cisco.



Cisco Cyber Vision Center Appliance Installation Guide, Release 4.3.0

First Published: 2021-01-01 Last Modified: 2023-12-13

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 © 2019–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	About this documentation 1
	Document purpose 1
	Warnings and notices 1
CHAPTER 2	Information and characteristics 3
	Information and characteristics 3
CHAPTER 3	Connect the Center 7
	Connect an external device 7
	Connect interfaces for communication 7
	Power up the Center 8
CHAPTER 4	Configure the Center 9
	Basic Center configuration 9
	Access the basic Center configuration 10
	Accept the End User License Agreement 10
	Select the language to match your keyboard 11
	Select the Center type 11
	Center 12
	Global Center 13
	Configure the Center's Administration Network Interface 14
	Set interfaces (dual or single) 16
	Configure the Center's DNS 16
	Synchronize the Center and the sensors to NTP servers 16
	Give the Center a name 18
	Set the Center's password 18

	Configure the Center's Collection network interface 19
	Authorize networks 19
	Complete the basic Center configuration 20
	Cisco Cyber Vision configuration 21
	Install the certificate in your browser 21
	Install Cisco Cyber Vision 27
	Configure the user interface security 30
	Upload a p12 31
	Generate a CSR 33
	Configure Center data synchronization 35
CHAPTER 5	Configure a Center DPI 39
	Configure a Center DPI 39
CHAPTER 6	Configure the Cisco Cyber Vision Center synchronization 4
	Global Center Configuration 43
	Center enrollment 43
	Center unenrollment 46
	Force the unenrollement of a Center 47
	Force the unemonement of a Center 47
CHAPTER 7	Upgrade procedures 49
CHAPTER 7	
CHAPTER 7	Upgrade procedures 49
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49 Check the Global Center and Centers' health 49
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49 Check the Global Center and Centers' health 49 Update the Global Center 50
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49 Check the Global Center and Centers' health 49 Update the Global Center 50 Update the sensors 50
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49 Check the Global Center and Centers' health 49 Update the Global Center 50 Update the sensors 50 Update hardware sensors 50
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49 Check the Global Center and Centers' health 49 Update the Global Center 50 Update the sensors 50 Update hardware sensors 50 Update IOx sensors 51
CHAPTER 7	Upgrade procedures 49 Architecture with a Global Center 49 Check the Global Center and Centers' health 49 Update the Global Center 50 Update the sensors 50 Update hardware sensors 50 Update IOx sensors 51 Architecture with a single Center 52
CHAPTER 7	Upgrade procedures49Architecture with a Global Center49Check the Global Center and Centers' health49Update the Global Center50Update the sensors50Update hardware sensors50Update IOx sensors51Architecture with a single Center52Update the Center52

I

I

CHAPTER 8 Certificate renewal 55

Renew the certificate of a Center 55
Update the Global Center fingerprint 56
Update a Center with sync fingerprint 60

Contents



About this documentation

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

Document purpose

This installation guide shows how to connect, configure and install Cisco Cyber Vision 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 4.3.0.

Warnings and notices

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

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



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



Important In

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



Note

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



Information and characteristics

• Information and characteristics, on page 3

Information and characteristics

The Cisco Cyber Vision 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 Cisco Deep Packet Inspection engine and send meaningful information to the Cisco Cyber Vision Center.
- The Cisco Cyber Vision **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.

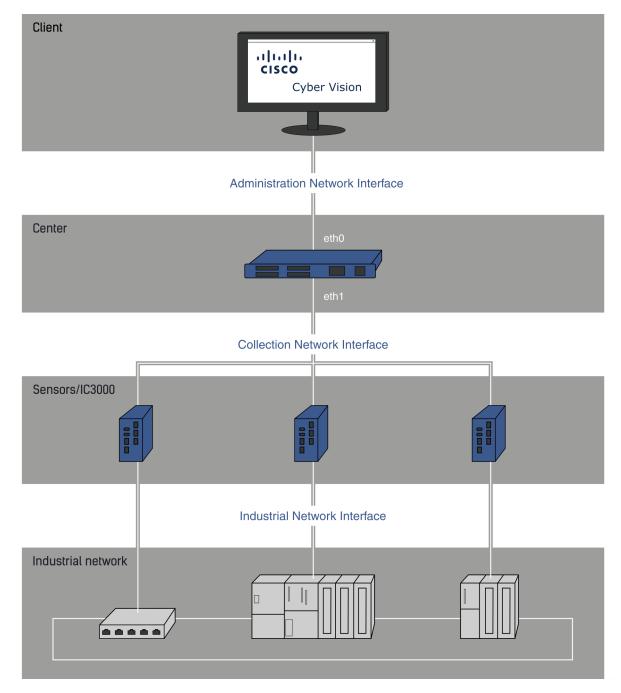
During the installation of the Center, you will have the opportunity to set up Center data synchronization to a Global Center. Although, if you choose to set up a global infrastructure, you must install the Global Center first, then the Centers, and finally, the sensors.

Networks or segments involved

From Cisco Cyber Vision 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 Cisco Cyber Vision 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).

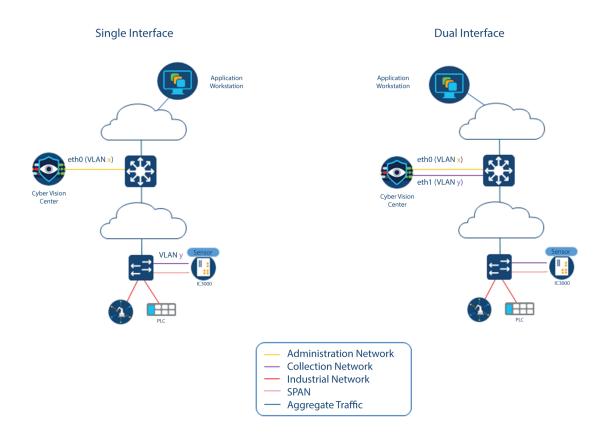
Example of a Cisco Cyber Vision installation (without Global Center):



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 Cisco Cyber Vision Architecture Guide for more information about defining Cisco Cyber Vision environment configuration.



