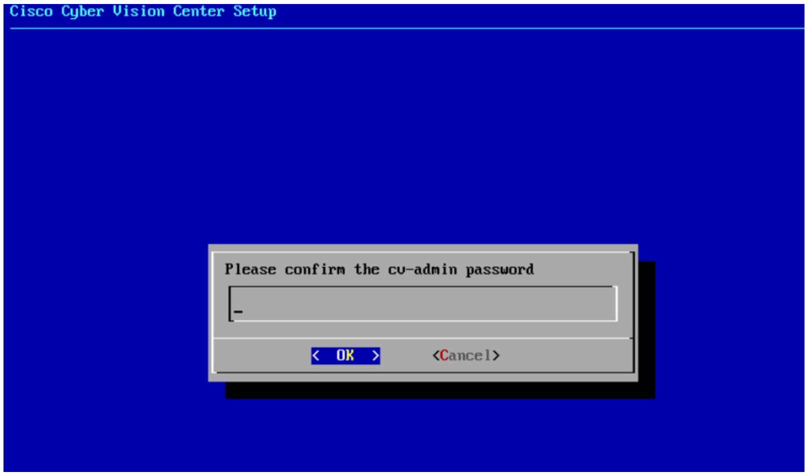
Set the Center's password

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



```
Cisco Cyber Vision Center Setup

Enter cv-admin password for this Center

Must be at least 16 characters long
Password must contain characters from at least
3 of the following characters class:
lowercase, capitals, numbers or punctuation.
```

Confirm the password.



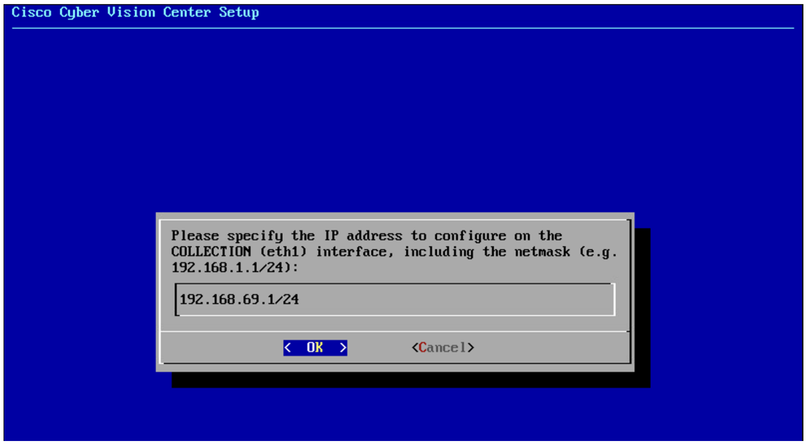
```
Cisco Cyber Vision Center Setup

Please confirm the cv-admin 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:



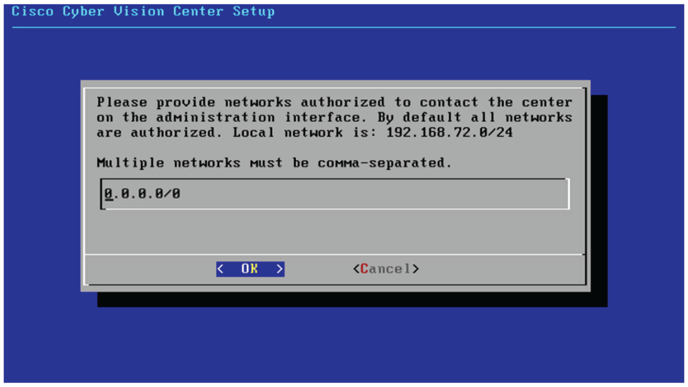
Cisco Cyber Vision Center Setup

Please specify the IP address to configure on the COLLECTION (eth1) interface, including the netmask (e.g. 192.168.1.1/24):

192.168.69.1/24

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.



Cisco Cyber Vision Center Setup

Please provide networks authorized to contact the center on the administration interface. By default all networks are authorized. Local network is: 192.168.72.0/24

Multiple networks must be comma-separated.

0.0.0.0/0

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 20 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.

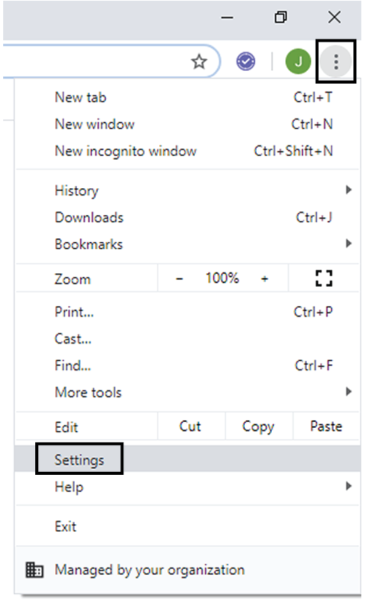
Step 2 Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.

The certificate is downloaded.

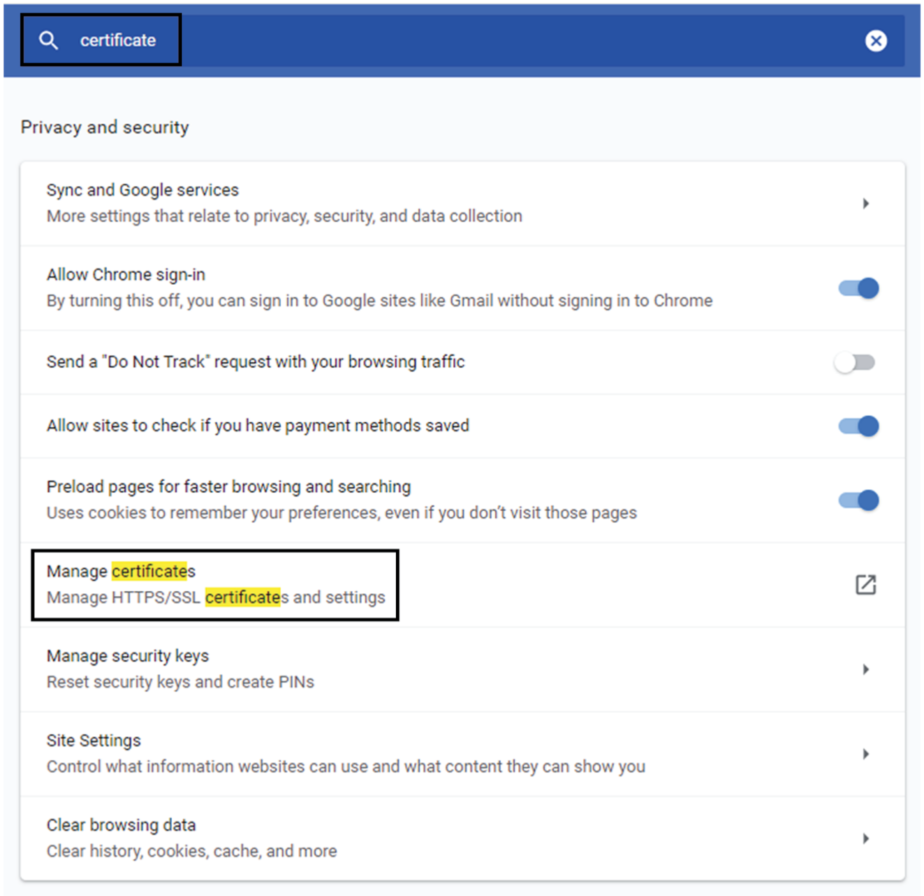
Step 3 Save the certificate on your computer.

Step 4 In the browser, access the settings.

Example: Chrome



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



certificate

Privacy and security

Sync and Google services
More settings that relate to privacy, security, and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

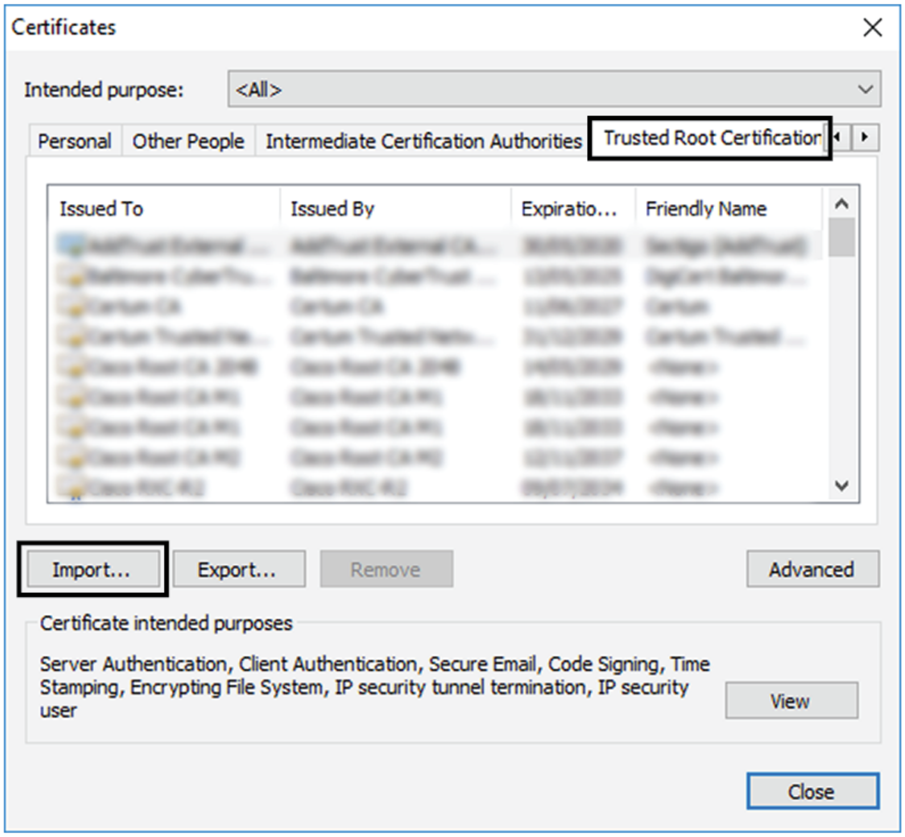
Manage certificates
Manage HTTPS/SSL certificates and settings

Manage security keys
Reset security keys and create PINs

Site Settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

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



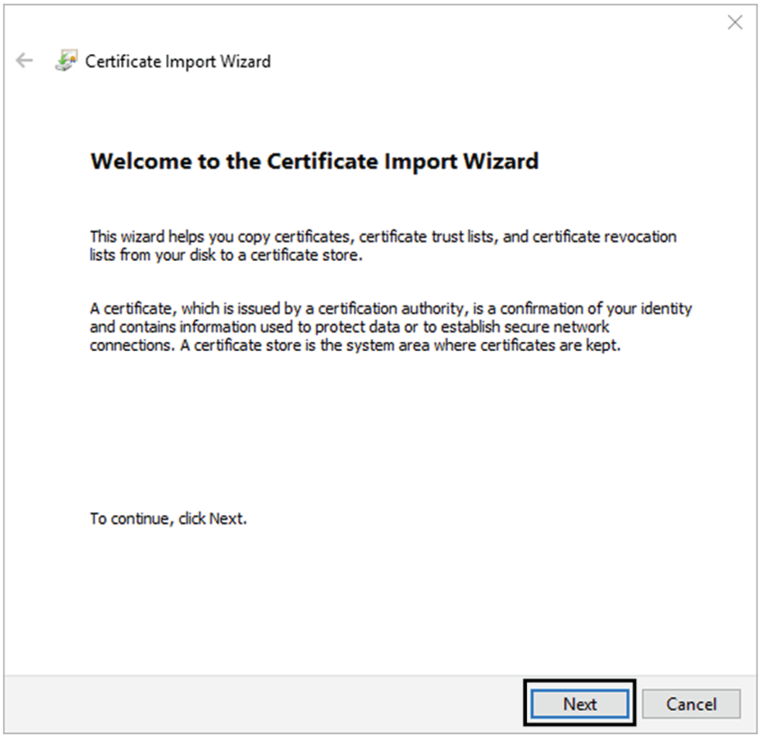
Intended purpose: <All>

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user

A certificate importation wizard opens.

Step 7 Go to the next step.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

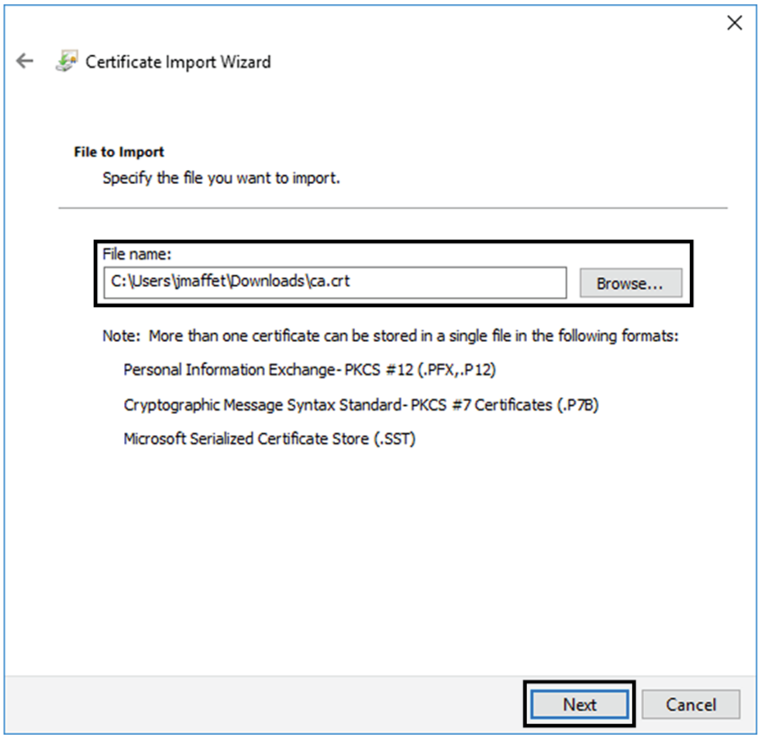
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 8 Search for the certificate you downloaded earlier.

Step 9 Go to the next step.



File to Import

Specify the file you want to import.

File name: C:\Users\jmaffet\Downloads\ca.crt

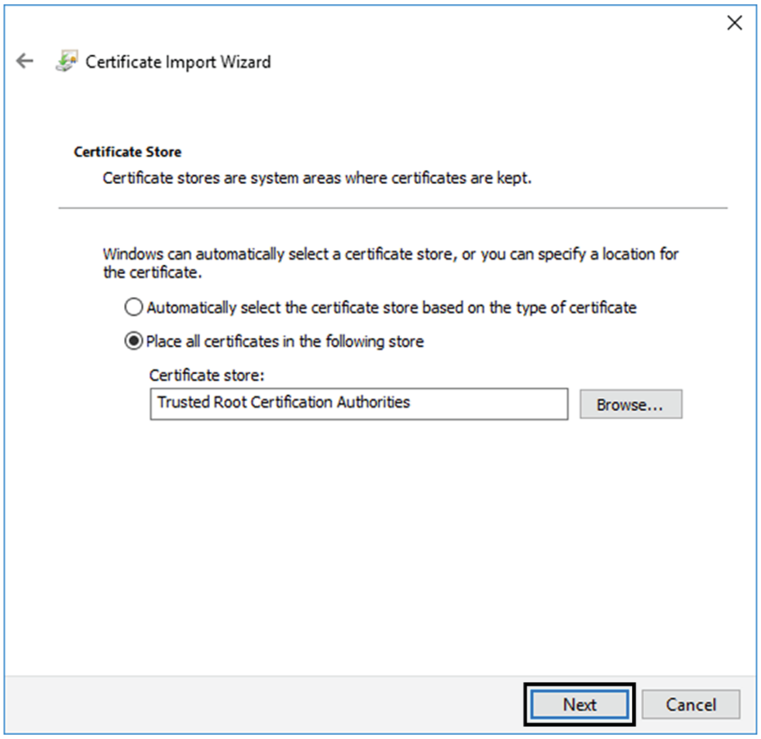
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Store

Certificate stores are system areas where certificates are kept.

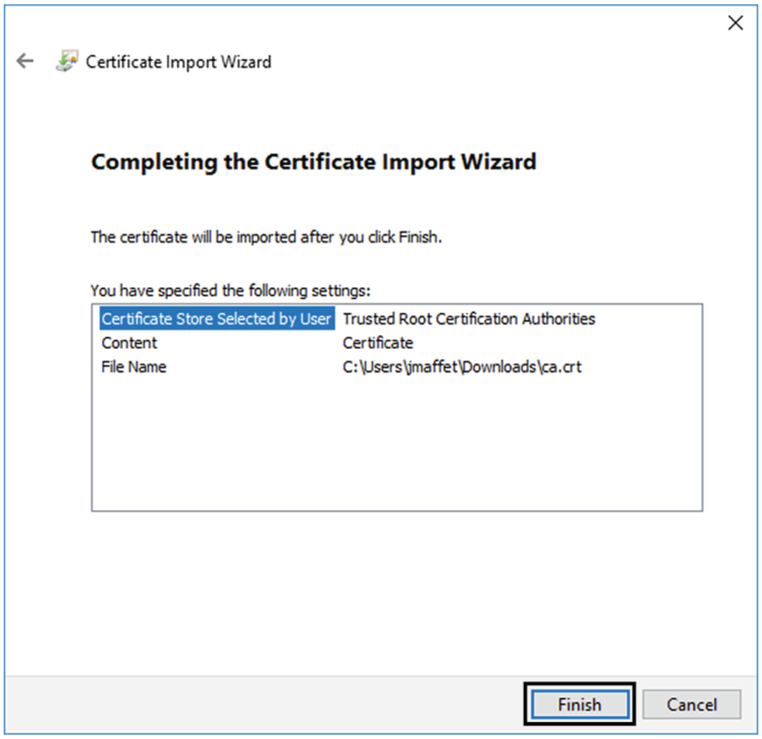
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

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



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\jmaffet\Downloads\ca.crt

What to do next

Install , on page 26

Install

Access the installation wizard:

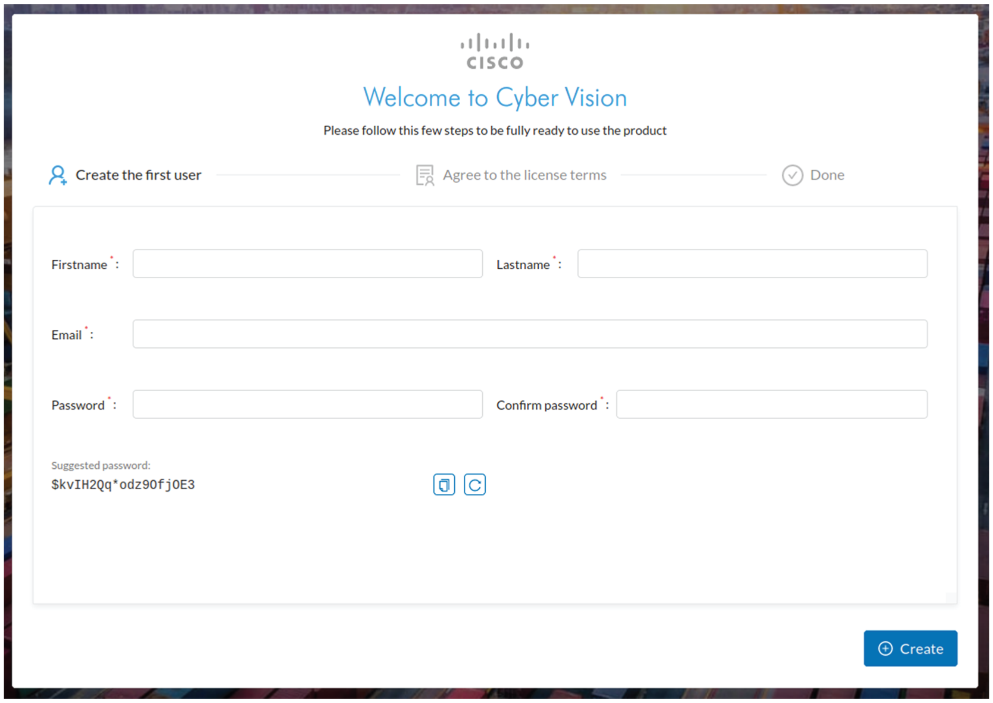
Procedure

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:**



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

Firstname * :

Lastname * :

Email * :

Password * :

Confirm password * :

Suggested password:

`$kvIH2Qq*odz90fjOE3`

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:

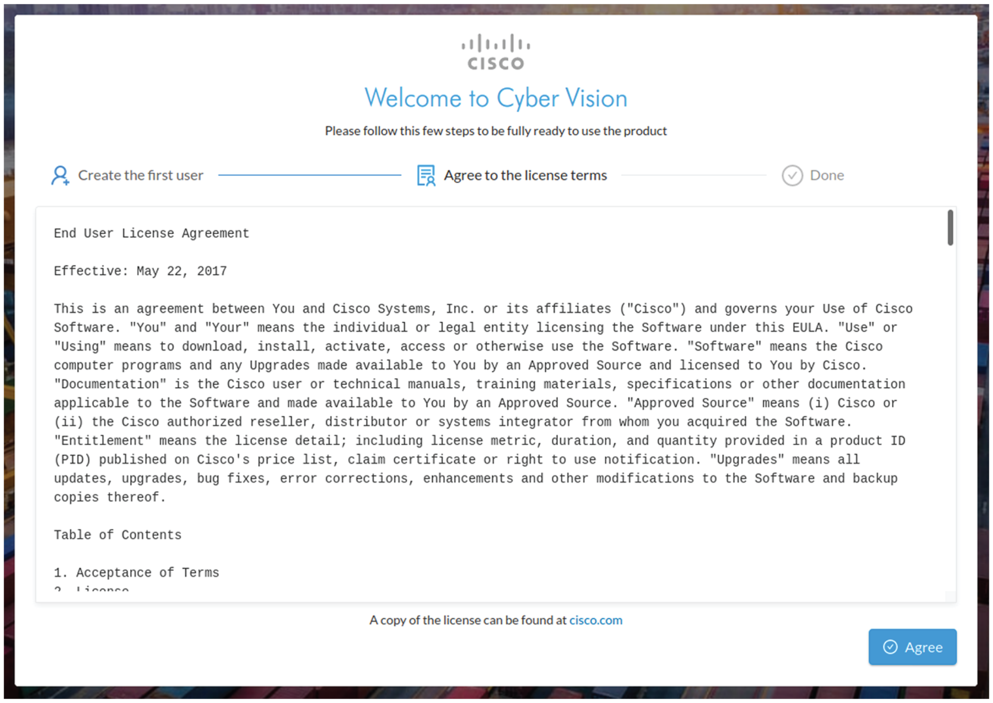
- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

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:**



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

