



Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.4.0

First Published: 2021-01-01

Last Modified: 2023-12-21

Americas Headquarters

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



CONTENTS

CHAPTER 1

About this documentation 1

Document purpose 1

Warnings and notices 1

CHAPTER 2

Getting started 3

Overview 3

Prerequisites 4

Supported features 4

Limitations 4

Configure the AWS environment 4

Create Elastic IPs 5

CHAPTER 3

Deploy the Cisco Cyber Vision Center 9

Create and configure the instance 9

Allocate an Elastic IP to the instance 17

Cisco Cyber Vision Center setup 19

Establish a serial connection 19

Open an SSH connection from AWS 21

Basic Center configuration 24

Accept the End User License Agreement 24

Select the language to match your keyboard 25

Select the Center type 25

Configure the Center's DNS 28

Synchronize the Center and the sensors to NTP servers 28

Give the Center a name 29

Authorize networks 30

Set DHCP 30
 Complete the basic Center configuration 31

CHAPTER 4 **Connect to the Center 33**

Using the GUI 33
 Using the console 34

CHAPTER 5 **Configure the Center 35**

Install Cisco Cyber Vision 35
 Cisco Cyber Vision configuration 38
 Install the certificate in your browser 38
 Install Cisco Cyber Vision 44
 Configure the user interface security 47
 Upload a p12 48
 Generate a CSR 50
 Configure Center data synchronization 52

CHAPTER 6 **Deploy sensors 57**

CHAPTER 7 **Configure the Cisco Cyber Vision Center synchronization 59**

Global Center Configuration 59
 Center enrollment 59
 Center unenrollment 62
 Force the unenrollment of a Center 63

CHAPTER 8 **Annex – Setup Center json file 65**

CHAPTER 9 **Center Backup and Restore 67**

Backup and Restore Constraints 67
 Backup Cyber Vision Center 68
 Restore Cyber Vision Center 68
 Automate the Backup of the Cyber Vision Center 69
 Bash Script 70

Cron 70



CHAPTER 1

About this documentation

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

Document purpose

Amazon Virtual Private Cloud (Amazon VPC) is for launching Amazon WebServices (AWS) resources into a customized virtual network. This virtual network looks like a traditional network, with the benefits of using the scalable infrastructure of AWS.

This document explains how to deploy Cisco Cyber Vision Virtual on AWS.

This manual 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

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



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



CHAPTER 2

Getting started

- [Overview, on page 3](#)
- [Prerequisites, on page 4](#)
- [Supported features, on page 4](#)
- [Limitations, on page 4](#)
- [Configure the AWS environment, on page 4](#)
- [Create Elastic IPs, on page 5](#)

Overview

AWS is a collection of remote computing services offered by Amazon.com, also called web services, that make up a cloud-computing platform. These services operate from 11 geographical regions across the world.

In general, the user should become familiar with the following AWS services when deploying Cisco Cyber Vision Center and Cisco Cyber Vision Global Center:

- Amazon Elastic Compute Cloud (EC2)
A web service that enables you to rent virtual computers to launch and manage your own applications and services, such as a Cisco Cyber Vision Center, in Amazon's data centers.
- Amazon Virtual Private Cloud (VPC)
A web service that enables you to configure an isolated private network that exists within the Amazon public cloud. You run your EC2 instances within a VPC.
- Amazon Simple Storage Service (S3)
A web service that provides you with a data storage infrastructure.

You create an account on AWS, set up the VPC and EC2 components (using either the AWS Wizards or manual configuration), and choose an Amazon Machine Image (AMI) instance. The AMI is a template that contains the software configuration needed to launch your instance.



Note The AMI images are not available for download outside of the AWS environment.

Prerequisites

- An Amazon account.
- An SSH client (required to access the Cisco Cyber Vision Center console).
- Communication path: public/elastic IPs for access to the Cisco Cyber Vision resources.
- An Elastic IP (the default public IP change after a reboot. This can cause an issue for sensors).
- Minimum configuration to run and test the product are 8 vCPU and 16GB RAM.
- SSD disks are mandatory.

Supported features

- Center
- Global Center



Note For details about Center resources, refer to the Cisco Cyber Vision VM Installation Guide available in cisco.com.

Limitations

The following features or hardware are not supported:

- Dual interface Centers.
- Sensors using the sensor management extension.

Configure the AWS environment

To deploy Cisco Cyber Vision on AWS you need to configure an Amazon VPC with your deployment-specific requirements and settings. In most situations, a setup wizard can guide you through your setup. AWS provides online documentation where you can find useful information about the services ranging from introduction to advanced features.

Refer to <https://aws.amazon.com/documentation/gettingstarted/> for more information.

Additional information:

VM sizing

Minimum – up to 500 components:

- CPU: Intel Xeon, 8 cores
- RAM: 16GB minimum
- Storage: 500GB SSD

Recommended:

For 10,000 components w/o Center DPI:

- CPU: Intel Xeon, 10 cores
- RAM: 32GB minimum
- Storage: 1TB SSD minimum, RAID-10

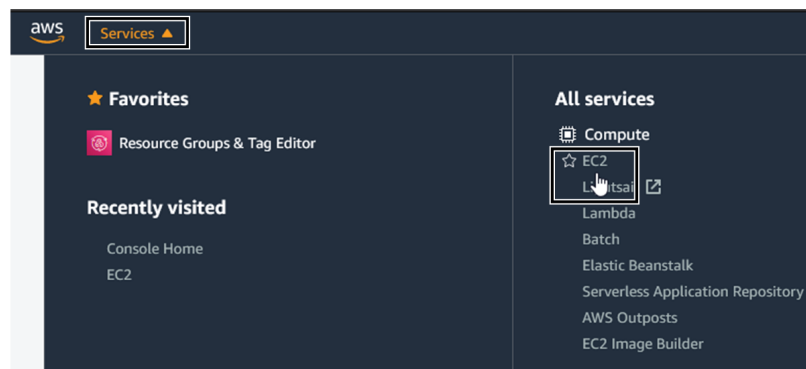
For more than 10,000 components or Center DPI:

- CPU: Intel Xeon, 16 cores
- RAM: 64GB minimum
- Storage: 1TB SSD minimum, RAID-10

Create Elastic IPs

When an instance is created, a public IP address is associated with the instance. That public IP address changes automatically when you stop and start the instance. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. Elastic IPs are reserved public IPs that are used for remote access to the Cisco Cyber Vision as well as other instances.

1. Access you Amazon account.
2. Navigate to Services > EC2.



3. Under Network & Security, click Elastic IPs.

The screenshot shows the AWS Management Console interface. On the left, the navigation menu is expanded to 'Network & Security', and 'Elastic IPs' is highlighted. A blue banner at the top right reads 'Welcome to the new EC2 console! We're redesigning the EC2 console to make it easier to use and improve performance. We want to hear from you about how you use them and let us know where we can make improvements. To switch between the old console and the new one, click here.' Below the banner, the 'Resources' section displays a table of Amazon EC2 resources in the Europe (Ireland) Region:

You are using the following Amazon EC2 resources in the Europe (Ireland) Region:		
Instances (running)	0	Dedicated Hosts
Elastic IPs	0	Instances
Key pairs	8	Load balancers
Placement groups	0	Security groups

4. Click Allocate Elastic IP address.

The screenshot shows the 'Elastic IP addresses' console page. The left navigation pane is expanded to 'Network & Security', and 'Elastic IPs' is highlighted. The main content area shows the 'Elastic IP addresses' section with a search bar, a refresh button, and an 'Actions' dropdown menu. The 'Allocate Elastic IP address' button is highlighted with a red box. Below the search bar, there is a table with columns for 'Name', 'Allocated IPv4 address', and 'Type'. The table is currently empty.