Connect the Center

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

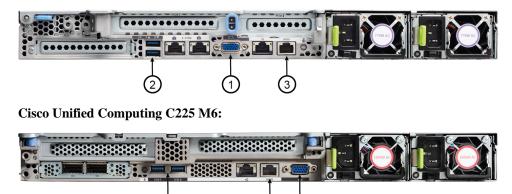
- Connect an external device, on page 7
- Connect interfaces for communication, on page 7
- Power up the Center, on page 8

Connect an external device

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

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

Cisco Unified Computing C220 M5:



Connect interfaces for communication

Cisco Unified Computing C220 M5:



Cisco Unified Computing C225 M6:

$\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$		

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.



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 Cisco Cyber Vision configuration, through a browser, to:
 - Create an admin account.
 - Configure the Center's data synchronization (Global Center and synchronized Centers only).
 - Basic Center configuration, on page 9
 - Cisco Cyber Vision configuration, on page 21

Basic Center configuration

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

Required information:

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

In the case of manual Administration network interface configuration:

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

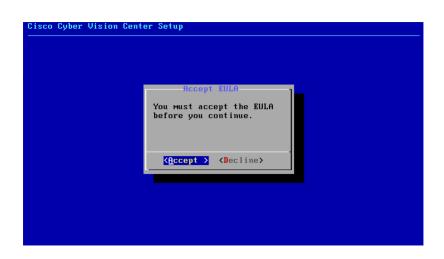
Access the basic Center configuration

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

Cisco Cyl	per Vision Center Setup
	Helcome This is the first boot of your Cisco Cyber Vision Center.
	<pre></pre>

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	
<u> </u>	
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: whw.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)	
188×	



Select the language to match your keyboard

Cyber Vision Cen	ter Setup	
Choose u	our keyboard Mapping.	
	IS American fr French	
	de German it Italian es Spanish	
	Cancel>	

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.

- gaster to to to to	Center Setup	
What tupe of	center do uou want to install?	1
What type of	center do you want to install?]
What type of	center do you want to install? Center Global Center Honitoring multiple centers	
What type of	Center Processing sensor data	
What type of	Center Processing sensor data Global Center Monitoring multiple centers	
What type of	Center Processing sensor data Global Center Monitoring multiple centers	

Center

If installing a Center, select the first option.

What type of	center do you want to install	?]
What type of]
What type of		ng sensor data	
What type of	Center Processi	ng sensor data	
What type of	Center Processi	ng sensor data	

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

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



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



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

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

Type the id into the basic Center configuration UUID field.

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.
<u>5</u> 64d1886-db38-bf9d-4235-f3c412f196d1
Cancel>

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

Global Center

If installing a Global Center, select the second option.



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

Are you trying to restore a Center and need to Manually set the center id ?
Ko > < Yes >

You will be directed to the next step.

Configure the Center's Administration Network Interface

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

The Administration network interface configuration can be done either:

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

co Cyber (Jision Center Setup
	Please select configuration type for the ACCESS interface HCP Automatic (DHCPv4) Manual Static IP and gateway
	Cancel>

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

• Manually:

Cisco Cyber Vision Center Setup	
Please select configuration type for the ACCESS interface	
DHCP Automatic (DHCPv4)	
Manual Static IP and gateway	
· · · · · · · · · · · · · · · · · · ·	
<pre>< OK <cancel></cancel></pre>	
Cisco Cyber Vision Center Setup 	
Setup Access Network Interface	
IP Address 10.2.3.182	
Netmask 24 Gateway 18.2.3.254	
188%	
< OK > <cancel></cancel>	

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

Set interfaces (dual or single)

This step is not applicable to a Global Center.

Regarding a Center, it is possible to:

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

o Cyber Vision C	enter setup
	<u> </u>
	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
	Cancel>

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

Configure the Center's DNS

Type a DNS server address and optional fallbacks.

Cisco Cyber Vision	Center Setup
	Setup DNS configuration Up to three Maximum, leave blank unnecessary fields Preferred 2008.67.222.222 Alt 1 2008.67.220.220 Alt 2 (DK) (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.

Please ent	er some NTP tim	e servers:	
		hronize the Cente rate correct cert	
server i ey ID and eparated ormat: se	s composed by i an AES 128 CMA by semicolon. rver_address[;k	ated by whitespac ts address and op C key value (32 h ey_id;key_value] use local time o	ntionally by a nex character)
10.2.3.25	4		
		(Cancel)	

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

Cisco Cyl	ber 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. 10.8.6.10:1:9:f6132554ad5a369370f08d536fa8fc9	
	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.

Time is a	юм: Tue Oct 29 16:37	7:43 2019 UTC	
	is incorrect, please 1DDhhmm[[CC]YY][.ss]]	specify current UTC tim)	e
Leave емј	oty or cancel to skip	p.	
-			
-			
	< 0K >	<cancel></cancel>	

Give the Center a name



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



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

Set the Center's password

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



Confirm the password.

Cisco Cyber Vision Cente	er Setun
	* 000kp
	Please confirm the cu-admin password
	-
	< OK > <cancel></cancel>

Configure the Center's Collection network interface

This step is not applicable to a Global Center.

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

Type the IP address of the Collection network interface:

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
	Cancel>

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.

on the adm	ministration inte	uthorized to contact erface. By default a work is: 192.168.72.	ll networks
		COMMa-separated.	0, 21
<u>0</u> .0.0.0/0	3		
	< 0K >	<cancel></cancel>	

Complete the basic Center configuration

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

Cisco Cyl	ber Vision Center Setup
	You can now connect your sensors on the dedicated network and power them on.
	You can download the self-signed CA at: http://10.2.3.102/ca.crt
	To finish the setup press OK to reboot then use your Web browser and go to: https://10.2.3.102/

Enter OK to finish the basic Center configuration.