```
End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco
Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco
computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation
applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software.
"Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID
(PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all
updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup
copies thereof.

Table of Contents

1. Acceptance of Terms
```

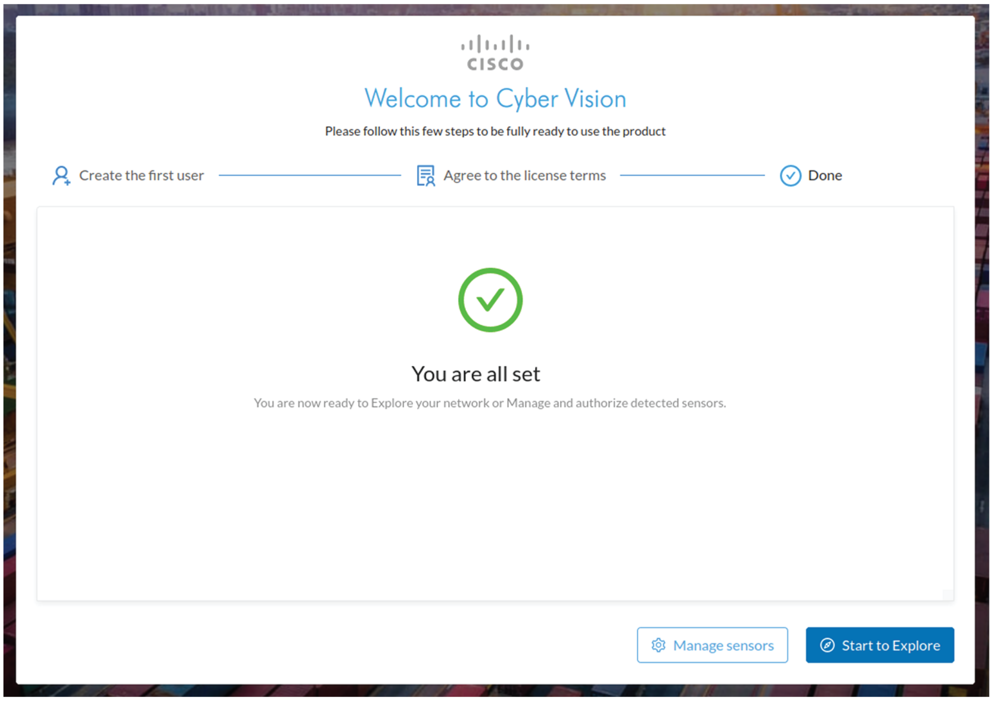
A copy of the license can be found at cisco.com

Step 7

Step 8 **Finish the installation:**

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

Step 9 Click Start to Explore.



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

You are all set

You are now ready to Explore your network or Manage and authorize detected sensors.

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

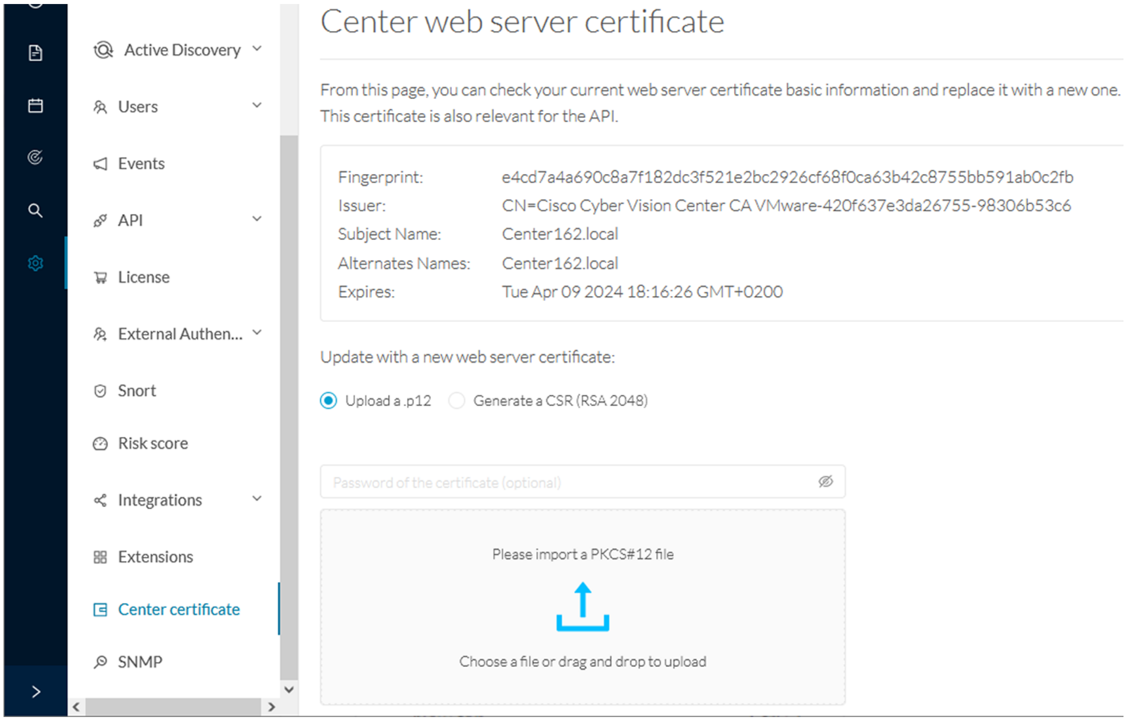
This section explains how to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

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.



Center web server certificate

From this page, you can check your current web server certificate basic information and replace it with a new one. This certificate is also relevant for the API.

Fingerprint: e4cd7a4a690c8a7f182dc3f521e2bc2926cf68f0ca63b42c8755bb591ab0c2fb
Issuer: CN=Cisco Cyber Vision Center CA VMware-420f637e3da26755-98306b53c6
Subject Name: Center162.local
Alternates Names: Center162.local
Expires: Tue Apr 09 2024 18:16:26 GMT+0200

Update with a new web server certificate:

● Upload a .p12 ○ Generate a CSR (RSA 2048)

Password of the certificate (optional)
Please import a PKCS#12 file
Choose a file or drag and drop to upload

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

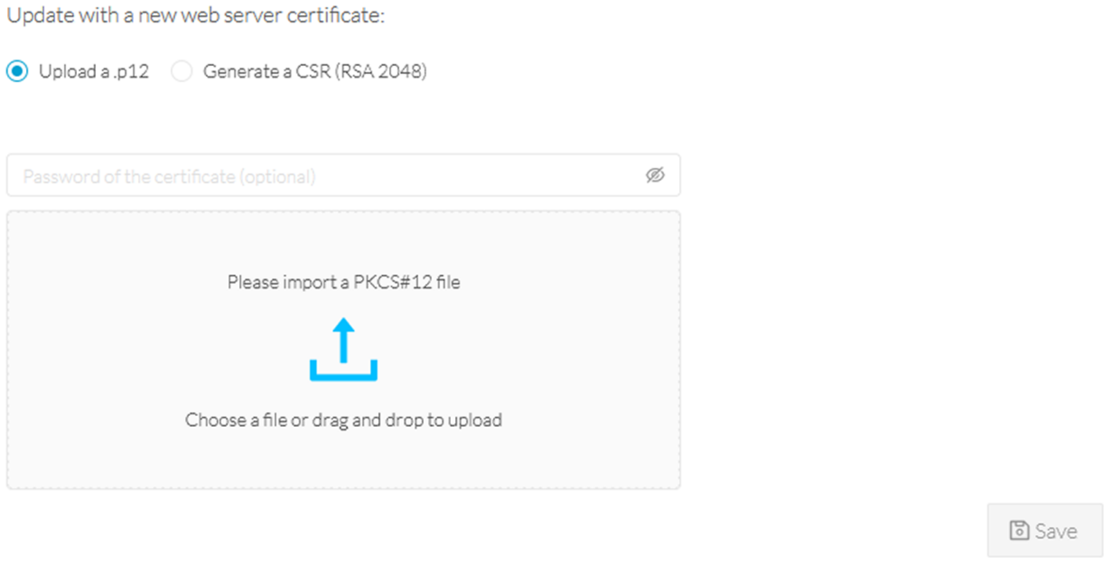
Upload a p12

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.



Update with a new web server certificate:

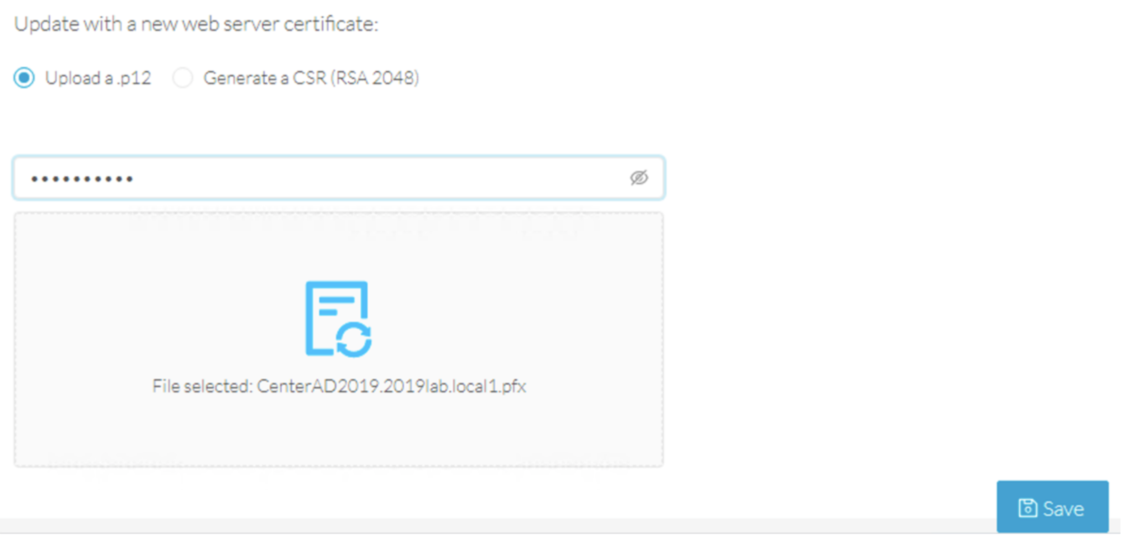
● Upload a .p12 ○ Generate a CSR (RSA 2048)

Password of the certificate (optional)
Please import a PKCS#12 file
Choose a file or drag and drop to upload
Save

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.



Update with a new web server certificate:

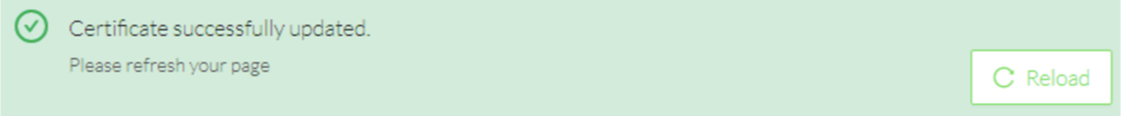
● Upload a .p12 ○ Generate a CSR (RSA 2048)

••••••••••

File selected: CenterAD2019.2019lab.local1.pfx

Step 4 Click Save.

The following message appears:



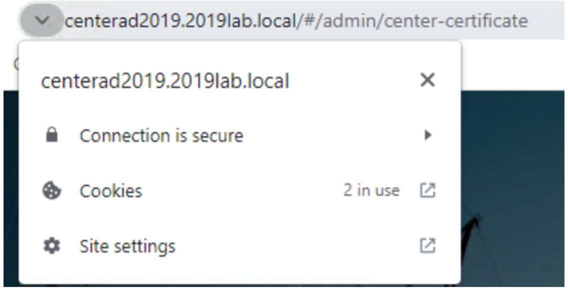
Certificate successfully updated.

Please refresh your page

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.



centerad2019.2019lab.local/#/admin/center-certificate

centerad2019.2019lab.local

Connection is secure

Cookies 2 in use

Site settings

What to do next

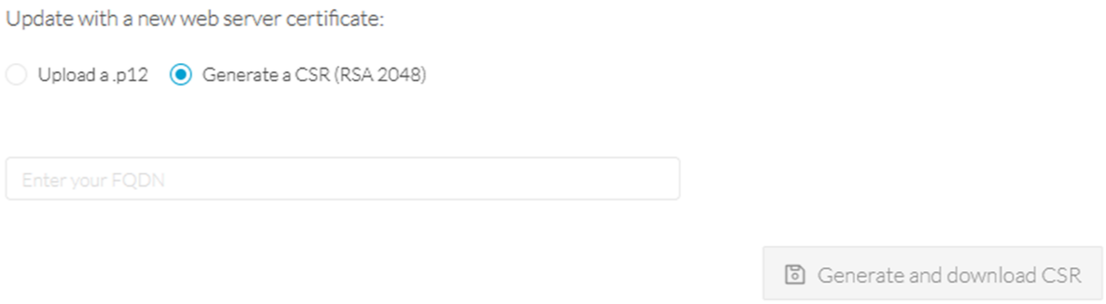
If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 34.

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.



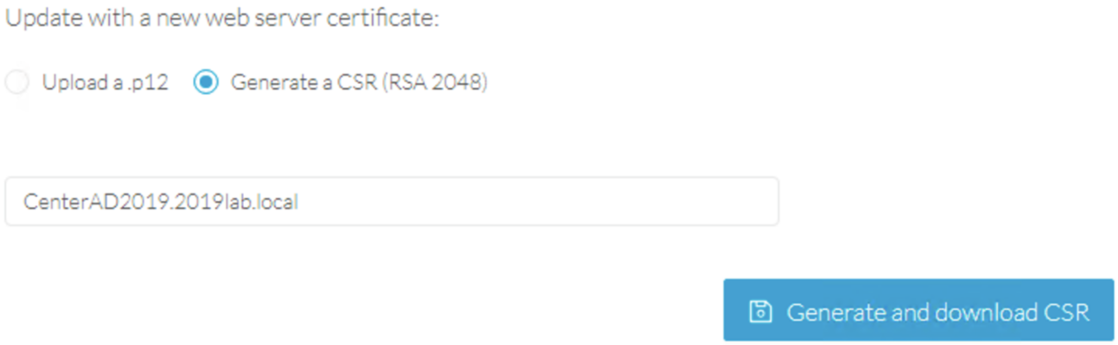
Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

Enter your FQDN

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

Step 3 Click the Generate and download CSR button.



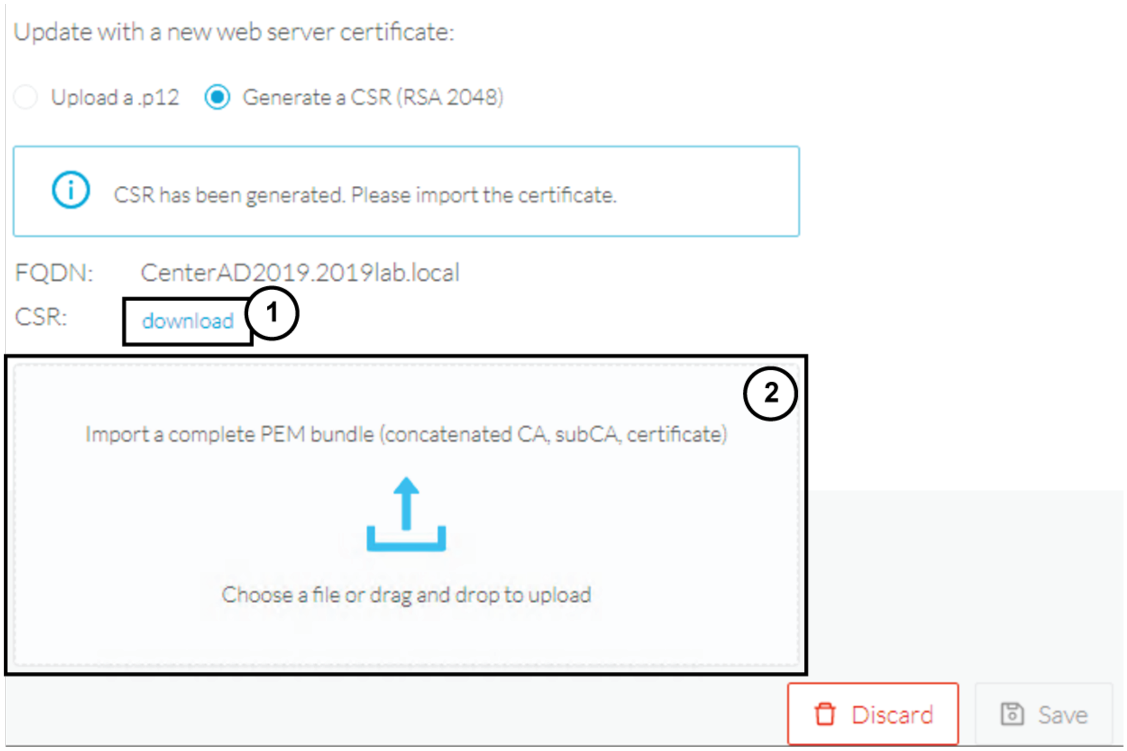
Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

CenterAD2019.2019lab.local

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

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



Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

CSR has been generated. Please import the certificate.

FQDN: CenterAD2019.2019lab.local

CSR: download

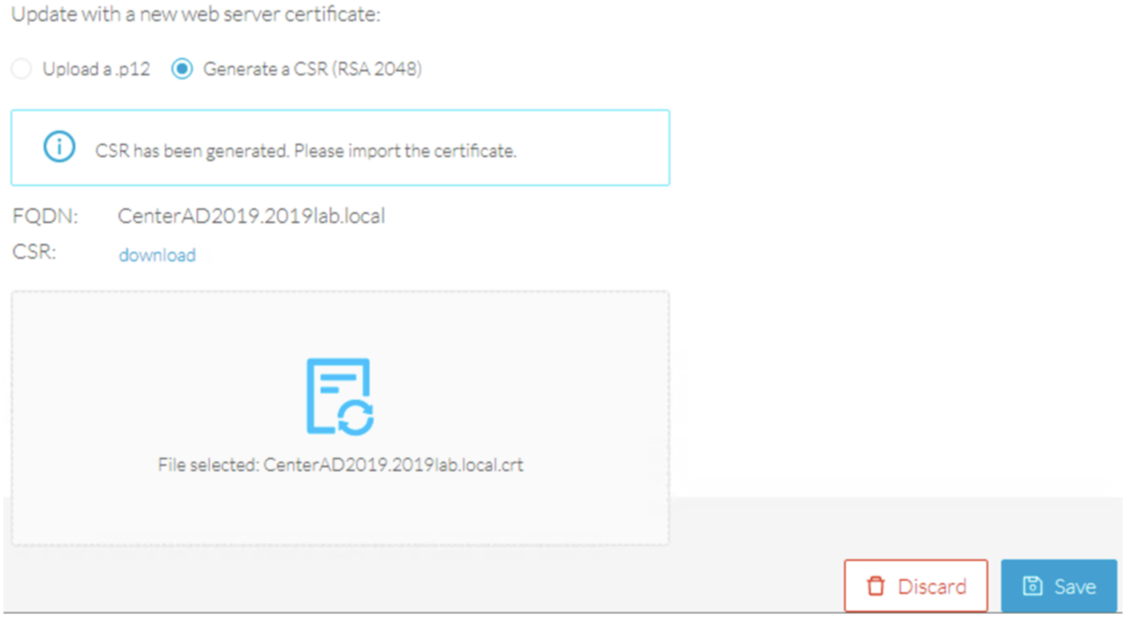
Import a complete PEM bundle (concatenated CA, subCA, certificate)

Choose a file or drag and drop to upload