5. Click Allocate to create the Elastic IP.

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Public IPv4 address pool

- Amazon's pool of IPv4 addresses
- Public IPv4 address that you bring to your AWS account (option disabled because no pools found) [Learn more](#)
- Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tag

Cancel [Allocate](#)

6. Check the new Elastic IP out.

aws Services Search for services, features, marketplace [Option+S] devops/wboudaa@cisco.com @ 3286-0807-8092 Ireland Support

Capacity Reservations

- Images
 - AMIs
- Elastic Block Store
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security
 - Security Groups
 - Elastic IPs**

Elastic IP addresses (1/1)

[Filter Elastic IP addresses](#) < 1 > [Clear filters](#)

Public IPv4 address: 54.195.222.37 [Clear filters](#)

<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation
<input checked="" type="checkbox"/>	-	54.195.222.37	Public IP	eipalloc-0



CHAPTER 3

Deploy the Cisco Cyber Vision Center

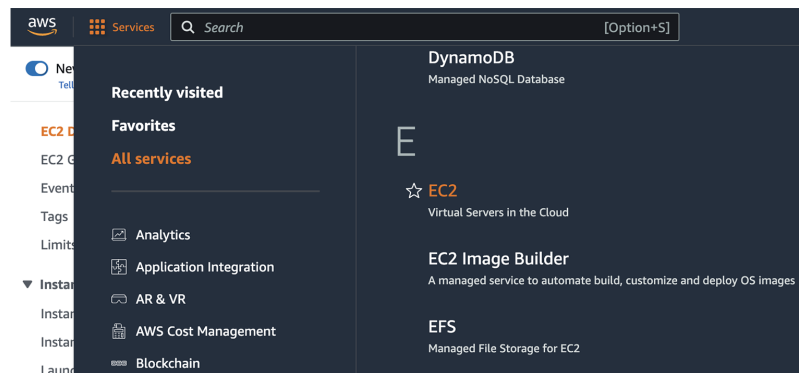
- Create and configure the instance, on page 9
- Allocate an Elastic IP to the instance, on page 17
- Cisco Cyber Vision Center setup, on page 19

Create and configure the instance

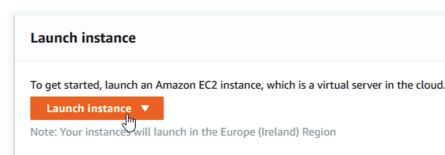
Procedure

Step 1 Go to <https://aws.amazon.com> Amazon Web Services and sign in.

Step 2 Navigate to **All services > EC2**.



Step 3 Click **Launch Instance**.



Step 4 Give the instance a name.

Step 5 Type "cyber vision" in the AMI search bar.

Create and configure the instance

aws Services Search [Option+S]

EC2 > Instances > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name [Add additional tags](#)

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Step 6

In the AWS Marketplace AMIs menu, select Cisco Cyber Vision BYOL.

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quickstart AMIs (0) **My AMIs (0)** **AWS Marketplace AMIs (1)** **Community AMIs (7)**

Commonly used AMIs Created by me AWS & trusted third-party AMIs Published by anyone

Refine results

Categories
Infrastructure
Software (1)

▼ Publisher
 Cisco (1)

▼ Pricing model
 Bring Your Own

cyber vision (1 result) showing 1 - 1

Sort By: Relevance

Cisco Cyber Vision BYOL
By Cisco | Ver 4.1.3

Cisco Cyber Vision is a cybersecurity solution specifically designed for organizations in power and water distribution, oil & gas, manufacturing and public transportation to ensure continuity, resilience and safety of their industrial operations. It provides asset owners with full visibility into...

[Select](#)

Step 7

Click **Continue**.

Cisco Cyber Vision BYOL
Cisco Systems, Inc. [0 AWS reviews](#)
[Bring Your Own License](#)

Overview | Product details | Pricing | Usage | Support

Cisco Cyber Vision is a cybersecurity solution specifically designed to ensure continuity, resilience and safety of industrial operations. It automatically discovers and monitors industrial assets and processes to detect threats and anomalies and extend IT security to the OT domain through seamless

Typical total price \$0.042/Hr Total pricing per instance for services hosted on t3.medium in us-east-1. See additional pricing information.	Latest version 4.3.0 Delivery methods Amazon Machine Image Operating systems Other Cyber Vision 4.3.0 Other Cyber Vision 4.1.4	Categories Security Network Infrastructure
--	---	--

[Continue](#)

Step 8 Slide down to instance type.

Supported instance families
<ul style="list-style-type: none">• C5, C5a, C5ad, C5d, C5n, C6g, C6gd• M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd• R5, R5a, R5ad, R5d, R5dn, R5n, R6, R6gd• T3, T3a, T4g• Z1d

Step 9 Select an instance type by typing for example "t3.xlarge".

The screenshot shows the 'Instance type' section of the AWS console. A dropdown menu is open, displaying search results for 't3.x'. The selected item is 't3.xlarge', which has a family of 't3', 4 vCPU, and 16 GiB Memory. To the right of the dropdown, there is a radio button for 'All generations' and a link to 'Compare instance types'.

Step 10 Select or create a new key pair.

The screenshot shows the 'Key pair (login)' section of the AWS console. It includes a text box for 'Key pair name - required' with the value 'JMA' and a 'Create new key pair' button.

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

JMA

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel Create key pair

A file called YOURKEYPAIRNAME.pem will be downloaded.

Step 11 Slide down to Network settings and click **Edit**.

▼ **Network settings** Info

Network Info

vpc-015e027ecdf241329

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Edit

Step 12 Set Auto-assign public IP to **Disable**.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-015e027ecdf241329 (default) [Info](#)

172.31.0.0/16

Subnet [Info](#)

No preference [Info](#) [Create new subnet](#)

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Inbound Security Group Rules appears.

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type [Info](#) Protocol [Info](#) Port range [Info](#)

ssh TCP 22

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Anywhere [Info](#) [Add CIDR, prefix list or security](#) e.g. SSH for admin desktop

0.0.0.0/0 [X](#)

▼ Security group rule 2 (TCP, 443, 0.0.0.0/0) [Remove](#)

Type [Info](#) Protocol [Info](#) Port range [Info](#)

HTTPS TCP 443

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Anywhere [Info](#) [Add CIDR, prefix list or security](#) e.g. SSH for admin desktop

0.0.0.0/0 [X](#)

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. [X](#)

[Add security group rule](#)

Step 13 Click **Add security group rule** to start configuring AWS firewall settings. Add the rules that provide access from users or other resources to the Center. List of the ports that need to be added:

- For Global Center <--> Center communication

Protocol	Port
AMPQ	TCP/5671
NTP	UDP/123
Syslog	UDP/TCP 514
SSH	TCP/22

- For CS workstation/ntp server <--> Center communication

Protocol	Port
HTTPS	TCP/443
SSH	TCP/22
NTP	UDP/123

- For Sensor <--> Center communication

Protocol	Port
AMPQ	TCP/5671
Syslog	UDP/10514

Example of security configuration:

Type	Protocol	Port range	Source type	Description
SSH	TCP	22	0.0.0.0/0	SSH
HTTPS	TCP	443	0.0.0.0/0	HTTPS
Custom TCP	TCP	5671	0.0.0.0/0	AMPQ
Custom UDP	UDP	123	0.0.0.0/0	NTP
Custom TCP	TCP	514	0.0.0.0/0	Syslog (for Global Center)
Custom UDP	UDP	514	0.0.0.0/0	Syslog (for Global Center)
Custom UDP	UDP	10514	0.0.0.0/0	Syslog (for sensor)

Step 14 Configure storage by changing the value or ,if needed, adding a new volume.

Note Make sure to setup the correct disk size as this information will remain and cannot be modified.

Note Do not use the Magnetic (Standard) for Volume Type.