Note A major change regarding the Center command line (CLI) access through serial console or SSH was made in Cisco Cyber Vision version 4.1.0. The user root is no longer usable to establish the connection. A new user called 'cv-admin' must be used. This user has limited rights and many CLI commands will require permission elevation:

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

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

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



Note

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

Cisco Cyber Vision configuration

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

- If you plan to use a self-signed certificate, you must Install the certificate in your browser, on page 21 and then access the Install Cisco Cyber Vision 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 Install Cisco Cyber Vision to configure users and sensors.
- 2. Configure the user interface security itself.

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

Browser requirements:

Cisco Cyber Vision 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 Cisco Cyber Vision, on page 27.

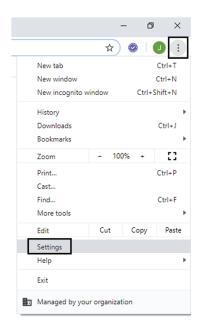
Procedure

- **Step 1** Open your browser.
- Step 2
 Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.

The certificate is downloaded.

- **Step 3** Save the certificate on your computer.
- **Step 4** In the browser, access the settings.

Example: Chrome



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

Q certificate	8
ivacy 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 <mark>certificate</mark> s Manage HTTPS/SSL <mark>certificate</mark> s and settings	Z
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.

I

Issued To	Issued By	Expiratio	Friendly Name	
Qualitizational -	Address Driverski CA.	3,01,213	Section (Address)	
whatevers Cyber Tru-	fallmare CyberTrust -	12000	Deploy 1 Ballener -	
Carbon CA	Certure CA	11,000,0017	Certure	
Cartue Trusted No.	Cartue Trusted Netwo	10102	Centure Trusted -	
Caro Real CA 2148	Case Reat CA 2048	1400.000	-Charter -	
Caro Real (A.W)	Caso Reat (A.W)	ALC: NO.	-Charter -	
Case Real (A.W)	Caso Real (A.M)	ALC: NO.	-Charge -	
Caro Real (A H)	Caso Reat (A H)	12112	-Charter -	
- Case Rec. R.L.	Caso RHC RU		Contra 2	•
			ing, Time	/ance

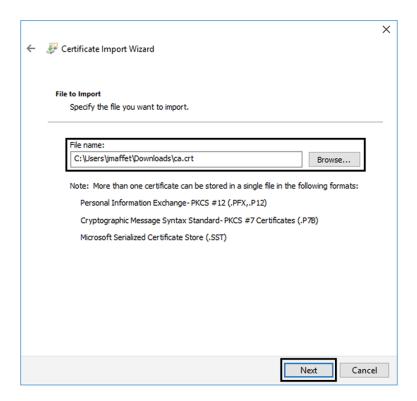
A certificate importation wizard opens.

Step 7 Go to the next step.



Step 8 Search for the certificate you downloaded earlier.

Step 9 Go to the next step.



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

Certificate Store				
	stores are system a	areas where certi	ficates are kept.	
Windows ca the certifica		ect a certificate s	tore, or you can spec	cify a location fo
Auto	matically select the	certificate store	based on the type of	certificate
Place	all certificates in th	ne following store		
Cert	ificate store:			_
Tru	sted Root Certificat	tion Authorities		Browse

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	
Finish	Cancel

What to do next

Install Cisco Cyber Vision, on page 27

Install Cisco Cyber Vision

Access the Cisco Cyber Vision installation wizard:

Procedure

Step 1	With yo	ur browser, access https:// <centername>/.</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 setu	p wizard used for the first access to Cisco Cyber Vision is displayed:
Step 3	Create	an admin account:

-		
Create the first user	$\overline{\mathbb{P}}_{\mathbb{R}}^{\mathbb{N}}$ Agree to the license terms	(√) Done
Firstname :	Lastname [*] :	
Email :		
Password :	Confirm password :	
Suggested password: \$kvIH2Qq*odz90fj0E3	OC	

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:

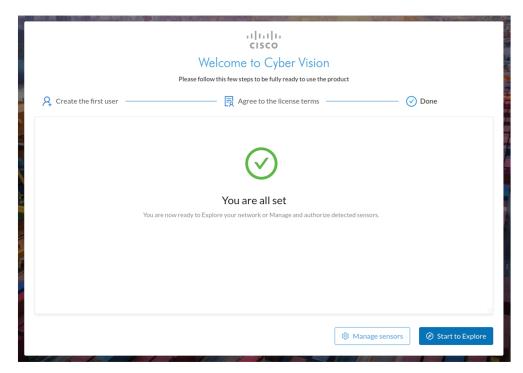
	cisco	
	Welcome to Cyber Vision	
	Please follow this few steps to be fully ready to use the product	
Create the first user	Agree to the license terms	⊘ Done
End User License Agreement		
Effective: May 22, 2017		
Software. "You" and "Your" means	and Cisco Systems, Inc. or its affiliates ("Cisco") the individual or legal entity licensing the Softwa .1, activate, access or otherwise use the Software.	are under this EULA. "Use" or
Software. "You" and "Your" means "Using" means to download, instal computer programs and any Upgrade "Documentation" is the Cisco user applicable to the Software and ma (ii) the Cisco authorized reselle "Entilement" means the license d (PID) published on Cisco's price	the individual or legal entity licensing the Softwa	are under this EULA. "Use" or "Software" means the Cisco licensed to You by Cisco. cations or other documentation ed Source" means (i) Cisco or acquired the Software. nity provided in a product ID on. "Upgrades" means all
Software. "You" and "Your" means "Using" means to download, instal computer programs and any Upgrade "Documentation" is the Cisco user applicable to the Software and ma (ii) the Cisco authorized reselle "Entitlement" means the license d (PID) published on Cisco's price updates, upgrades, bug fixes, err copies thereof. Table of Contents	the individual or legal entity licensing the Software. 1, activate, access or otherwise use the Software. Is made available to You by an Approved Source and D or technical manuals, training materials, specific de available to You by an Approved Source. "Approve r, distributor or systems integrator from whom you letail; including license metric, duration, and quar list, claim certificate or right to use notification	are under this EULA. "Use" or "Software" means the Cisco licensed to You by Cisco. cations or other documentation ed Source" means (i) Cisco or acquired the Software. nity provided in a product ID on. "Upgrades" means all

Step 7

Step 8 Finish the installation:

The Center is now correctly installed and Cisco Cyber Vision is ready to operate.