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.



Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

CSR has been generated. Please import the certificate.

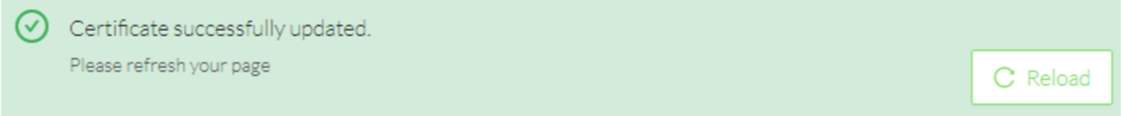
FQDN: CenterAD2019.2019lab.local

CSR: download

File selected: CenterAD2019.2019lab.local.crt

Step 7 Click Save.

The following message appears:



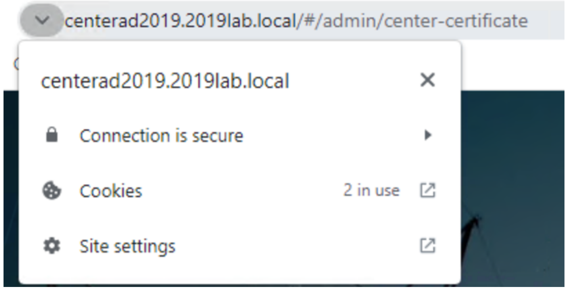
Certificate successfully updated.

Please refresh your page

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.



centerad2019.2019lab.local/#/admin/center-certificate

centerad2019.2019lab.local

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.

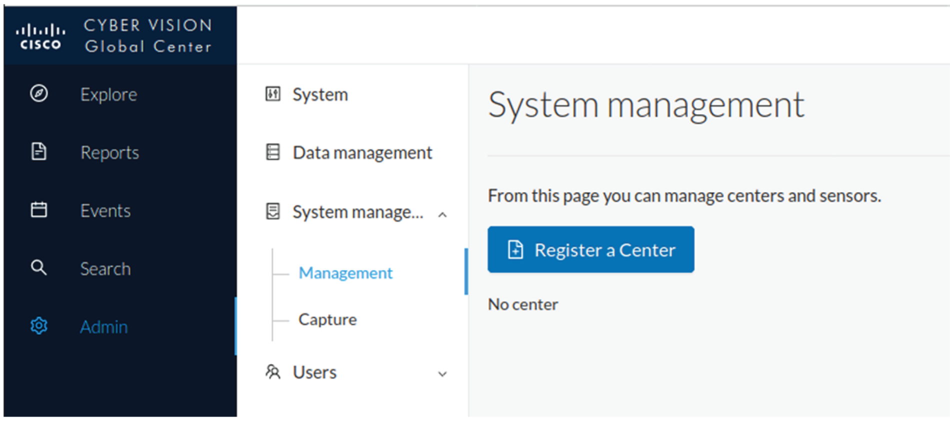
Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists of registering the Center in the Global Center and enrolling the Center to the Global Center. To do so, you need to open each's 's GUI.

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.



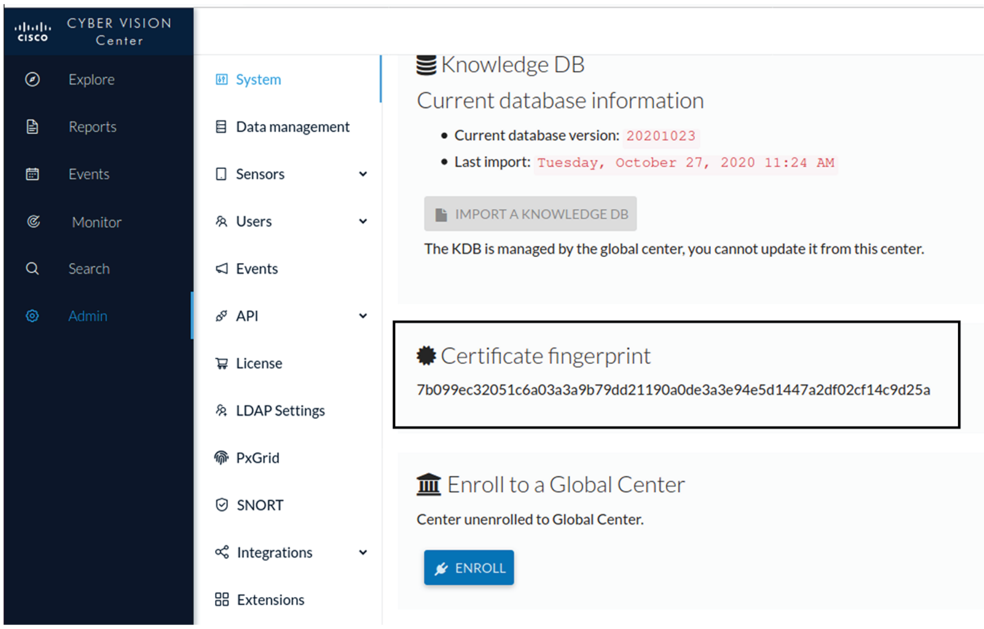
From this page you can manage centers and sensors.

No center

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.



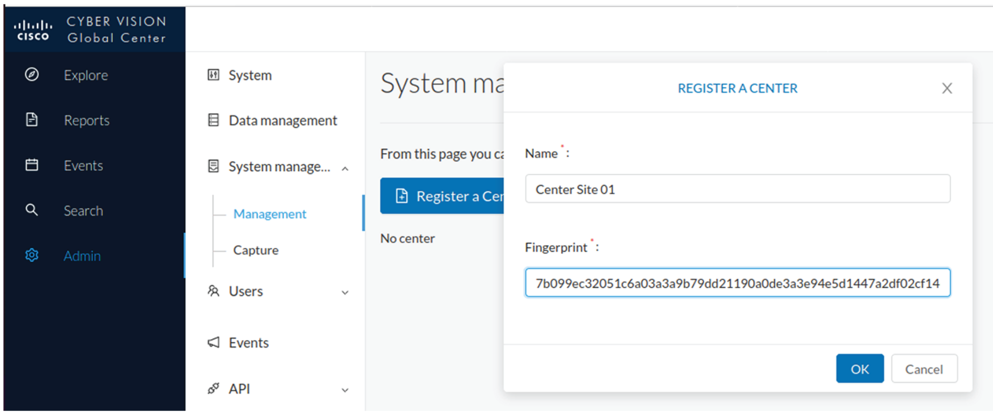
- Current database version: 20201023
- Last import: Tuesday, October 27, 2020 11:24 AM

The KDB is managed by the global center, you cannot update it from this center.

7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14c9d25a

Center unenrolled to Global Center.

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

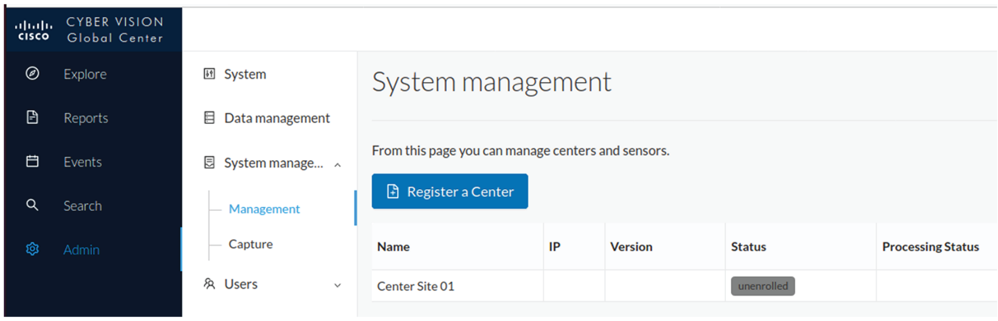


Name * : Center Site 01

Fingerprint * : 7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14

Step 6 Click **OK**.

The Center appears in the list as unenrolled.



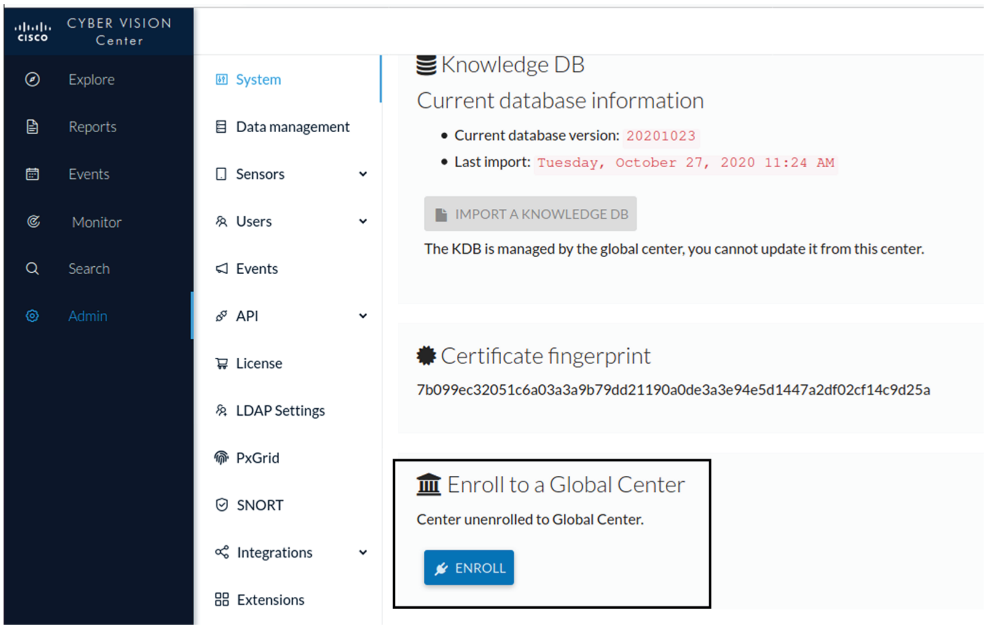
System management

From this page you can manage centers and sensors.

Name	IP	Version	Status	Processing Status
Center Site 01			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.



Knowledge DB

Current database information

- Current database version: 20201023
- Last import: Tuesday, October 27, 2020 11:24 AM

IMPORT A KNOWLEDGE DB

The KDB is managed by the global center, you cannot update it from this center.

Certificate fingerprint

7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14c9d25a

Enroll to a Global Center

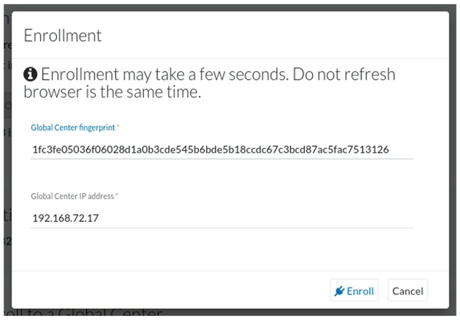
Center unenrolled to Global Center.

ENROLL

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**.



Enrollment

Enrollment may take a few seconds. Do not refresh browser is the same time.

Global Center fingerprint *

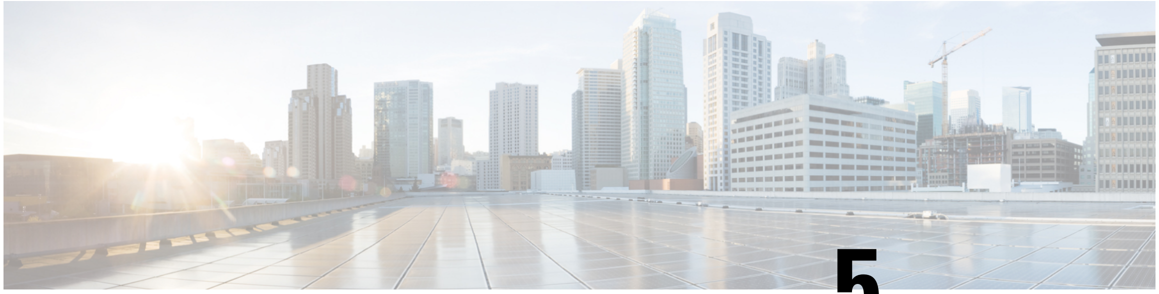
1fc3fe05036f06028d1a0b3cde545b6bde5b18ccdc67c3bcd87ac5fac7513126

Global Center IP address *

192.168.72.17

Enroll Cancel

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:

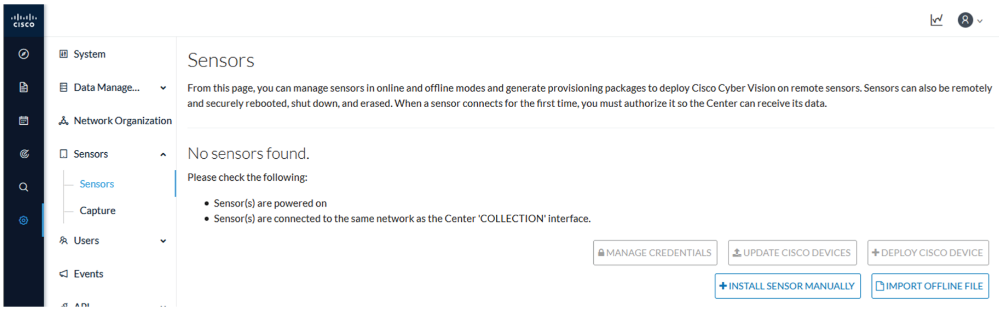
- If the server has a dual interface, that is, the Administration interface is on eth0 and the Collection interface is on eth1, then eth2 will be used for the Center DPI.
- If the server has a single interface, that is, the Administration and Collection interfaces are on the same interface, then eth1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



Sensors

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

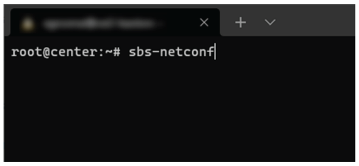
No sensors found.

Please check the following:

- Sensor(s) are powered on
- Sensor(s) are connected to the same network as the Center 'COLLECTION' interface.

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

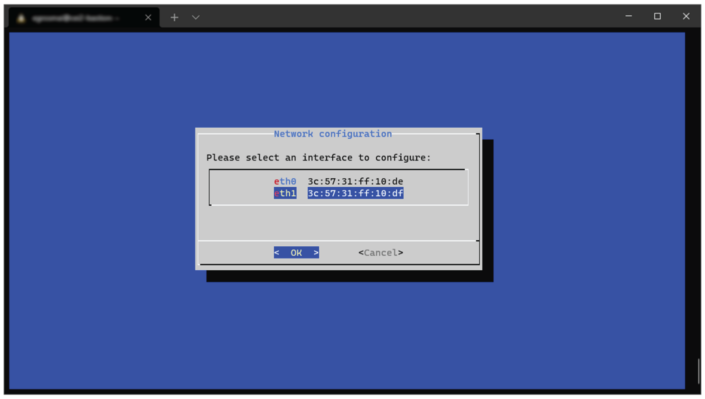
sbs-netconf



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

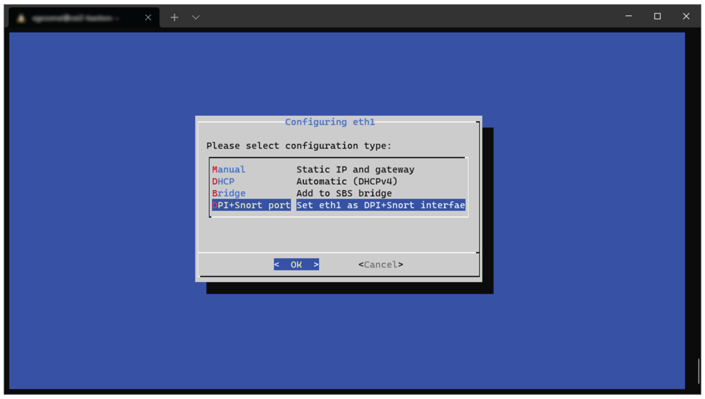
Step 3 In the case of a single interface, select the eth1 interface.

In the case if a dual interface, select eth2.