Note Default type will be SSD.

For example, we change 100 GiB default value to 500.

▼ **Configure storage** [Info](#) Advanced

1x GiB ▼ Root volume (Not encrypted)

i Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

↻ Click refresh to view backup information ↻
 The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

Step 15 Depending on the Center type, fill the Advanced Details > User data part at the bottom of the page.

User data - *optional* [Info](#)
 Upload a file with your user data or enter it in the field.

User data has already been base64 encoded

If a json file is used to specify the type of the Center, this step will be skipped during the installation.

- To deploy a Center, leave the textbox empty.
- To deploy a Center with sync, the minimal configuration is:

```
{
  "center-type": "Local Center",
}
```

- To deploy a Global Center, the minimal configuration is:

```
{
  "center-type": "Global Center",
}
```

For all json parameters, refer to [Annex – Setup Center json file](#).

Step 16 Review the settings on the right summary and click **Launch instance**.

▼ **Summary**

Number of instances [Info](#)

1

[Software Image \(AMI\)](#)
Cisco Cyber Vision BYOL
ami-045d09fc2dd6111e2

[Virtual server type \(instance type\)](#)
t3.xlarge

[Firewall \(security group\)](#)
New security group

[Storage \(volumes\)](#)
1 volume(s) - 500 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance

The following status should appear.

EC2 > Instances > Launch an instance

~ Launching instance
Subscribing to Marketplace AMI 64%

▶ Details

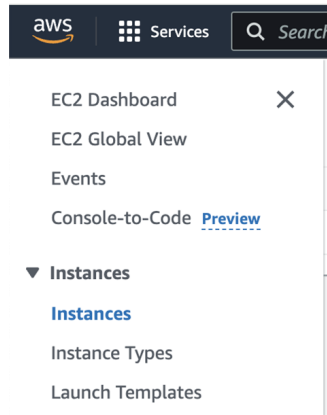
Please wait while we launch your instance.
Do not close your browser while this is loading.

EC2 > Instances > Launch an instance

✔ Success
Successfully initiated launch of instance (i-014b63c1220a99342)

Allocate an Elastic IP to the instance

1. Click **Instances** in AWS left menu.



2. Choose your instance on the instances list and copy your instance ID.

Name	Instance ID	Instance state	Instance type	Status check	Alarm
-	i-0710fe2b5d36ec422	Stopped	t3.small	-	No al
-	i-08a2fda60d270e4b2	Running	t2.micro	2/2 checks passed	No al
-	i-06e504824ccf8624f	Running	t2.micro	2/2 checks passed	No al
-	i-08f59928e6f5ec898	Running	t3.medium	2/2 checks passed	No al
-	i-0c2b04853a5dc4d4c	Running	t3.medium	2/2 checks passed	No al
-	i-014e278d0360f811e	Running	t3.medium	2/2 checks passed	No al
-	i-04beddd7712c65b1e	Terminated	c5a.large	-	No al
-	i-0b19cd5b75ee7cffa	Running	c5a.large	Initializing	No al

Instance summary		
Instance ID	Public IPv4 address	Private IPv4 addresses
i-0b19cd5b75ee7cffa	-	172.31.7.229

3. Click **Elastic IPs** in AWS left menu.

Allocate an Elastic IP to the instance

aws Services Search for services, features, marketplace products, and docs [Option+S]

- Network & Security
 - Security Groups **New**
 - Elastic IPs **New****
 - Placement Groups
 - Key Pairs
 - Network Interfaces **New**
- Load Balancing
 - Load Balancers
 - Target Groups **New**
- Auto Scaling
 - Launch Configurations

Welcome to the new EC2 console!
We're redesigning the EC2 console to make it easier to use and improve performance. We're listening to your feedback, so please let us know what you think of the new console and let us know where we can make improvements. To switch between the old console and the new console, click on the link in the top right corner of the console.

Resources

You are using the following Amazon EC2 resources in the Europe (Ireland) Region:

Instances (running)	0	Dedicated Hosts
Elastic IPs	0	Instances
Key pairs	8	Load balancers
Placement groups	0	Security groups

4. Click the created Elastic IP.

aws Services Search for services, features, marketplace [Option+S] devops/wboudaa@cisco.com @ 3286-0807-8092 Ireland Support

Capacity Reservations

- Images
- AMIs
- Elastic Block Store
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security
 - Security Groups
 - Elastic IPs**

Elastic IP addresses (1/1) [Refresh] [Actions] **Allocate Elastic IP address**

Filter Elastic IP addresses < 1 > [Settings]

Public IPv4 address: 54.195.222.37 [Clear filters]

<input checked="" type="checkbox"/>	Name	Allocated IPv4 address	Type	Allocation ID
<input checked="" type="checkbox"/>	-	54.195.222.37	Public IP	eipalloc-0

5. Click Associate Elastic IP address.

aws Services Search for services, features, marketplace [Option+S] devops/wboudaa@cisco.com @ 3286-0807-8092 Ireland Support

Capacity Reservations

- Images
- AMIs
- Elastic Block Store
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs
 - Network Interfaces **New**
- Load Balancing

EC2 > Elastic IP addresses > 54.195.222.37

54.195.222.37 [Actions] **Associate Elastic IP address**

Summary

Allocated IPv4 address 54.195.222.37	Type Public IP	Allocation ID eipalloc-047232ca6e635d00c	Association ID -
Scope VPC	Associated instance ID -	Private IP address -	Network interface ID -
Network interface owner account ID -	Public DNS -	NAT Gateway ID -	Address pool Amazon

6. Select Instance.

7. Paste the instance ID previously copied.

8. Click in the field and select the private IP address of the created Center.
9. Click **Associate**.

EC2 > Elastic IP addresses > 54.195.222.37 > Associate Elastic IP address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (54.195.222.37)

Elastic IP address: 54.195.222.37

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. [Learn more](#)

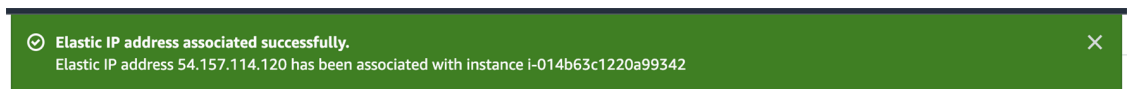
Instance

Private IP address
The private IP address with which to associate the Elastic IP address.

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassociated

The following status should appear.



Cisco Cyber Vision Center setup

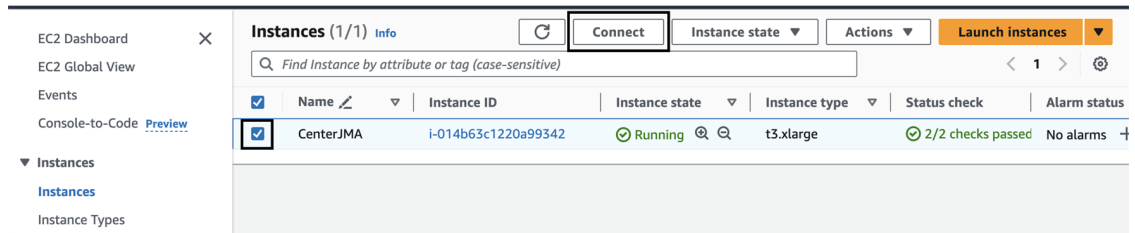
Establish a serial connection or open an SSH connection from AWS and then proceed to the basic Center configuration.