Step 9 Click Start to Explore.



Cisco Cyber Vision installation is now complete.

What to do next

If you aim to use an enterprise certificate, proceed with Configure the user interface security, on page 30.

If you already installed a self-signed certificate, and if you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 35.

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

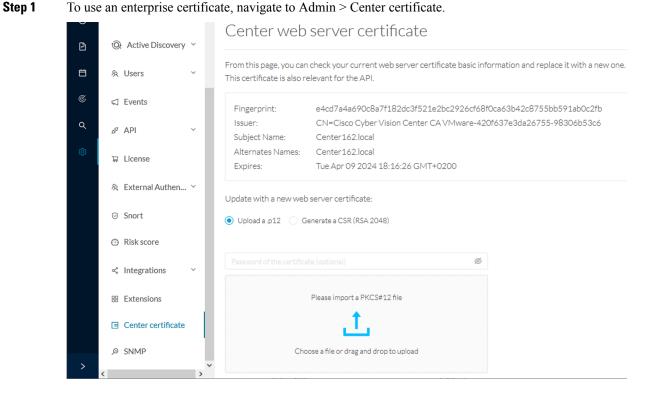
Configure the user interface security

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



L

Step 2 You can Upload a p12 orGenerate a CSR.

Upload a p12

Before you begin

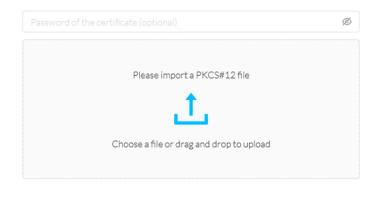
The p12 (or Microsoft pfx) file must contain a private key, a password, and the field "X509v3 Subject Alternative Name" must contain the Center DNS name.

Procedure

Step 1 Select Upload a .p12.

Update with a new web server certificate:





🗟 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.

C Reload

•••••	ø	
E	3	
File selected: CenterAD2	019.2019lab.local1.pfx	
		🖻 s
k Save.		2

Step 5 Click Reload.

Step 4

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.

	~ c	enterad2019.2019lab.local/#/ac	dmin/cer	nter-ce	ertificate
<	cen	terad2019.2019lab.local		×	
		Connection is secure		۲	
	٩	Cookies	2 in use	Z	
	٥	Site settings		Ľ	1

What to do next

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

If you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Cisco Cyber Vision 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)	
		Generate and download CSR
Step 2 Step 3	Enter the Center FQDN as registered on your DNS server. 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	
		Generate and download CSR
	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		
i 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		
	Discard	🐻 Save

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.

	ith a new web server certificate: la.p12 () Generate a CSR (RSA 2048)	
i	CSR has been generated. Please import the certificate.	
	CenterAD2019.2019lab.local download	
	File selected: CenterAD2019.2019lab.local.crt	
		🗋 Discard 🛽 🗴 Save



The following message appears:



Step 8 Click Reload.

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

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

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

 centerad2019.2019lab.local
 ×

 Connection is secure
 •

 Cookies
 2 in use

 Site settings
 2

What to do next

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

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

Configure Center data synchronization

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

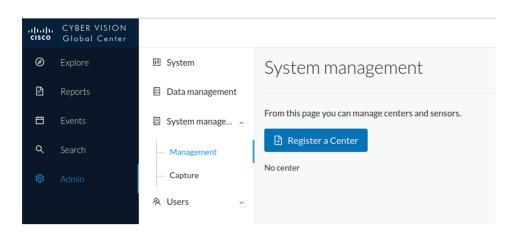
Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists of registering the Center in the Global Center and enrolling the Center to the Global Center. To do so, you need to open each's Cisco Cyber Vision's GUI.



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

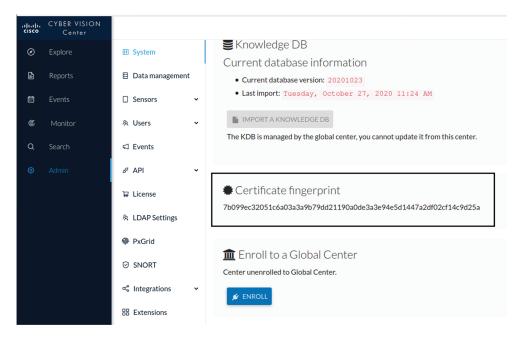
Procedure

Step 1In the Global Center's Cisco Cyber Vision GUI, navigate to Admin > System Management > Management.Step 2Click the Register a Center button.

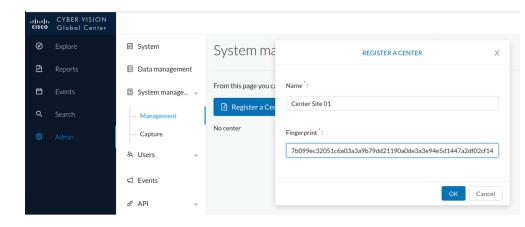


The window "Register a Center" pops up, ready to be filled. Now you must access the Center's GUI to retrieve its fingerprint.