```
Network configuration

Please select an interface to configure:

eth0   3c:57:31:ff:10:de
eth1   3c:57:31:ff:10:df
```

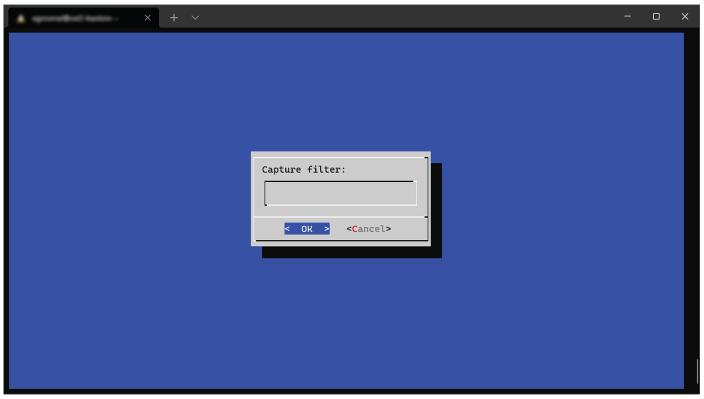
Step 4 Select the interface as DPI+Snort port.



```
Configuring eth1

Please select configuration type:

Manual           Static IP and gateway
DHCP             Automatic (DHCPv4)
Bridge           Add to SBS bridge
DPI+Snort port   Set eth1 as DPI+Snort interfae
```

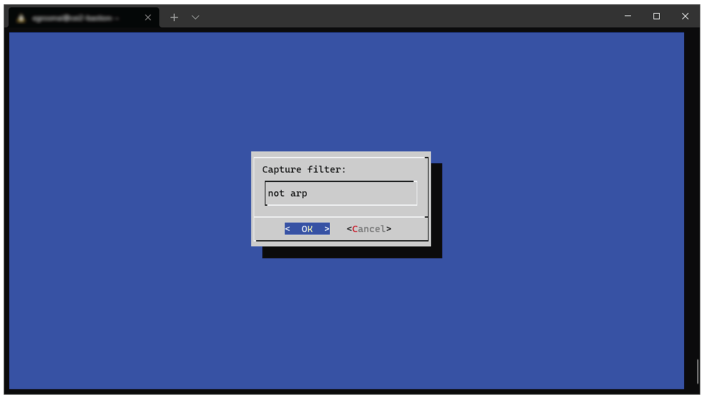
Step 5 Configure a capture filter mode. You can do that later in the sensor page clicking the Capture mode button.

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



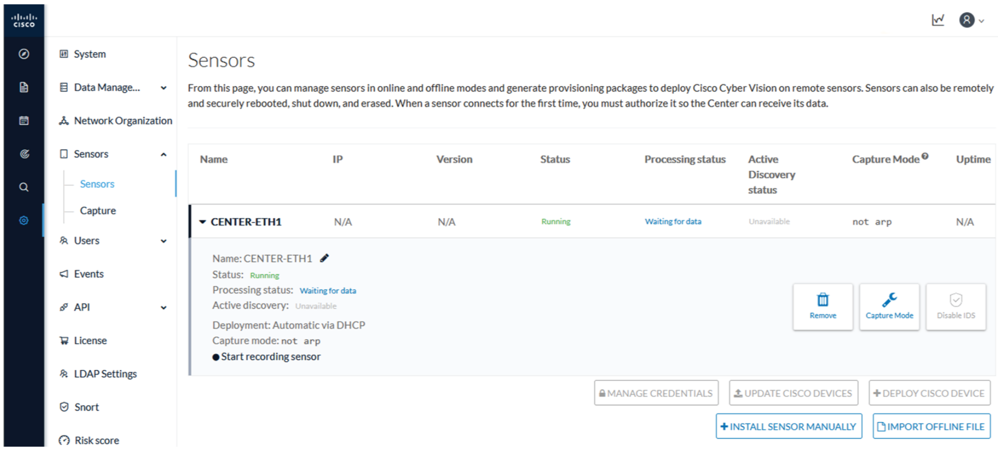
```
Capture filter:

<  OK  >   <Cancel>
```

For example, you can type "not arp".