Establish a serial connection

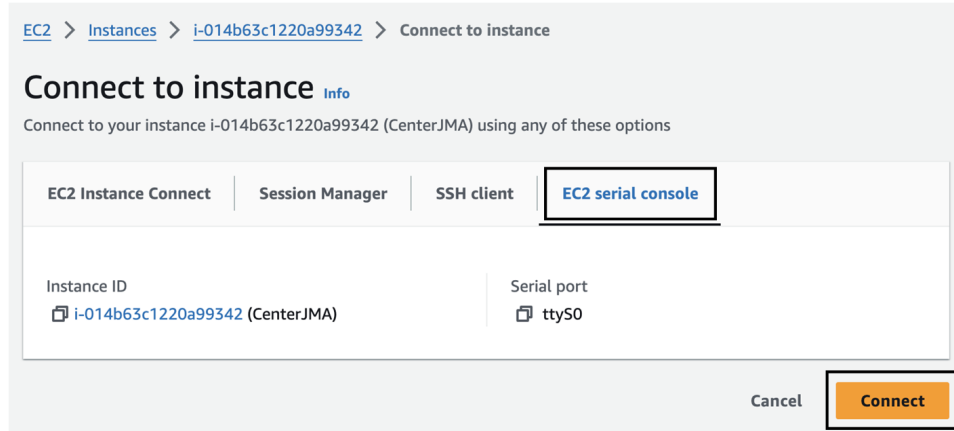
Procedure

- Step 1** In the Instances menu, select the instance you just created and click **Connect**.

Establish a serial connection



Step 2 Click **EC2 serial console**.

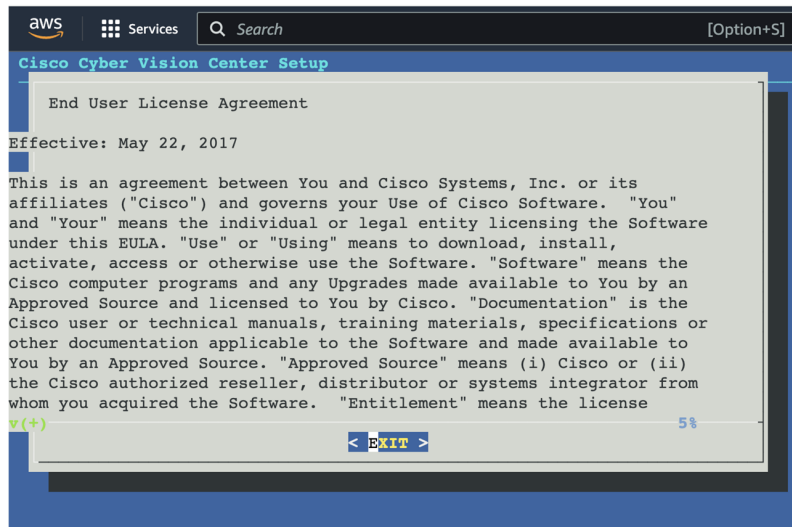


Step 3 Click **Connect**.

Step 4 A new window with a shell prompt opens in the browser.

Step 5 Press **Enter**.

The Cisco Cyber Vision Center Setup appears.



Step 6 Press **Enter**.

Open an SSH connection from AWS

1. Go to instances to check the information of the created machine.

The screenshot displays the AWS Management Console interface for an EC2 instance. The main content area shows the 'Instance summary for i-0b19cd5b75ee7cffa'. The instance is in a 'Running' state. Key details include: Instance ID: i-0b19cd5b75ee7cffa, Public IPv4 address: 54.195.222.37, Instance state: Running, Instance type: c5a.large, AMI ID: ami-0ddb5a307abb22bd2, and AMI name: Cyber Vision Center - 4.0.0-RC4. The 'Connect' button is visible in the top right corner.

The key previously created or chosen will be automatically added to `/data/etc/ssh/userkey/root`.



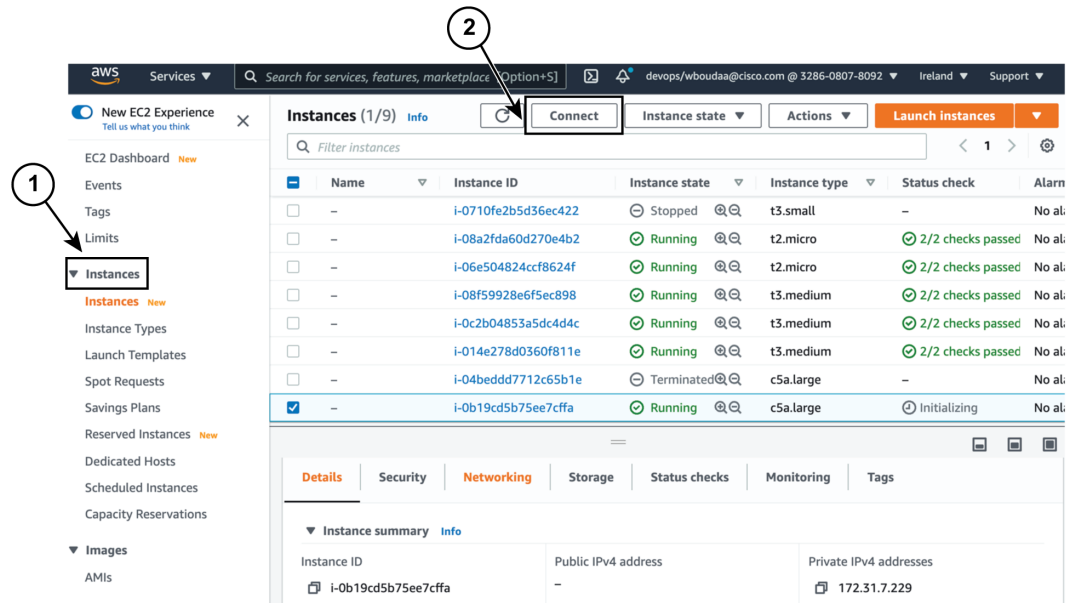
Note It is possible to add multiple keys on that file if an access is needed from another device that is not using the same certificates than the installed one.

This key is downloaded locally or already exists.

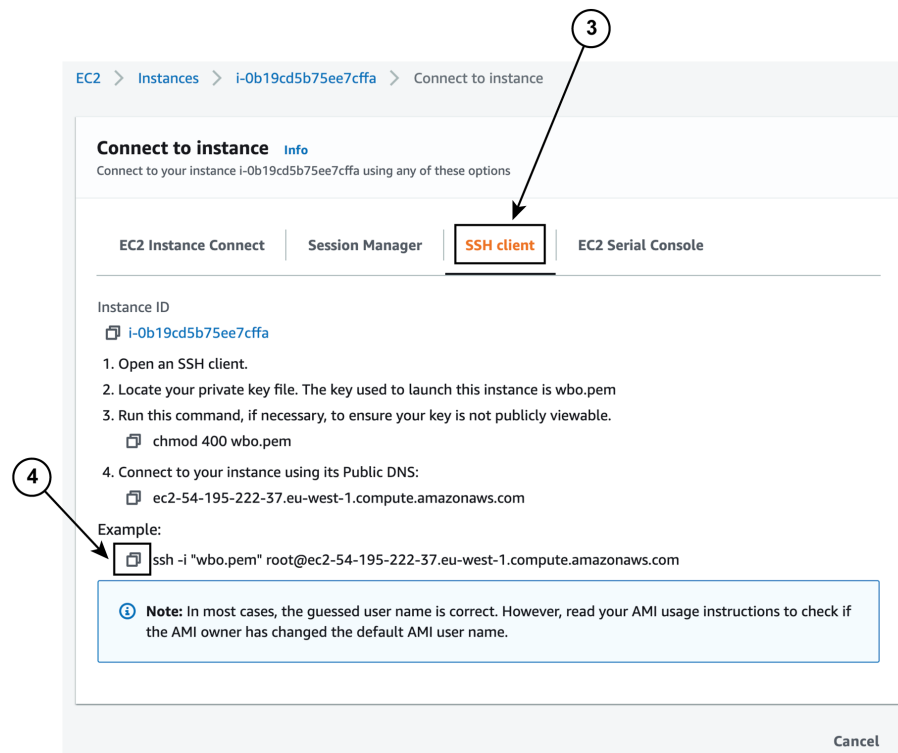
Please follow the steps below to connect using SSH and finalize the installation.