- **Step 3** In the Center's Cisco Cyber Vision GUI, navigate to Admin > System.
- **Step 4** Scroll down to Certificate fingerprint and copy it.



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



Step 6

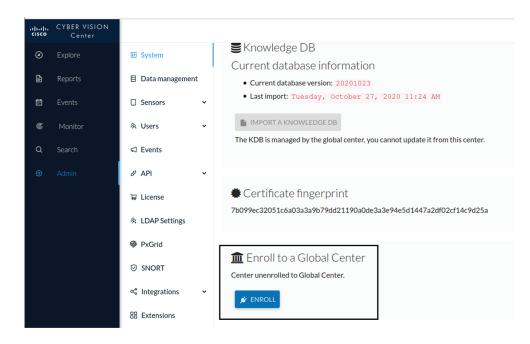
field Click OK.

The Center appears in the list as unenrolled.

 cisco	CYBER VISION Global Center										
Ø	Explore	년 System	System manag	emen	t						
Ð	Reports	Data management									
Ħ	Events	System manage ^	From this page you can manage centers and sensors.								
۹	Search	— Management	Register a Center								
\$	Admin	— Capture	Name	IP	Version	Status	Processing Status				
		冬 Users 🗸	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.



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 browser is the same time.	not refresh
Global Center Ingerprint - 	ac5fac7513126
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.



Configure a Center DPI

• Configure a Center DPI, on page 39

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 Cisco Cyber Vision sensors administration page.

.ili.ili. cisco		<u>₩</u> ⊗ -
Ø	E System	Sensors
۵	目 Data Manage 🗸	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.
	& Network Organization	
¢	Sensors	No sensors found.
Q	- Sensors	Please check the following:
۵	- Capture	Sensor(s) are powered on Sensor(s) are connected to the same network as the Center 'COLLECTION' interface.
	冬 Users 🗸 🗸	AMANAGE CREDENTIALS
	IA DI	

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



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

In the case if a dual interface, select eth2.

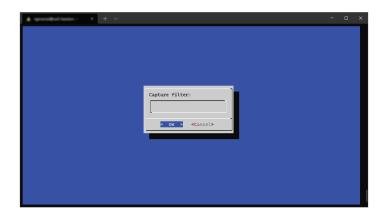
× + ~		-	×
	Network-configuration		
	Please select an interface to configure: eth0_3C:57:31:ff:10:de Eth1_Ec:57:531:ff:10:df		
	< OK > <cancel></cancel>		

Step 4 Select the interface as DPI+Snort port.

* ×	+ ~	-	۵	×
	Configuring-eth1			
	Please select configuration type: Manual Static IP and gatemay DHCP Automatic (DHCPW) Bridge Add to 555 bridge Pleasnort port Set ethi as DPleasnort interfae			
	< OK → <cancel></cancel>			

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

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



For example, you can type "not arp".

× + ~	- 0	×
	Capture filter:	
	not arp	
	< OK > <cancel></cancel>	

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

I System	Sensors							
Data Manage Å Network Organiz	and securely rebooted, s				packages to deploy Cisco Cyb nust authorize it so the Cente		sors. Sensors can also	be remo
Sensors Sensors	• Name	IÞ	Version	Status	Processing status	Active Discovery status	Capture Mode [♥]	Uptir
 Capture 	✓ CENTER-ETH1	N/A	N/A	Running	Waiting for data	Unavailable	not arp	N/A
条 Users	Name: CENTER-ET	C114 A						
	Status: Running							
& API	 Processing status: Active discovery: 					Û	"C	
₩ License	Deployment: Auto Capture mode: not • Start recording s	arp				Remove	Capture Mode	Disable IDS
ℜ LDAP Settings								
⊖ Snort					MANAGE CREDENTIALS	LUPDATE CISCO DEVIC	+ DEPLOY CISC	O DEVIC
Risk score					+ 0	NSTALL SENSOR MANUA	LLY DIMPORT OF	FLINE FIL

I



Configure the Cisco Cyber Vision Center synchronization

• Global Center Configuration, on page 43

Global Center Configuration

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

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

Enrollment and unenrollement will be described below.

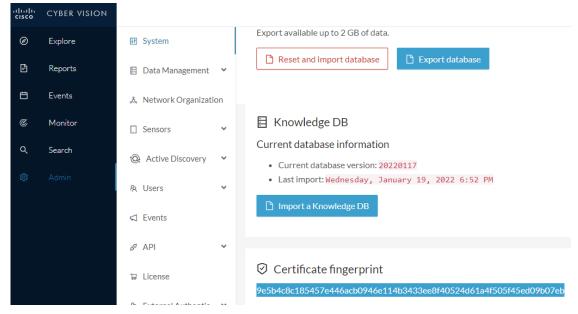
Center enrollment

Before you begin

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

Procedure

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



- **Step 2** Move to the Global Center user interface, Admin menu, in the **System management**, navigate to the **Management** menu. Click on the button **Register a Center** and:
 - a) Fill the Name field with the name you would like to have for this center
 - b) Paste the Certificate fingerprint copied above

ıılıılı cısco	CYBER VISION Global Center			
Ø	Explore	₩ System	System managem	REGISTER A CENTER X
Ē	Reports	🗐 Data Management 🛛 💙	From this page you can manage cer	
Ħ	Events	System management	Register a Center	Name : My Center 01
م	Search	— Management		Fingerprint : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61
ø		첫 Users 🗸 🗸		OK Cancel
		🖾 Events		OK Calice

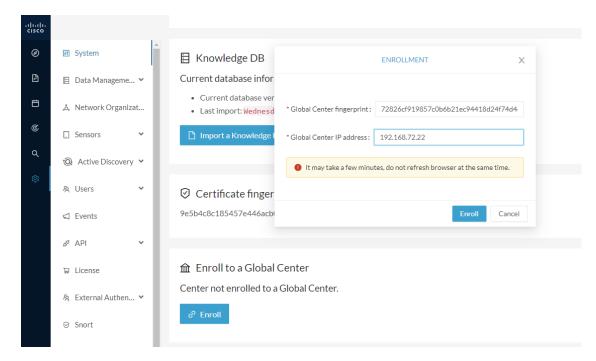
Step 3 Stay in the Global Center, on the same menu (Admin - System management - Management) and copy the Fingerprint of the Global Center.