```
Capture filter:
not arp

<  OK  >   <Cancel>
```

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



Sensors

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
CENTER-ETH1	N/A	N/A	Running	Waiting for data	Unavailable	not arp	N/A

Name: CENTER-ETH1
Status: Running
Processing status: Waiting for data
Active discovery: Unavailable
Deployment: Automatic via DHCP
Capture mode: not arp
● Start recording sensor

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

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.

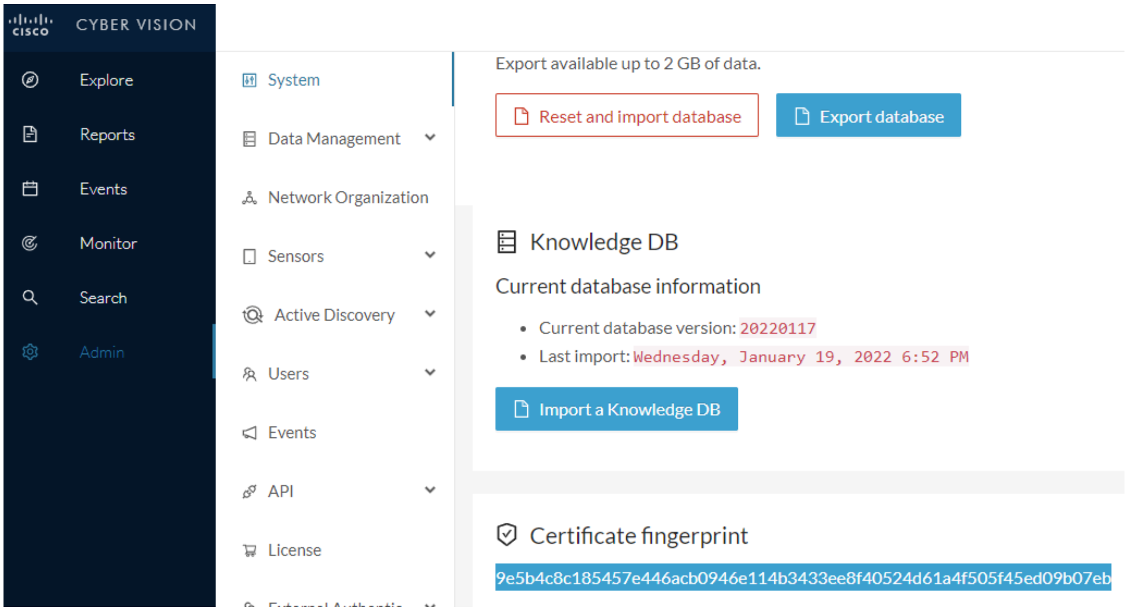
Center enrollment

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.



Export available up to 2 GB of data.

Knowledge DB

Current database information

- Current database version: 20220117
- Last import: Wednesday, January 19, 2022 6:52 PM

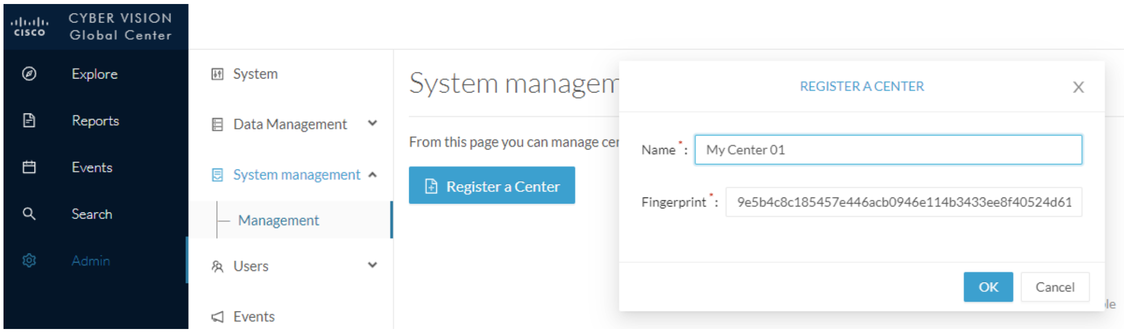
Certificate fingerprint

9e5b4c8c185457e446acb0946e114b3433ee8f40524d61a4f505f45ed09b07eb

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

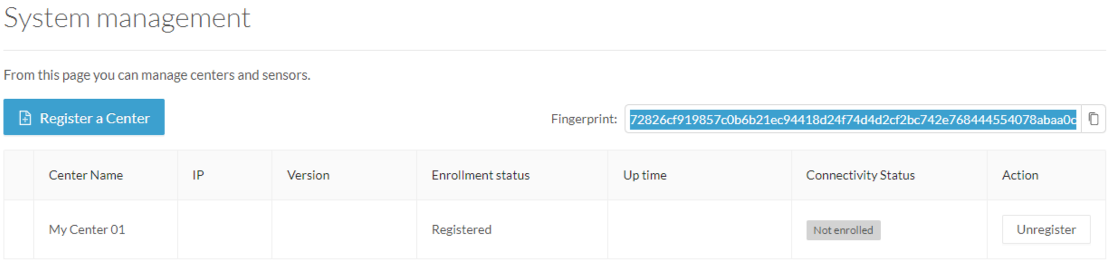


From this page you can manage cer

Name * : My Center 01

Fingerprint * : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61

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



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

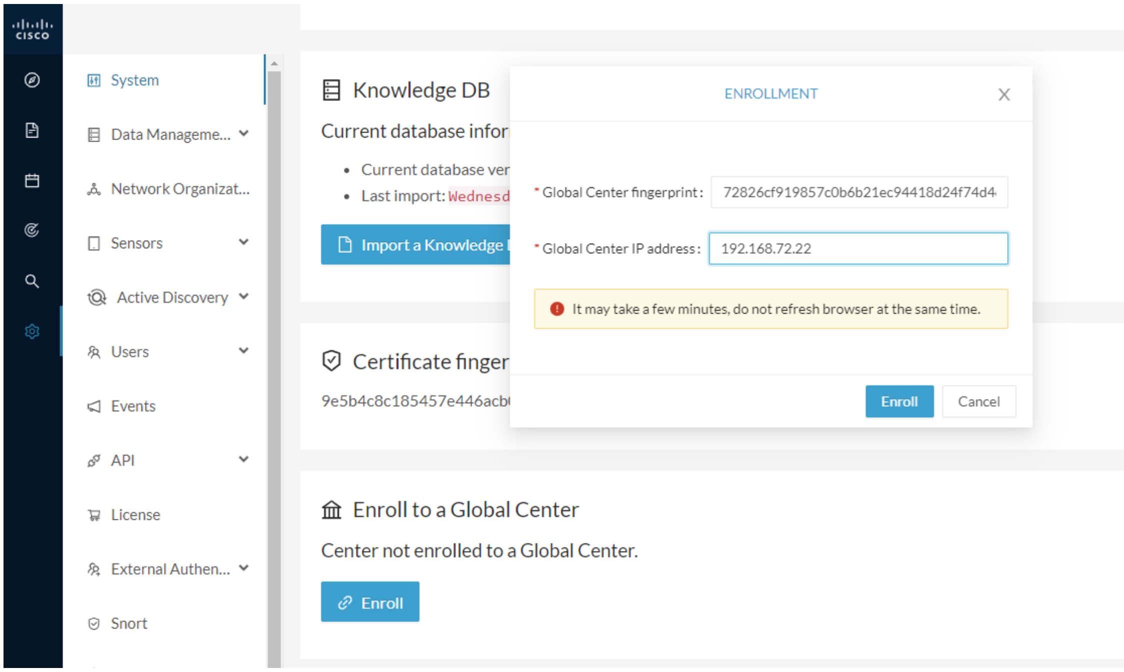
Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
My Center 01			Registered		Not enrolled	Unregister

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**



Knowledge DB

Current database infor

- Current database ver
- Last import: Wednesd

Certificate finger

9e5b4c8c185457e446acb

ENROLLMENT

* Global Center fingerprint: 72826cf919857c0b6b21ec94418d24f74d4

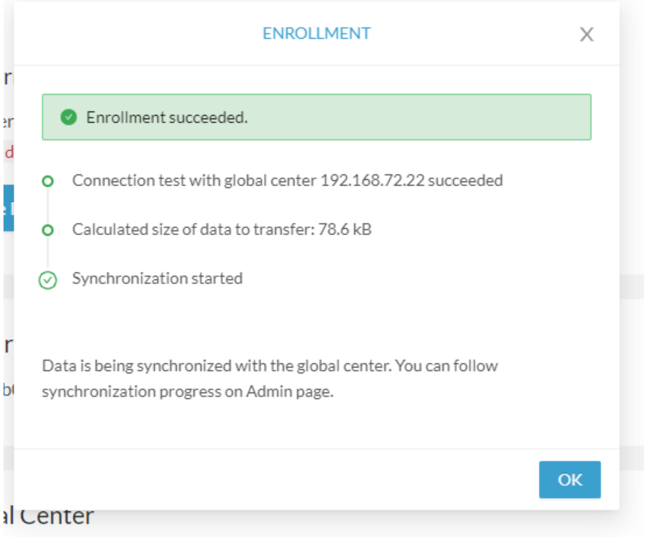
* Global Center IP address: 192.168.72.22

It may take a few minutes, do not refresh browser at the same time.

Enroll to a Global Center

Center not enrolled to a Global Center.

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**.



ENROLLMENT

Enrollment succeeded.

Connection test with global center 192.168.72.22 succeeded

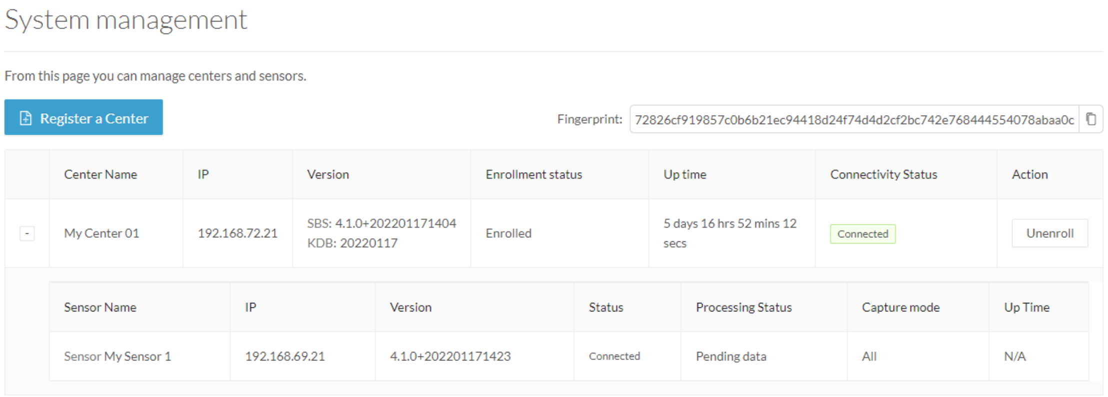
Calculated size of data to transfer: 78.6 kB

Synchronization started

Data is being synchronized with the global center. You can follow synchronization progress on Admin page.

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.



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
-	My Center 01	192.168.72.21	SBS: 4.1.0+202201171404 KDB: 20220117	Enrolled	5 days 16 hrs 52 mins 12 secs	Connected	Unenroll

Sensor Name	IP	Version	Status	Processing Status	Capture mode	Up Time
Sensor My Sensor 1	192.168.69.21	4.1.0+202201171423	Connected	Pending data	All	N/A

Center unenrollment

Before you begin

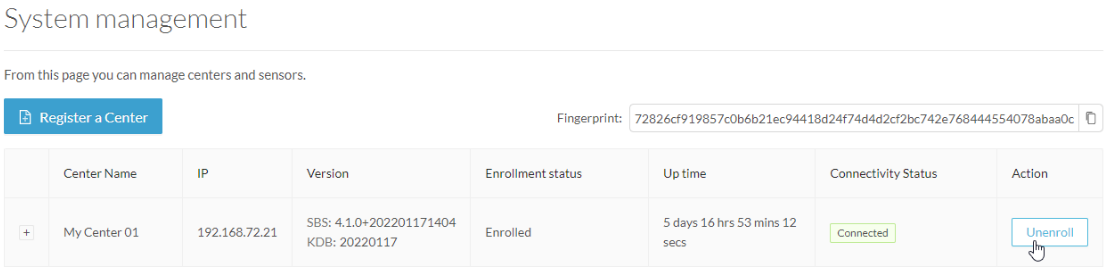
A Center can be unenrolled whenever it is needed, for example as a maintenance operation to replace the Center or the Global Center. This will delete all the Center's data in the Global Center.

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.



System management

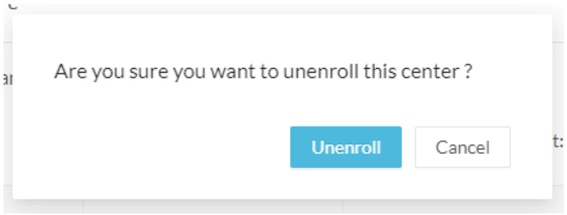
From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
+	My Center 01	192.168.72.21	SBS: 4.1.0+202201171404 KDB: 20220117	Enrolled	5 days 16 hrs 53 mins 12 secs	Connected	Unenroll

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

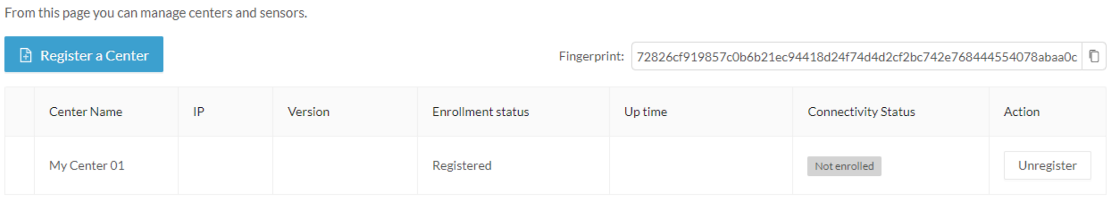
Step 3 A popup asking for confirmation appears. Click **Unenroll** to start the process.



Are you sure you want to unenroll this center ?

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.



From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
	My Center 01			Registered		Not enrolled	Unregister

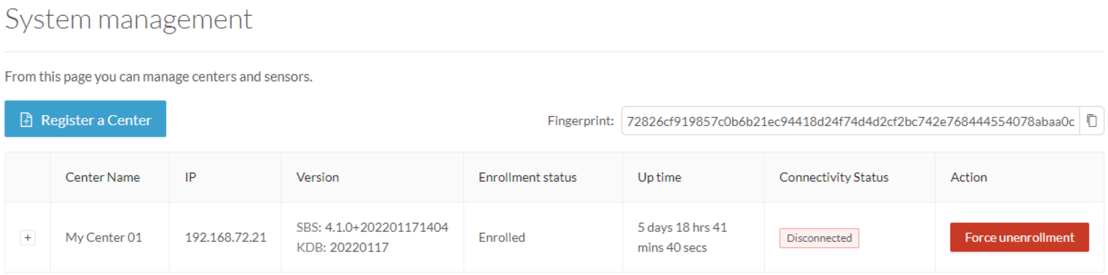
Force the unenrollement of a Center

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.



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
+	My Center 01	192.168.72.21	SBS: 4.1.0+202201171404 KDB: 20220117	Enrolled	5 days 18 hrs 41 mins 40 secs	Disconnected	Force unenrollment

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:

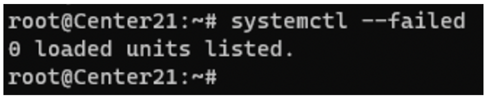
Procedure

Step 1 Connect to the Center in SSH.

Step 2 Type the following command:

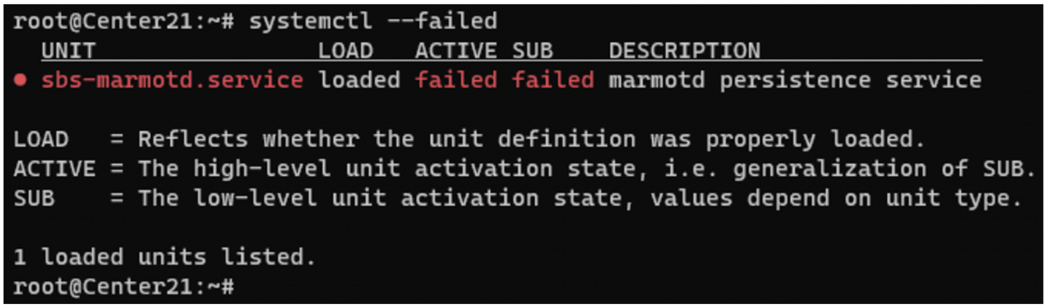
```
systemctl --failed
```