2. In the AWS EC2 management console, click Instances (1).
3. Choose the needed instance and click the Connect button (2).

Open an SSH connection from AWS



4. Access the SSH Client menu (3) and follow the steps described in it.



5. Copy and paste the example (4) into the ssh client and replace 'root' with 'cv-admin', like below:
ssh -i wbo.pem cv-admin@ec2-54-195-222-376.eu-west-1.compute.amazonaws.com
6. Once connected to the Center, type the following command:


```
sudo -i
```

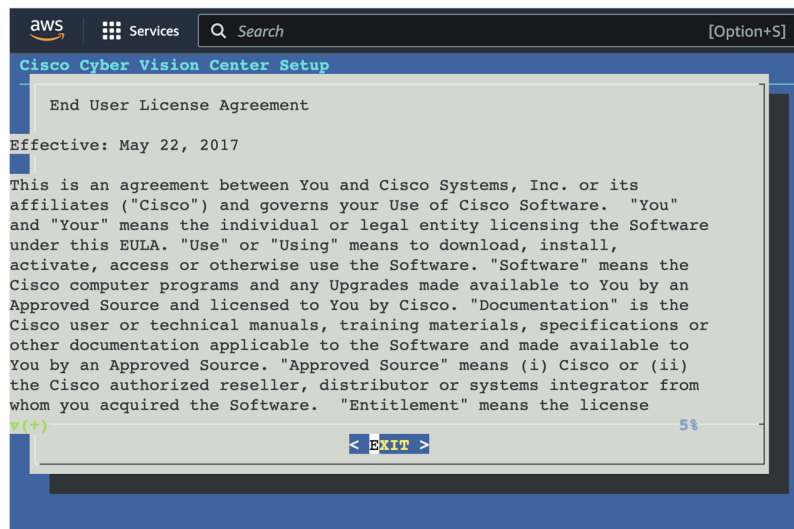
7. Type the following command:

```
setup-center
```

```
SBS 4.0.0
cv-admin@ec2-52-31-40-71:~$
cv-admin@ec2-52-31-40-71:~$
cv-admin@ec2-52-31-40-71:~$ sudo -i
root@ec2-52-31-40-71:~#
root@ec2-52-31-40-71:~# setup-center|
```

8. Press **Enter**.

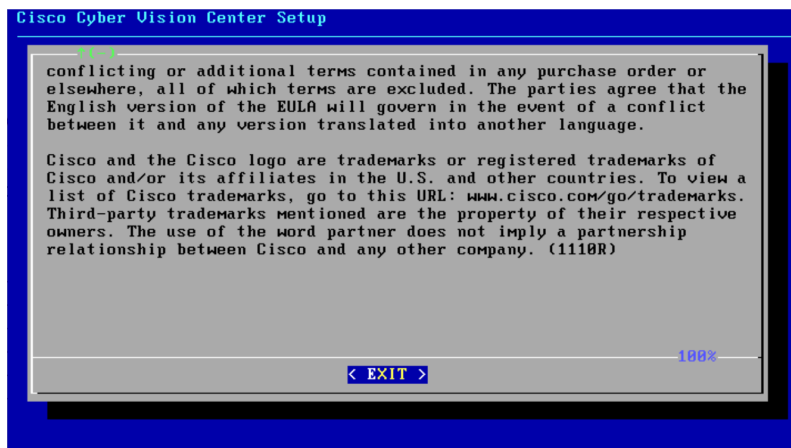
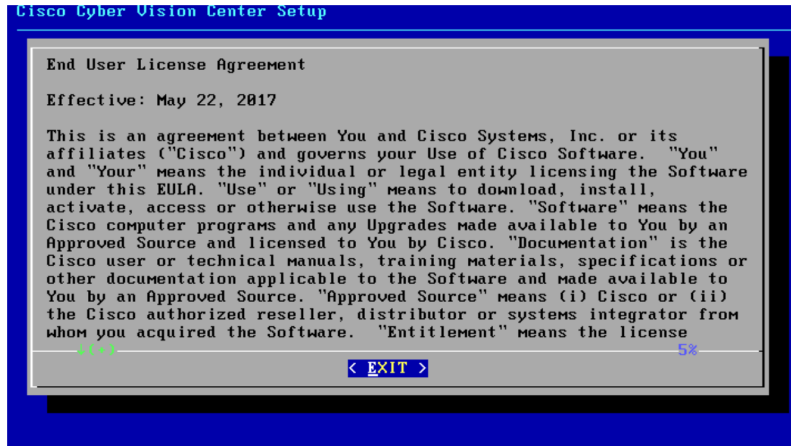
The Cisco Cyber Vision Center Setup appears.



9. Press **Enter**.

Basic Center configuration

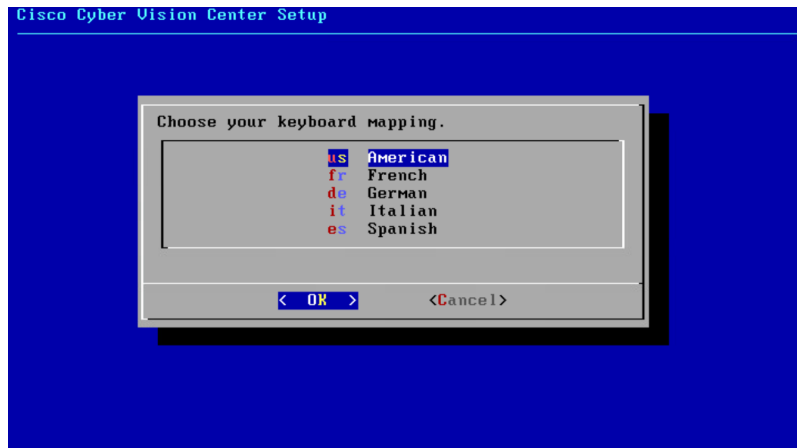
Accept the End User License Agreement



Select the language to match your keyboard



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

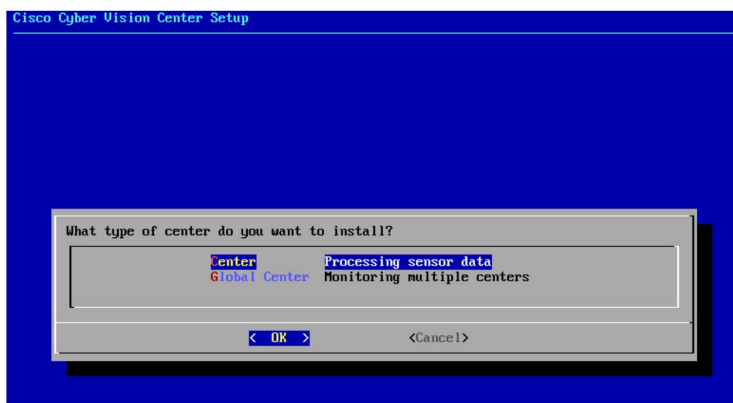


Select the Center type

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

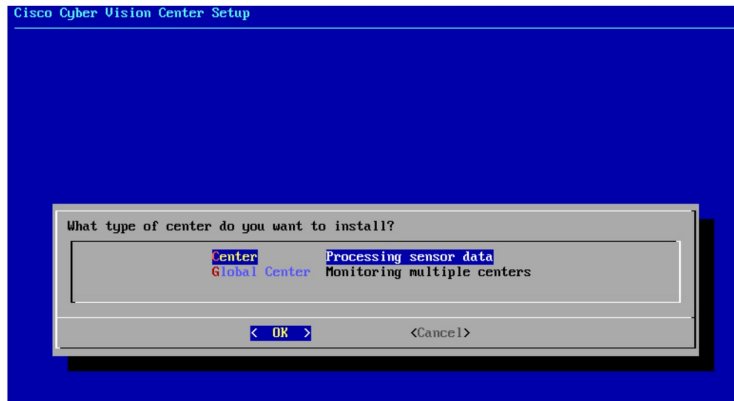
- A **Center** receives metadata from sensors and store them into an internal database (Postgresql). It can be standalone or synchronized with a Global Center. A Center with sync is similar to a standalone Center from a functionality point of view, except for the link to a Global Center. You must install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

Select the type of Center you want to install.