System management

From	From this page you can manage centers and sensors.						
Ð	Register a Center			Fingerprin	nt: 72826cf919857c0b6b21ec9	94418d24f74d4d2cf2bc742e76844	4554078abaa0c
	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
	My Center 01			Registered		Notenrolled	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



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	Х
r er d	S Enrollment succeeded.	
a	 Connection test with global center 192.168.72.22 succeeded Calculated size of data to transfer: 78.6 kB Synchronization started 	
r bi	Data is being synchronized with the global center. You can follow synchronization progress on Admin page.	
al C	Lenter	ок

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

	is page you can manage egister a Center	e centers :	and senso	rs.		Fir	gerprint: 72	826cf	f919857c0b6b21ec94418	3d24f7	4d4d2cf2bc742e7684	14554078abaa0c
	Center Name	IP		Version		Enrollment state	ıs	Up	time	Con	nectivity Status	Action
-	My Center 01	192.16	8.72.21	SBS: 4.1.0+2 KDB: 20220	202201171404 1117	Enrolled		5 d sec	lays 16 hrs 52 mins 12 cs	Con	inected	Unenroll
	Sensor Name		IP		Version		Status		Processing Status		Capture mode	Up Time
	Sensor My Sensor 1		192.168	69.21	4.1.0+202201	171423	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.

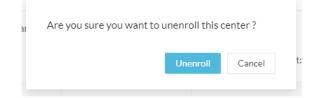
Step 2 Click Unenroll on the Center required.

System management

From th	nis page you can manag	e centers and senso	rs.				
₽ R	legister a Center			Fingerprint: 7	2826cf919857c0b6b21ec9441	8d24f74d4d2cf2bc742e768444	554078abaa0c 🗓
	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.



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.

L

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.

Register a Center			Fingerpri	int: 72826cf919857c0b6b21ec	94418d24f74d4d2cf2bc742e76844	4554078abaa0c
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.

0			
51	/ctom	management	
\mathcal{I}	JULIII	management	

From th	From this page you can manage centers and sensors.						
₽ R	Register a Center			Fingerprint:	72826cf919857c0b6b2	lec94418d24f74d4d2cf2bc74	2e768444554078abaa0c
	Center Name	IP	Version	Enrollment status	Uptime	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



Upgrade procedures

- Architecture with a Global Center, on page 49
- Architecture with a single Center, on page 52

Architecture with a Global Center

Check the Global Center and Centers' health

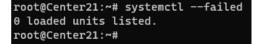
It is highly recommended that you check the health of the Centers connected to the Global Center and of the Global Center itself before proceeding to the update. To do so:

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.



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 Cisco Cyber Vision application or using its Command Line Interface.

To update the Global Center:

- Through the Cisco Cyber Vision 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 Cisco Cyber Vision 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</version>
Step 2	Launch the update using the following command: sbs-update install /data/tmp/CiscoCyberVision-update-sensor- <version>.dat</version>

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 Cisco Cyber Vision, 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 Cisco Cyber Vision application or using its Command Line Interface.

- Through the Cisco Cyber Vision application:
- 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):
- 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</version>
Step 2	Launch the update using the following command:
	sbs-update install /data/tmp/CiscoCyberVision-update-sensor- <version>.dat</version>

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</version>				
Step 2 Step 3	In Cisco Cyber Vision, navigate to Admin > Extensions. 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 Step 5	Navigate to Admin > Sensors > Sensor Explorer. 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</version>				

- 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

I



Certificate renewal

The certificates generated by Cisco Cyber Vision have a validity of two years.

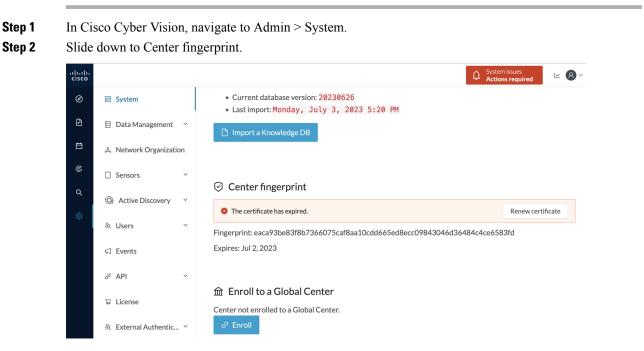
Certificates renewal should be automatic. However, manual procedures to renew the Global Center certificate and Centers with sync exist in case automatic ones are not possible.

• Renew the certificate of a Center, on page 55

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



A message indicates that the certificare has expired.

I

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.					
	Go Back (Recommended) Advanced					
	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					
	Go Back (Recommended) Accept the Risk and Continue					

- 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.

$\leftarrow \rightarrow$	C	🔿 🔒 https:/	/10.2.2.20	5/#/admin/system-mar	agement	ۍ ۲		500	Ŧ	മ ≡			
.ılı.ılı. cısco									~	8 ~			
Ø	টা System		Syst	em manage	ement								
8	🗄 Data Man	agement 🗠	From th	rom this page you can manage centers and sensors.									
Ë	🗵 System ma	anagement	F R	egister a Center	Fingerprint: 78d77	'68dfd3a9de558e68fc8d940e0a	f82f8_129529df	443141696	23183	f37f9			
۹	冬 Users	~			00010027003300001001740002	10210012732701	403101070	201001	5/1/ 1				
¢	⊲ Events			Center Name	IP	Version	Enrollment sta	atus		Up time			
	_ଣ API	~	+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated glob			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 th	is page you can manage	e centers and sense	ors.		
🗈 R	egister a Center		Fingerprint:	78d7768dfd3a9de558e68	3fc8d940e0af82f8e129529df4d31d169623183f37f9
	Center Name	IP	Version	Enrollment status	Up time The center needs to be informed of
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated global center fingerprint ()	the new fingerprint of the Global Centers: 17 hrs 37 mins 39 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.