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

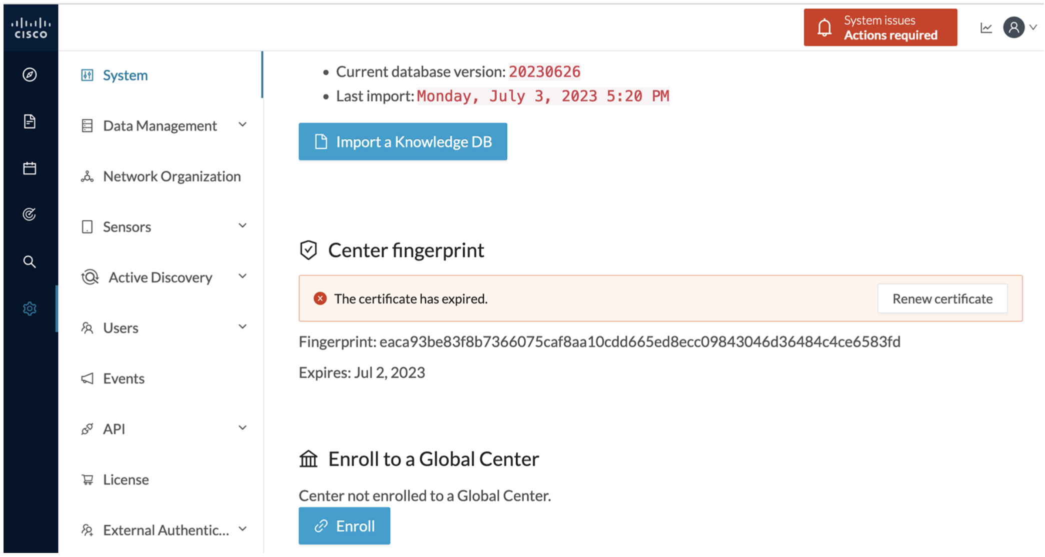
Renew the certificate of a Center

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.



- Current database version: 20230626
- Last import: Monday, July 3, 2023 5:20 PM

Center fingerprint

The certificate has expired.

Fingerprint: eaca93be83f8b7366075caf8aa10cdd665ed8ecc09843046d36484c4ce6583fd

Expires: Jul 2, 2023

Enroll to a Global Center

Center not enrolled to a Global Center.

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

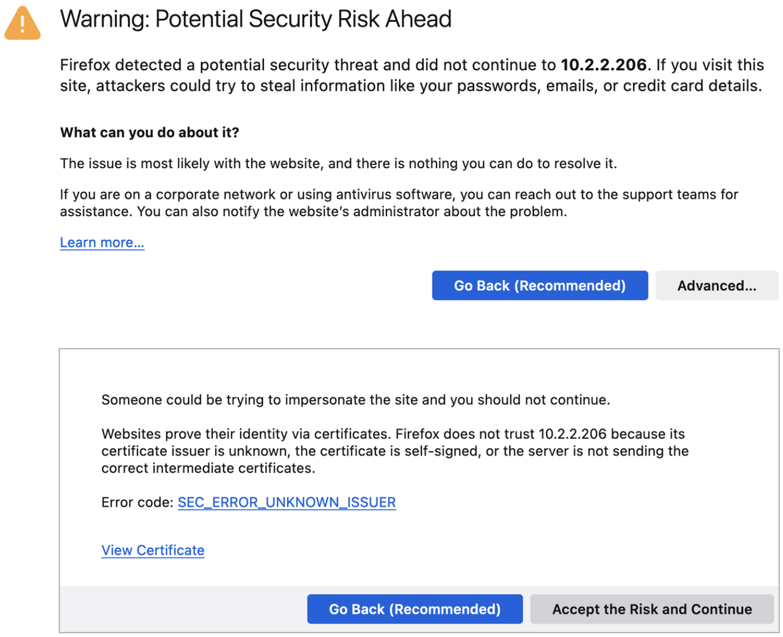
Before you begin

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.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.2.2.206**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

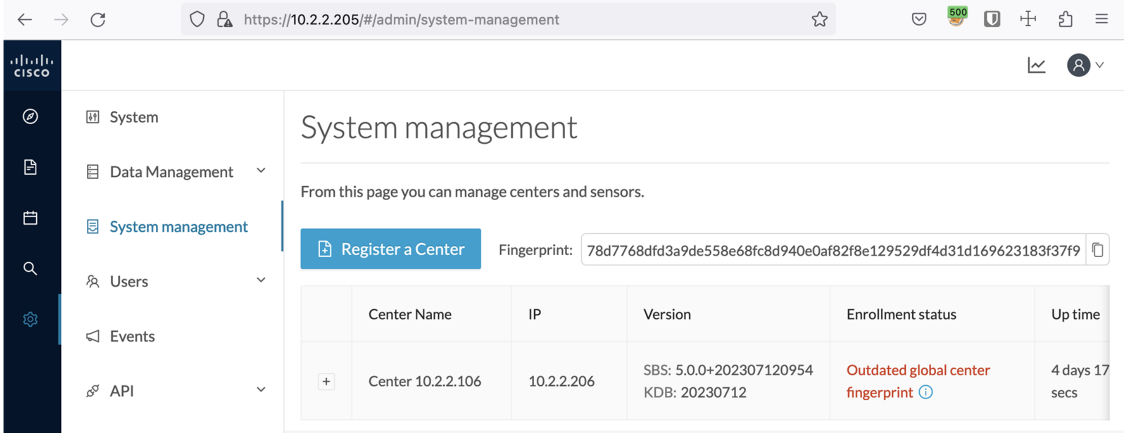
Websites prove their identity via certificates. Firefox does not trust 10.2.2.206 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

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.



System management

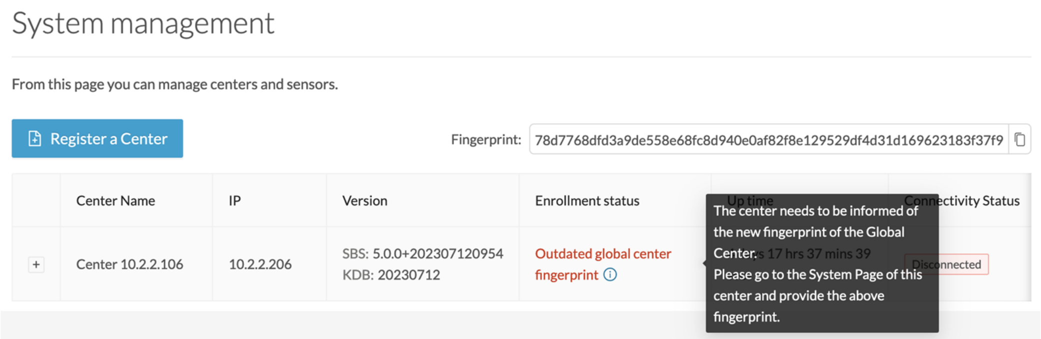
From this page you can manage centers and sensors.

Register a Center   Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9

	Center Name	IP	Version	Enrollment status	Up time
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated global center fingerprint ⓘ	4 days 17 secs

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.


System management

From this page you can manage centers and sensors.

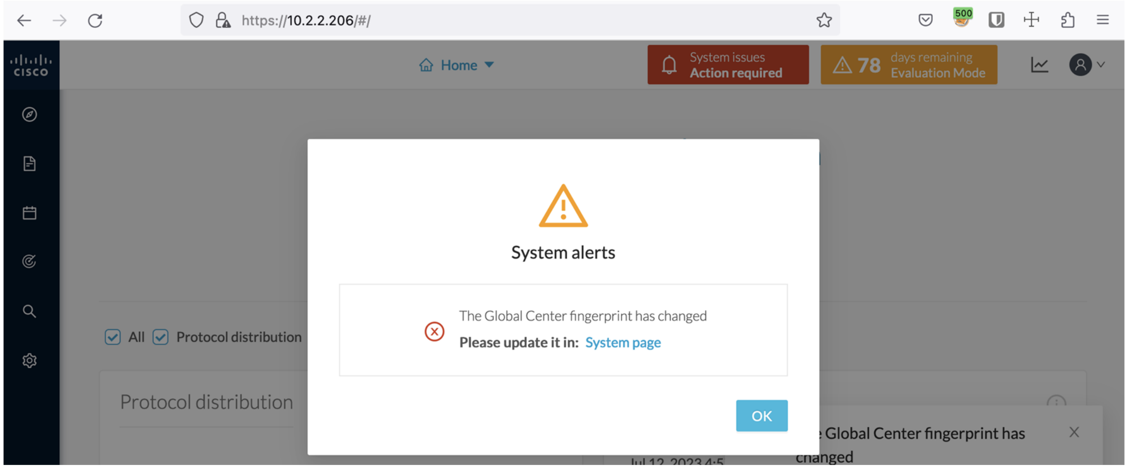
Register a Center   Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated global center fingerprint ⓘ	s 17 hrs 37 mins 39	Disconnected

The center needs to be informed of the new fingerprint of the Global Center. Please go to the System Page of this center and provide the above 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.



System alerts

The Global Center fingerprint has changed

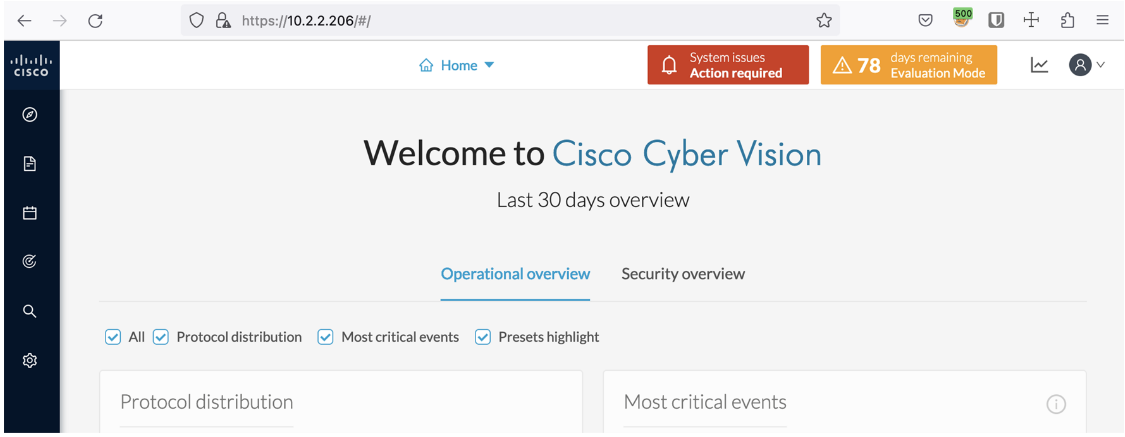
Please update it in: System page

OK

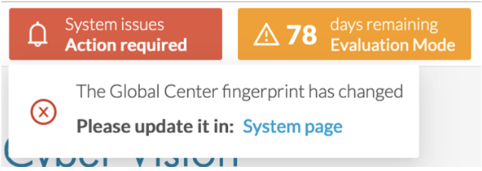
Global Center fingerprint has changed

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.



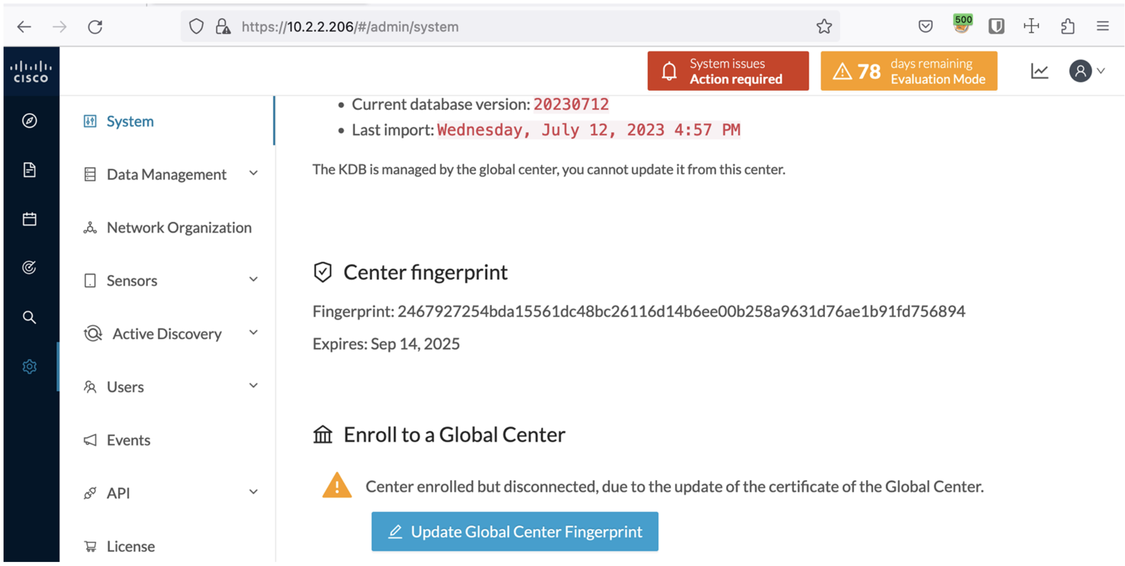
The Global Center fingerprint has changed

Please update it in: System page

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**.



- Current database version: 20230712
- Last import: Wednesday, July 12, 2023 4:57 PM

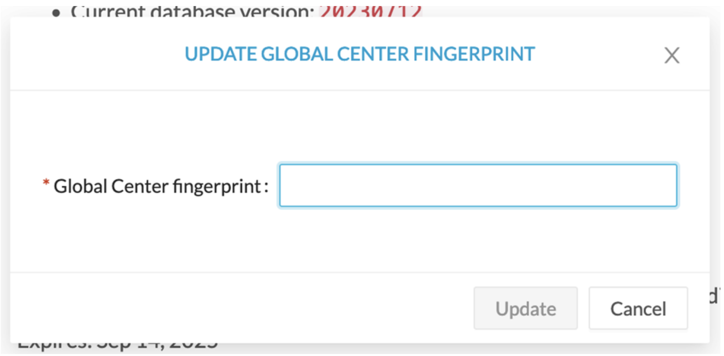
The KDB is managed by the global center, you cannot update it from this center.

Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894

Expires: Sep 14, 2025

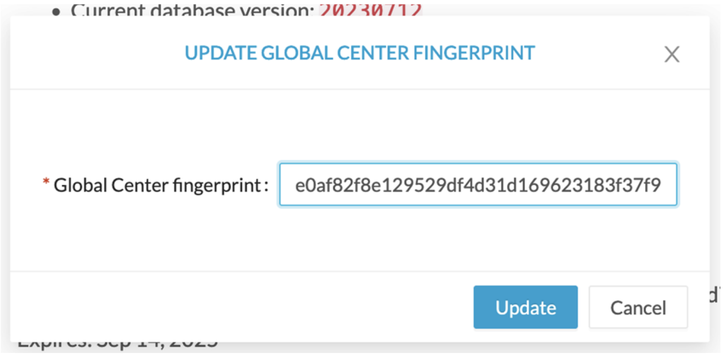
Center enrolled but disconnected, due to the update of the certificate of the Global Center.

The Update Global Center fingerprint window pops up.


• Current database version: 20230712
UPDATE GLOBAL CENTER FINGERPRINT
Update
Cancel
Expires: Sep 14, 2025

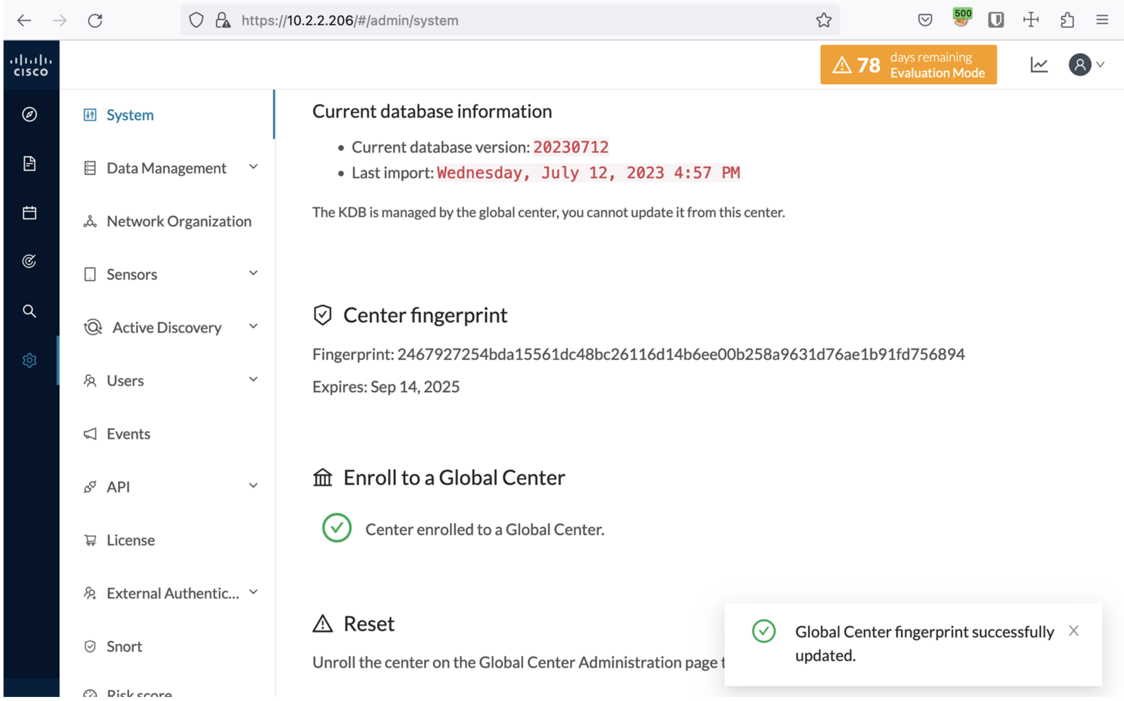
* Global Center fingerprint :

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


• Current database version: 20230712
UPDATE GLOBAL CENTER FINGERPRINT
Update
Cancel
Expires: Sep 14, 2025

* Global Center fingerprint : e0af82f8e129529df4d31d169623183f37f9

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



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

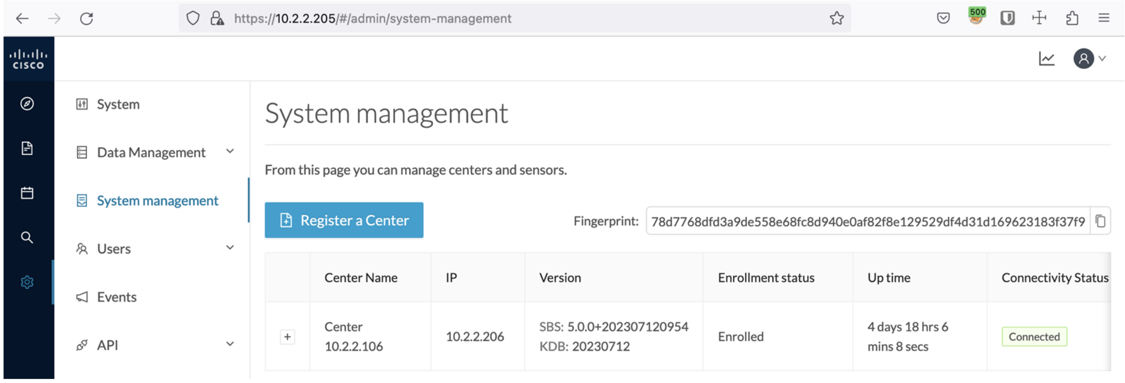
Center enrolled to a Global Center.

Reset

Unroll the center on the Global Center Administration page t

Global Center fingerprint successfully updated.

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



System management

From this page you can manage centers and sensors.

Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Enrolled	4 days 18 hrs 6 mins 8 secs	Connected

What to do next

Repeat the previous steps for each Center with sync.

Update a Center with sync fingerprint

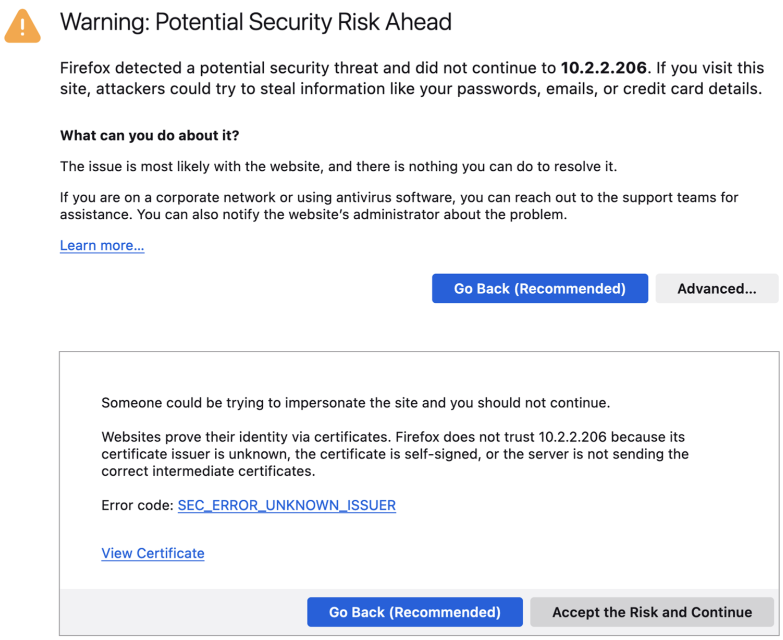
Before you begin

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.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.2.2.206**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more…

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 10.2.2.206 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

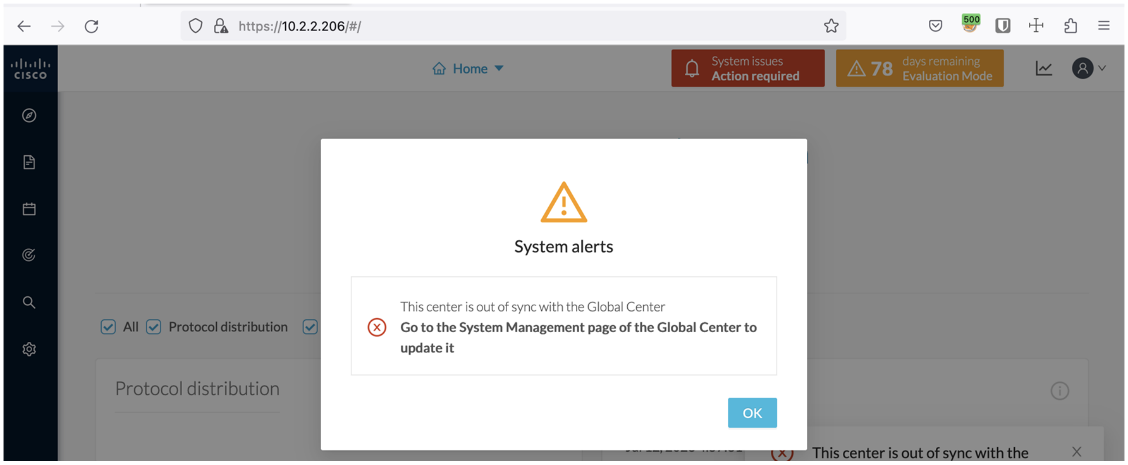
Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

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.



https://10.2.2.206/#/

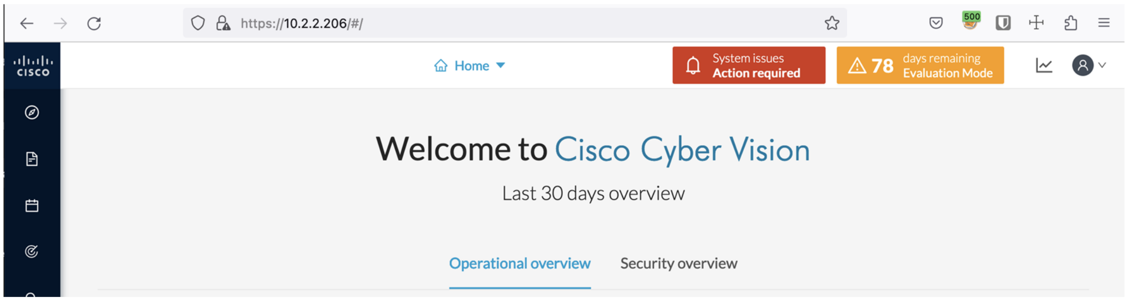
System alerts

This center is out of sync with the Global Center
Go to the System Management page of the Global Center to update it

This center is out of sync with the

Step 4 Click **OK**.

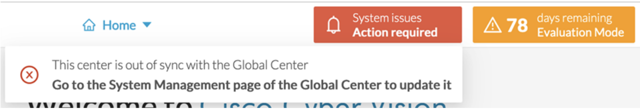
A red banner is displayed at the top of 's user interface.



Welcome to Cisco Cyber Vision

Last 30 days overview

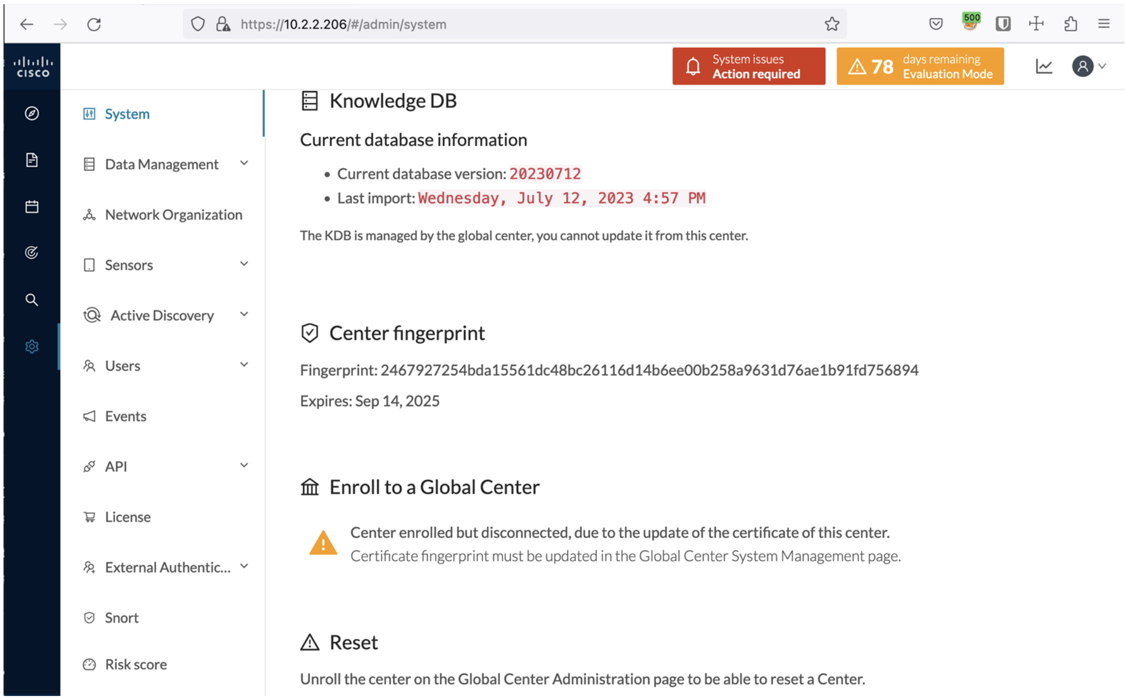
If you click the red banner, you will see the same message that appeared in the previous popup.



This center is out of sync with the Global Center

Go to the System Management page of the Global Center to update it

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



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

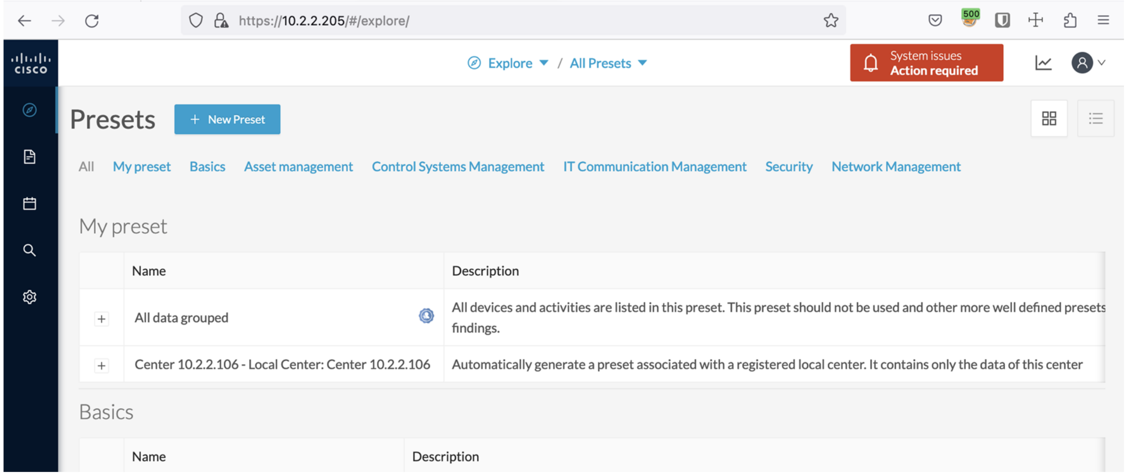
Enroll to a Global Center

Center enrolled but disconnected, due to the update of the certificate of this center.
Certificate fingerprint must be updated in the Global Center System Management page.

Reset

Unroll the center on the Global Center Administration page to be able to reset a Center.

Step 5 Access the **Global Center**.



Presets

All | My preset | Basics | Asset management | Control Systems Management | IT Communication Management | Security | Network Management

My preset

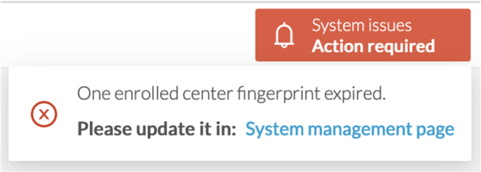
	Name	Description
+	All data grouped	All devices and activities are listed in this preset. This preset should not be used and other more well defined presets findings.
+	Center 10.2.2.106 - Local Center: Center 10.2.2.106	Automatically generate a preset associated with a registered local center. It contains only the data of this center

Basics

	Name	Description

Step 6 Click the red banner.

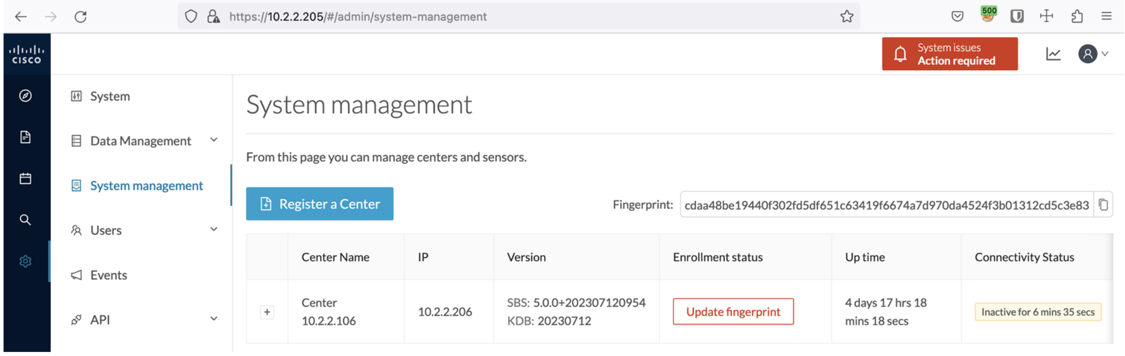
A message indicating that a Center fingerprint is expired is displayed with a shortlink to access the administration system management page.



One enrolled center fingerprint expired.

Please update it in: 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.



System management

From this page you can manage centers and sensors.

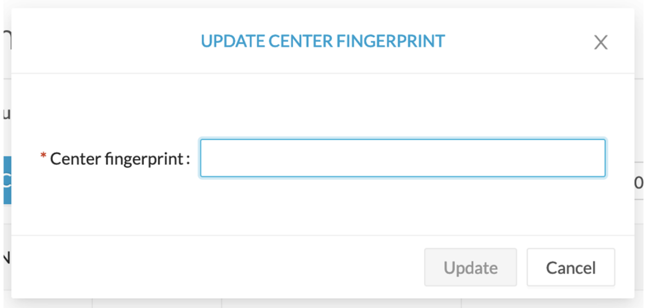
Register a Center

Fingerprint: cdaa48be19440f302fd5df651c63419f6674a7d970da4524f3b01312cd5c3e83

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Update fingerprint	4 days 17 hrs 18 mins 18 secs	Inactive for 6 mins 35 secs

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

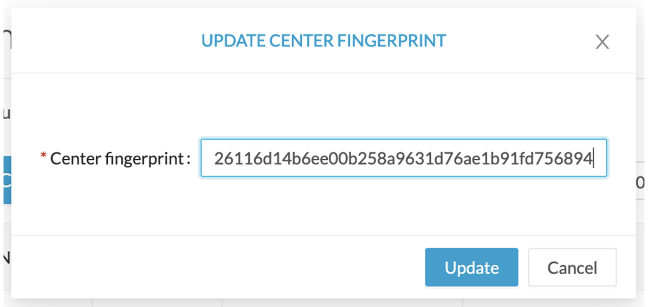
An Update Center fingerprint window pops up.



UPDATE CENTER FINGERPRINT

* Center fingerprint:

Step 8 Paste the Center fingerprint.

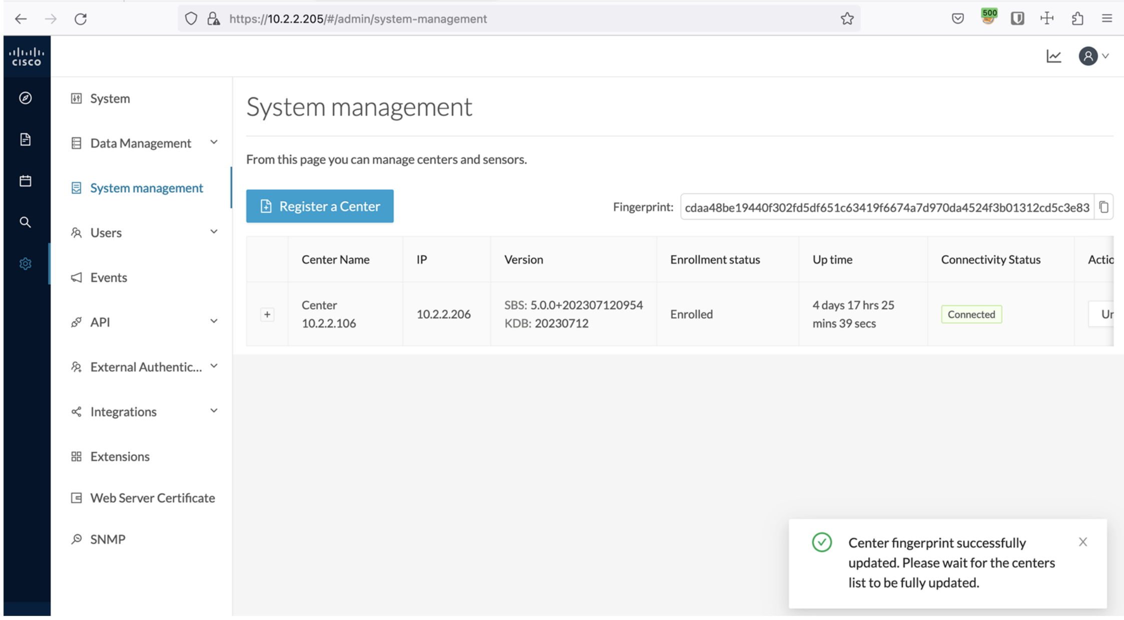


UPDATE CENTER FINGERPRINT

* Center fingerprint: 26116d14b6ee00b258a9631d76ae1b91fd756894

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.



https://10.2.2.205/#/admin/system-management

System management

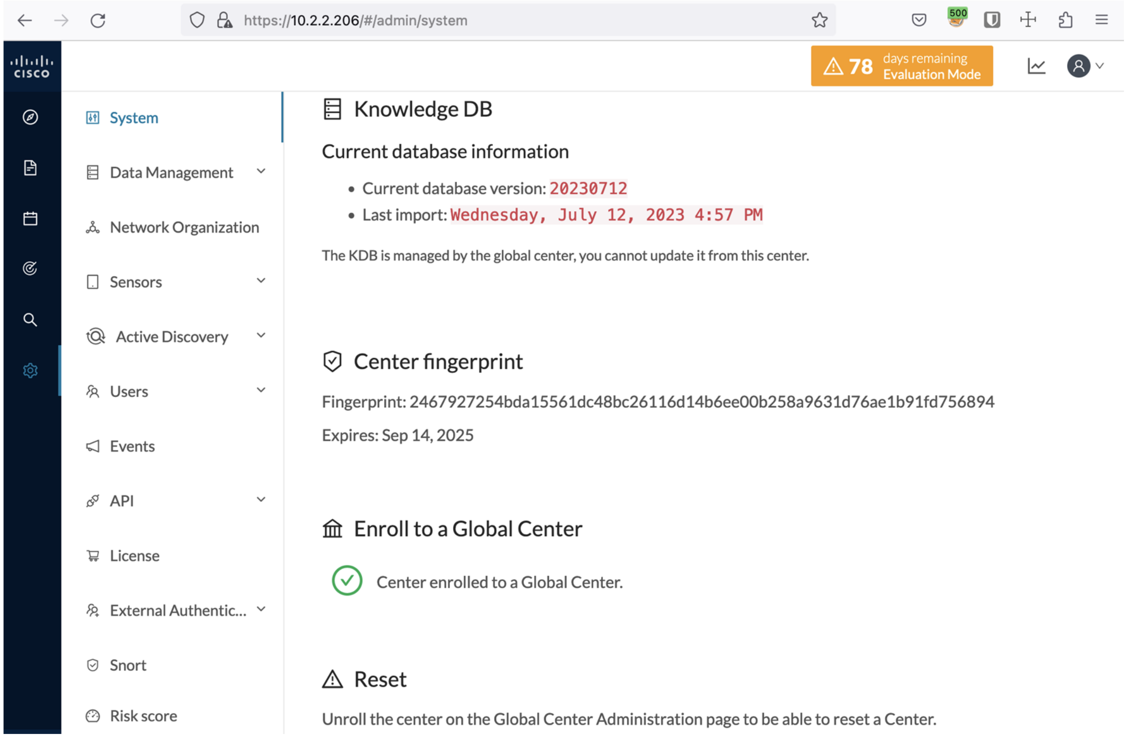
From this page you can manage centers and sensors.

Fingerprint: cdaa48be19440f302fd5df651c63419f6674a7d970da4524f3b01312cd5c3e83

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Actic
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Enrolled	4 days 17 hrs 25 mins 39 secs	Connected	Ur

Center fingerprint successfully updated. Please wait for the centers list to be fully updated.

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



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

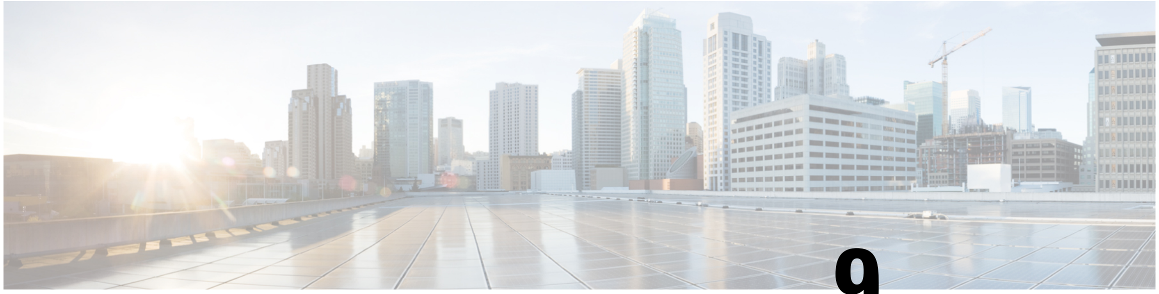
Expires: Sep 14, 2025

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

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

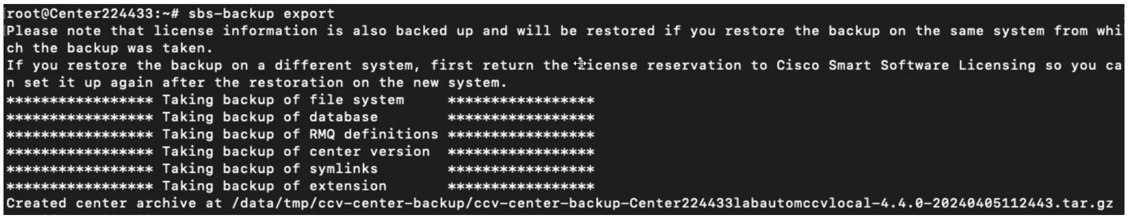
Procedure

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

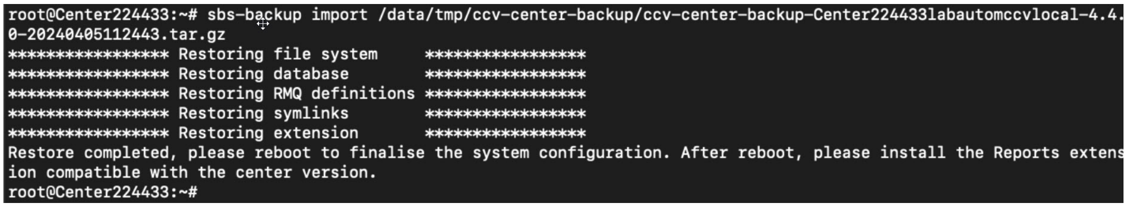
Copy the center backup file to the new center's **/data/tmp/ folder**.

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

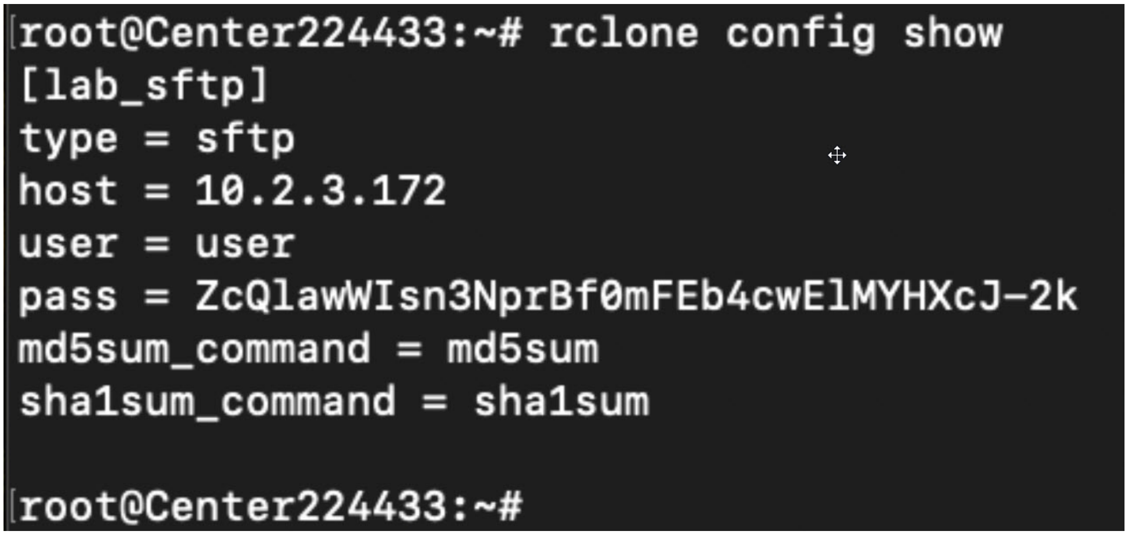
Step 1 To handle the complex authentication of object storage systems, rclone requires configuration due to the information being stored in a config file. The simplest way to create this config is by running rclone with the config option:

```
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'.`

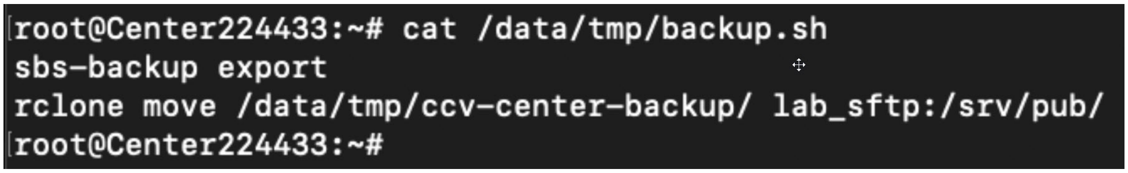
Bash Script

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/
```



```
root@Center224433:~# cat /data/tmp/backup.sh
sbs-backup export
rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
root@Center224433:~#
```

Cron

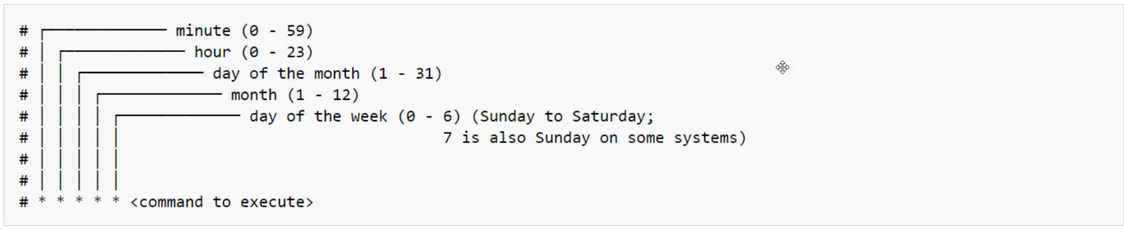
You can schedule a bash script using cron to back up Cyber Vision data and send the backup file to a remote drive.

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>
```