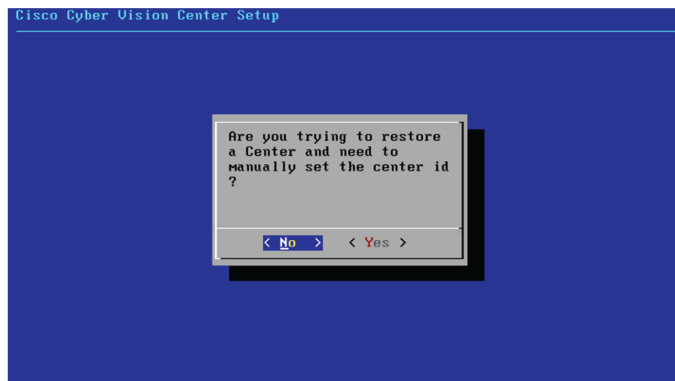
Center

If installing a Center, select the first option.

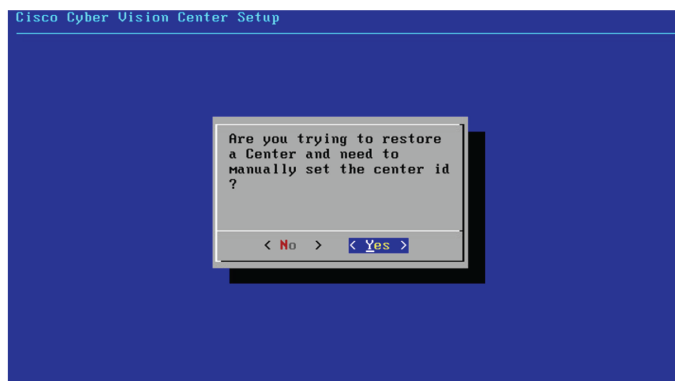


Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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



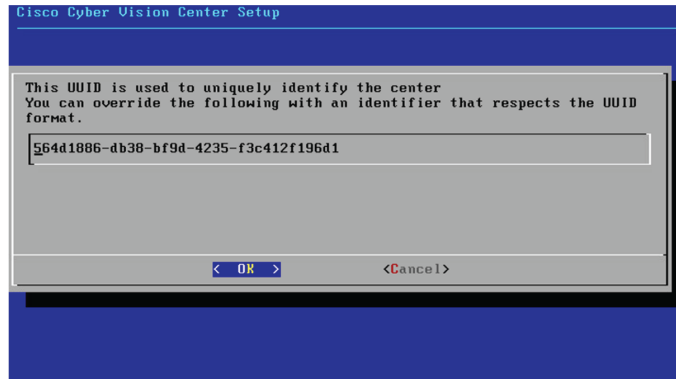
If you're reinstalling the Center and want to restore it, select Yes.



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

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

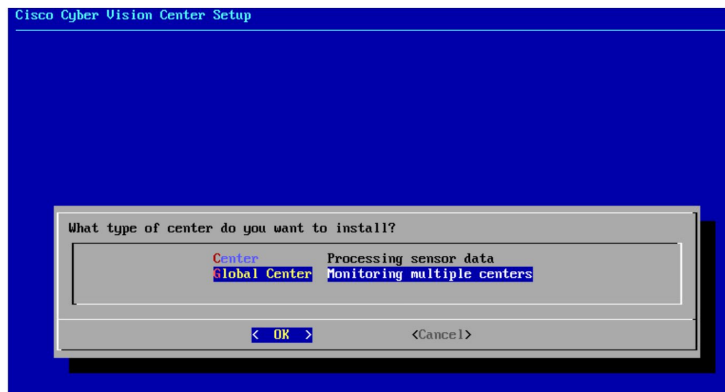
Type the id into the basic Center configuration UUID field.



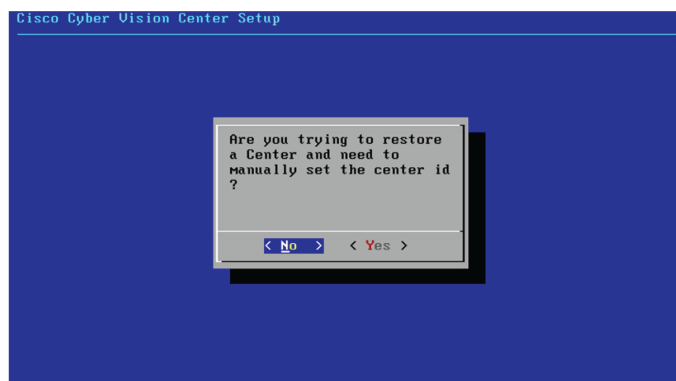
Click OK. You will be directed to the next step.

Global Center

If installing a Global Center, select the second option.



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



You will be directed to the next step.

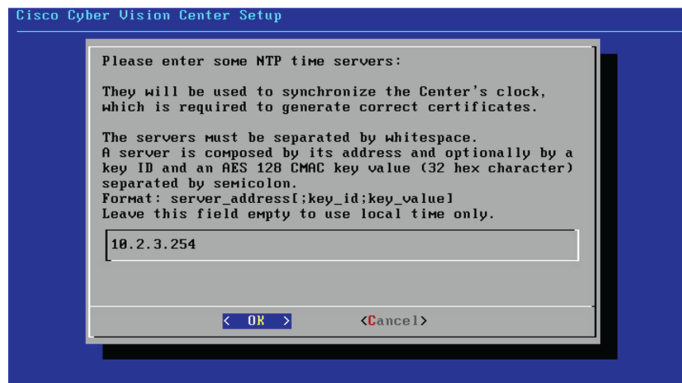
Configure the Center's DNS

Type a DNS server address and optional fallbacks.

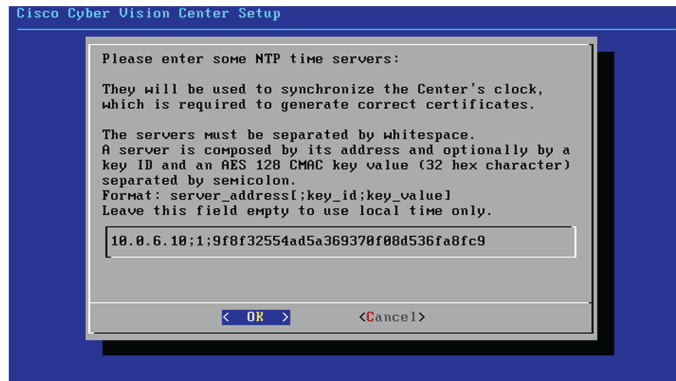


Synchronize the Center and the sensors to NTP servers

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



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

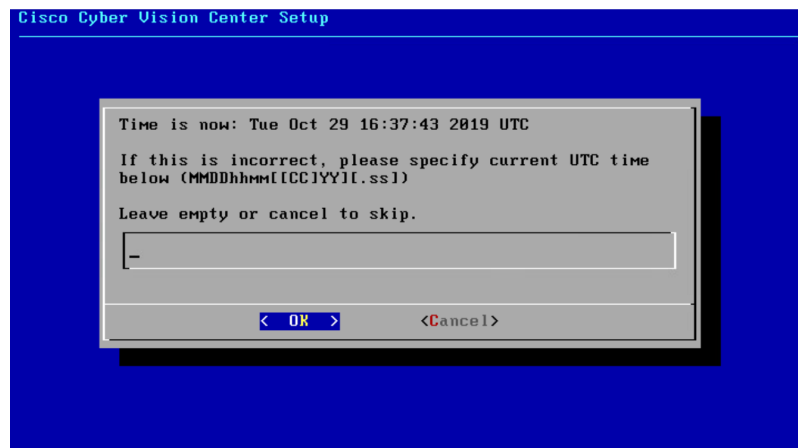


The synchronization takes a few seconds.