$\leftarrow \ \ \rightarrow$	C https://10.2.2.206/#/			\$	⊽ 👺 🚺	• +	ഫ ≡
uluilu cisco		ŵ Home ▼	System issues Action required	▲ 78	days remaining Evaluation Mode	~	8~
Ø							
£							
8		\triangle					
C		System ale	erts				
۹		The Global Center fing					
ŵ	All Protocol distribution	Please update it in: S	ystem page				
	Protocol distribution		ОК	Clabelo			
			Jul 12 2023 4-5	e Global C cnanged	enter fingerprint	has	×

Step 7 Click OK.

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

$\leftarrow \rightarrow$	C 🗘 https://10.2.2.206/#/		\$	S 🎆 🚺	Ŧ	එ ≡			
uluilu cisco	l Home ▼	System issues Action required	▲ 78	days remaining Evaluation Mode	~	8 ~			
Ø									
ß	Welcome to C	Cisco Cyber Visic	on						
Ħ	Last 30 days overview								
¢	Operational overv	iew Security overview							
Q ¢	 ✓ All ✓ Protocol distribution ✓ Most critical events ✓ Presets highlight 								
	Protocol distribution	Most critical events							

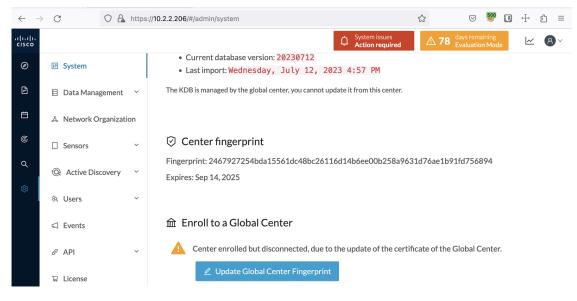
If you click the red banner, you will see the same message that appeared in the previous popup, with a link to the System page to update the Global Center fingerprint.

¢	System issues Action required	∆ 78	days remaining Evaluation Mode				
	The Global Center fi	ngerprint ha	as changed				
(\times)	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.



The Update Global Center fingerprint window pops up.

Current database version: 20230712 UPDATE GLOBAL CENTER FINGERPRINT							
* Global Center fingerprint :							
Update Cano	el d'						



Paste the Global Center fingerprint and click Update.

Current database vers	ion: 20230712						
UPDATE GLOBAL CENTER FINGERPRINT							
* Global Center fingerprint :	eOaf82f8e129529df4d31d169623183f37f9						
LAPII 63, JUP 17, 2023	Update Cancel						

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

\leftarrow	\rightarrow	C C) 🔒 https:,	//10.2.2.206/#/admin/system		☆	ତ 💱		\oplus	ර =
.ılı.ılı. cısco						▲ 78 day Ev	/s remaining aluation Mod	e	~	8 ~
Ø		₩ System		Current database information						
F		🗄 Data Manager	ment ~	 Current database version: 20230712 Last import: Wednesday, July 12, 2023 4:57 PM 						
Ë		ిం, Network Orga	anization	The KDB is managed by the global center, you cannot update it from this	center.					
C		. Sensors	~							
Q		Q Active Discov	very ~	Center fingerprint						
\$		糸 Users	~	Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b Expires: Sep 14, 2025	0258a963:	1d/6ae1b91fc	1/56894			
		⊲ Events								
		a ST API	~	命 Enroll to a Global Center						
		₩ License		Center enrolled to a Global Center.						
		条 External Auth	entic ~							
		⊙ Snort		▲ Reset Unroll the center on the Global Center Administration page t	\sim	lobal Center fi odated.	ngerprint s	ucces	sfully	×
		@ Dick core								

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

\leftarrow	\rightarrow	C	O 🔓 htt	ps://10.2.2	.205/#/admin/syste	m-management	\$	☆ 🛛 🐺 🚺 🕂 원 🗏						
cisco										<u>~</u> 8 ·				
Ø		₩ System		Syst	em mana	gement								
£		🗏 Data Manage	ement ~	From this page you can manage centers and sensors.										
Ħ		System mana	gement	₽ R	Register a Center Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9									
α		冬 Users	~											
		⊲ Events			Center Name	IP	Version	Enrollment status	Up time	Connectivity Status				
		S API	~	+	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

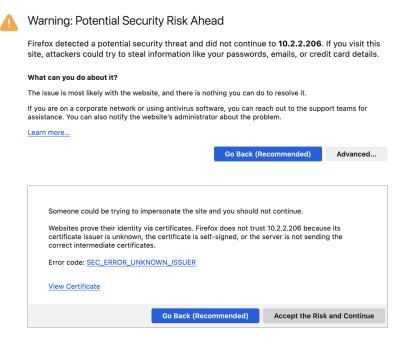
You need access to the Center with sync and its Global Center.

Procedure

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

This warning page indicates that the certificate has been renewed.

I



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.

$\leftarrow \ \ \rightarrow$	C A https://10.2.2.206/#/			☆	. 😌 🔤		Ε	ງ ≡
.ı ı.ı ı. cısco		☆ Home ▼	System issues Action required		78 days remaining Evaluation Mode		~	8~
Ø	_							
Ē.								
Ħ								
C		System alerts						
۹	All Protocol distribution	This center is out of sync with the Global Center Go to the System Management page of the Glo	abal Center to					
礅		update it						
-	Protocol distribution		ок					
		201 mij m	(x)	This ce	nter is out of sync wit	h the		×

Step 4 Click OK.

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

I

$\leftarrow \ \ \rightarrow \ \ \mathbf{G}$	○ A https://10.2.2.206/#/	۲3 ۲	?	\bigtriangledown	500	\pm	ර	≡
cisco	Home Home System issues Action required		∆ 78	days rema Evaluatio	aining <mark>n Mode</mark>	~	٩	×
Ø								
₽.	Welcome to Cisco Cyber Vision							
H	Last 30 days overview							
C C	Operational overview Security overview							

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

	☆ Home ▼	¢	System issues Action required	∆ 78	days remaining Evaluation Mode
\otimes	This center is out of sync with the Global Center Go to the System Management page of the G		enter 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.

$\leftarrow \rightarrow$	C C http	s://10.2.2.206/#/admin/system 🟠 🖂 🐨 💟 🕂 🖞 =
.ılı.ılı. cısco		Q System issues Action required ▲ 78 days remaining Evaluation Mode ∠ ⑧
Ø	<section-header> System</section-header>	E Knowledge DB
F	目 Data Management 💙	Current database information Current database version: 20230712
Ë	هُ، Network Organization	Last import: Wednesday, July 12, 2023 4:57 PM The KDB is managed by the global center, you cannot update it from this center.
¢	. Sensors 🗸	The KOD is managed by the global center, you cannot update it form this center.
ব গ্রু	ⓐ Active Discovery ↔	⊘ Center fingerprint
~	糸 Users ~	Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894
	⊲ Events	Expires: Sep 14, 2025
	ഴ്API ∽	爺 Enroll to a Global Center
	'긒 License	Center enrolled but disconnected, due to the update of the certificate of this center.
	糸 External Authentic ゞ	Certificate fingerprint must be updated in the Global Center System Management page.
	⊙ Snort	
	② Risk score	\triangle Reset Unroll the center on the Global Center Administration page to be able to reset a Center.

Step 5 Access the **Global Center**.

\leftarrow	C	O A https://10.2.2.205/#/explor	e/		ŝ	v 🦉	U	Ŧ	එ ≡
.ı ı.ı ı. cısco					¢	System issues Action required		~	8~
Ø	Pres	ets + New Preset						88	:=
£.	All N	ly preset Basics Asset management Cont	rol Syst	ems Management IT Communication Management Securi	ty Networ	rk Management			
Ħ	Mv n	reset							
۹	, թ								
~		Name		Description					
ŝ	+	All data grouped	٥	All devices and activities are listed in this preset. This preset shiftings.	hould not be u	used and other mor	re well	defined	presets
	+	Center 10.2.2.106 - Local Center: Center 10.2.	2.106	Automatically generate a preset associated with a registered l	ocal center. I	t contains only the	data of	this ce	nter
	Basic	S							
		Name	Desc	iption					

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.

	System issues Action required
\otimes	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.

$\leftarrow \rightarrow$	С	C) 🔓 ht	ttps:// 10.2 .	.2.205/#/admin/syste	m-management				☑ 💱	•	එ ≡
uluilu cisco										m issues n required	Ŀ	⊻ 8 ×
Ø	₩ S	ystem		Syst	em manag	ement						
Ē	Data Management From this page you can manage centers and sensors.											
Ħ	E S	ystem managemer	nt	🗄 Re	egister a Center		Fingerpri	nt: cdaa48be19440f302fd5df6	51c63419f6674a7d97	0da4524f3l	p01312cd	5c3e83
٩	ΑU	lsers	~									
\$	⊲ E	vents			Center Name	IP	Version	Enrollment status	Up time	Conn	ectivity St	atus
	s ^g A	PI	~	+	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	Inact	tive for 6 mi	ns 35 secs

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

An Update Center fingerprint window pops up.

٦		UPDATE CENTER FINGERPRINT	×
u	* Center fingerprint :		
٦		Update Cancel	

Step 8 Paste the Center fingerprint.

٦		UPDATE CENTER FINGERPRINT	<
u	* Center fingerprint :	26116d14b6ee00b258a9631d76ae1b91fd756894]
١		Update Cancel	

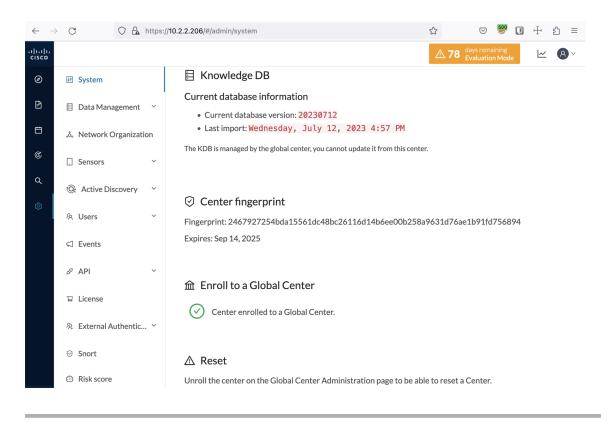
A message indicating that the Center fingerprint successfully updated appears.

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

0

$\leftarrow \rightarrow$	C OA	https://10.	2.2.205/#/admin/syste	em-management			â	S 🙈 T 🕂	ර =
uluilu cisco								~	8 ~
Ø	If System	Sys	tem manag						
£	🗐 Data Management 🗠	From t	his page you can mana	age centers and s	ensors.				
Ë	System management	- F1 F	Register a Center		Fingerpi	int: cdaa48be19440f30	2fd5df651c63419f6674a	7d970da4524f3b01312cd5c	3e83 🕅
۹	冬 Users ~								
\$	⊲ Events		Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Actic
	م مر	+	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
	ℜ External Authentic Υ								
	« Integrations ~								
	器 Extensions								
	Web Server Certificate								
	,∞ SNMP						<u> </u>	erprint successfully ease wait for the centers y updated.	×

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



I