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



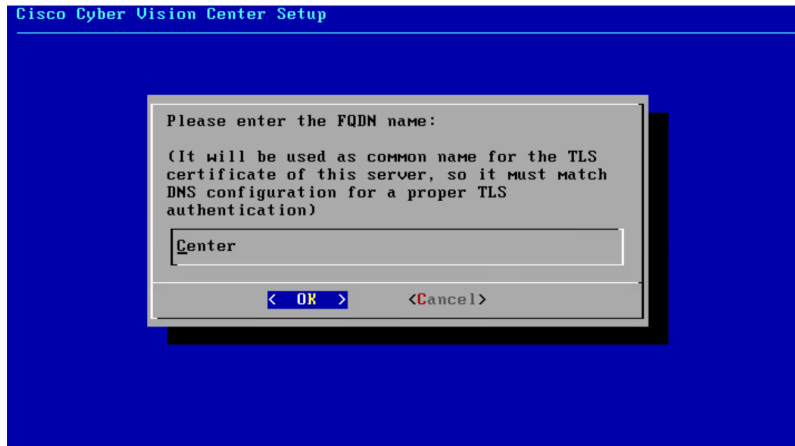
Note The time is set in UTC standard.



Give the Center a name



Note This name will be used in the Center certificate.



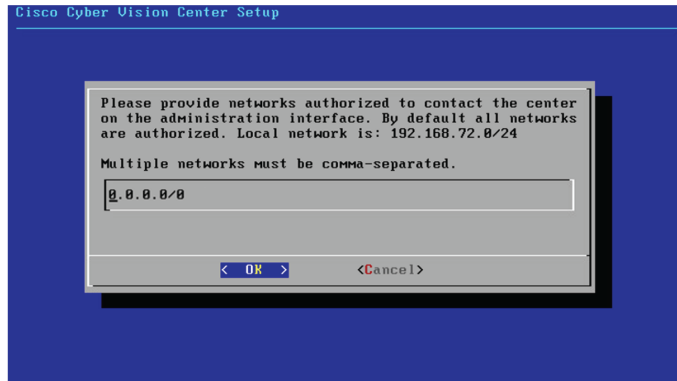
Enter the Center name provided by your administrator or type 'Default' which is a secure value.



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

Authorize networks

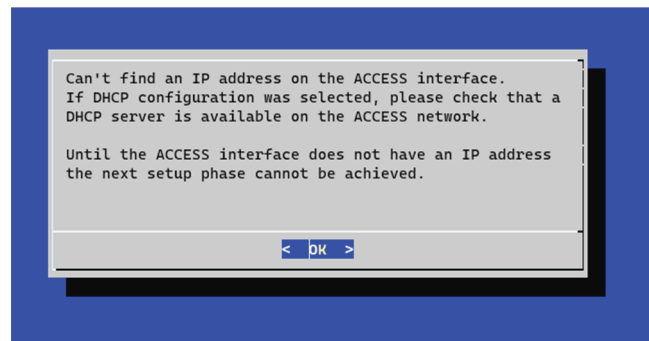
This step allows you to restrict IP addresses that can connect to the Administration interface. If no IP is entered, all networks are authorized by default.



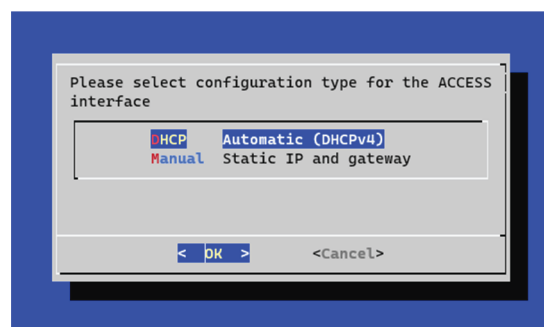
Set DHCP

Procedure

Step 1 If the following message appears, select OK.

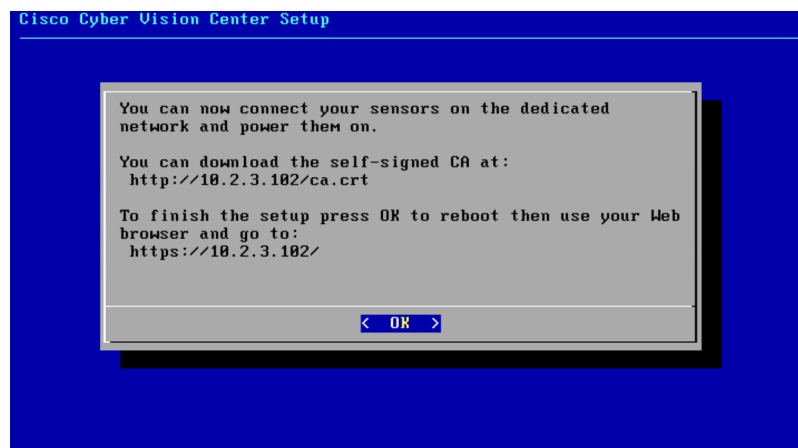


Step 2 Select DHCP.



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.



Enter OK to finish the basic Center configuration.

```

..:~::~: Cisco Cyber Vision ..:~::~:
Log in to this Cisco Cyber Vision instance using https://192.168.72.22
VMware, Inc. VMware Virtual Platform
CPU: 4 x Intel(R) Core(TM) i7-8809G CPU @ 3.10GHz
RAM: 7.74 Gib
Single interface: no

WARNING, READ THIS BEFORE ATTEMPTING TO LOGON
Confidential Information

This system is for the use of authorized users only. Individuals using this computer without
authority, or in excess of their authority, are subject to having all of their activities on
this system monitored and recorded by system personnel. In the course of monitoring
individuals improperly using this system, or in the course of system maintenance, the
activities of authorized users may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such monitoring reveals possible criminal
activity, system personnel may provide the evidence of such monitoring to law enforcement
officials.

SBS 4.1.0 center tty1
center login: _

```



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

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

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



CHAPTER 4

Connect to the Center

You can connect to the Center:

- Using the [Using the GUI](#).
- Using the [Using the console](#).
- [Using the GUI, on page 33](#)
- [Using the console, on page 34](#)

Using the GUI

The Public IP address and FQDN of your instance will be available on the Instance summary page:

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0b19cd5b75ee7cffa	54.195.222.37 open address	172.31.7.229
Instance state	Public IPv4 DNS	Private IPv4 DNS
Running	ec2-54-195-222-37.eu-west-1.compute.amazonaws.com open address	ip-172-31-7-229.eu-west-1.compute.internal
Instance type	Elastic IP addresses	VPC ID
c5a.large	54.195.222.37 [Public IP]	vpc-77b96d0e
AWS Compute Optimizer finding	IAM Role	Subnet ID
Opt-in to AWS Compute Optimizer for recommendations. Learn more	-	subnet-919a9cf7

1. In your browser, use the public IP address or the FQDN to download and save the certificate:
 - `https://<Public IPV4 address>/ca/crt`
 - `https://<Public IPV4 DNS>/ca/crt`
2. In your browser, use the following address to access Cisco Cyber Vision:
`https://<CENTERNAME>/.`

You can proceed with [Install Cisco Cyber Vision](#).

Using the console

You can connect to the Center using the AWS serial console.



Note Serial Console is only supported in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (Oregon), Europe (Ireland), Europe (Frankfurt), Asia Pacific (Sydney), Asia Pacific (Tokyo), Asia Pacific (Singapore).

To use the serial console, click Actions > Monitor and troubleshoot > EC2 Serial Console.

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with options like 'EC2 Dashboard', 'Events', 'Tags', 'Limits', and 'Instances'. The main area displays a list of EC2 instances. One instance is selected, and a context menu is open over it. The menu includes options like 'Launch instances', 'Connect', 'Stop instance', 'Start instance', 'Reboot instance', 'Hibernate instance', 'Terminate instance', 'Instance settings', 'Networking', 'Security', 'Image and templates', and 'Monitor and troubleshoot'. The 'Monitor and troubleshoot' option is expanded, showing a sub-menu with 'EC2 Serial Console' highlighted.

The root password by default will be the instance ID of the Center you created.

Supported instance families:

- A1
- C5, C5a, C5ad, C5d, C5n, C6g, C6gd
- M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd
- R5, R5a, R5ad, R5d, R5dn, R5n, R6, R6gd
- T3, T3a, T4g
- Z1d



CHAPTER 5

Configure the Center

- [Install Cisco Cyber Vision, on page 35](#)
- [Cisco Cyber Vision configuration, on page 38](#)

Install Cisco Cyber Vision

Access the Cisco Cyber Vision 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 Cisco Cyber Vision 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

👤 Create the first user — 📄 Agree to the license terms — ✅ Done

Firstname : Lastname :
 Email :
 Password : Confirm password :
 Suggested password:
 SkvIH2Qq*odz90fj0E3 📄 📋

[Create](#)

Step 4**Step 5**

Enter the information required.

Note Email will be asked for login access.

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

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

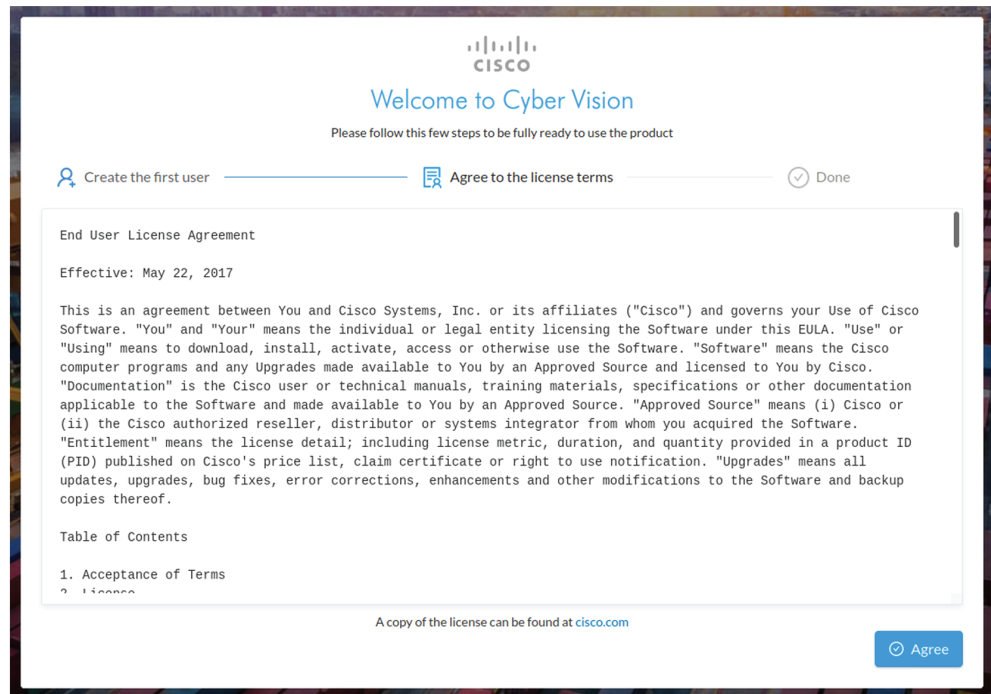
Passwords should be changed regularly to ensure the integrity of the platform and the industrial network security.

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

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

Step 6

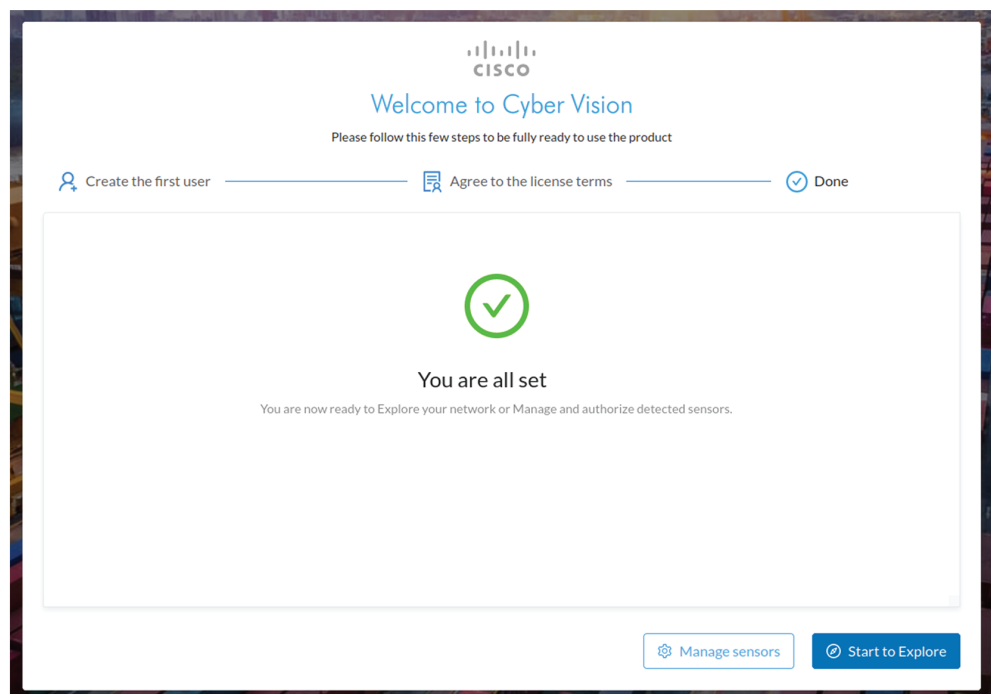
Accept the software license agreement:

**Step 7****Step 8 Finish the installation:**

The Center is now correctly installed and 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 47](#).

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 52](#).

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.

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 38](#) 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 install a Cisco Cyber Vision self-signed certificate in your browser.

Before you begin

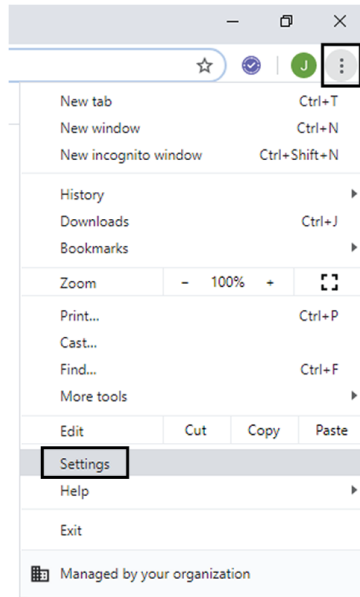
Perform this task if you aim to install a self-signed certificate. If you're planning to use an enterprise certificate, proceed directly with [Install Cisco Cyber Vision, on page 35](#).

Procedure

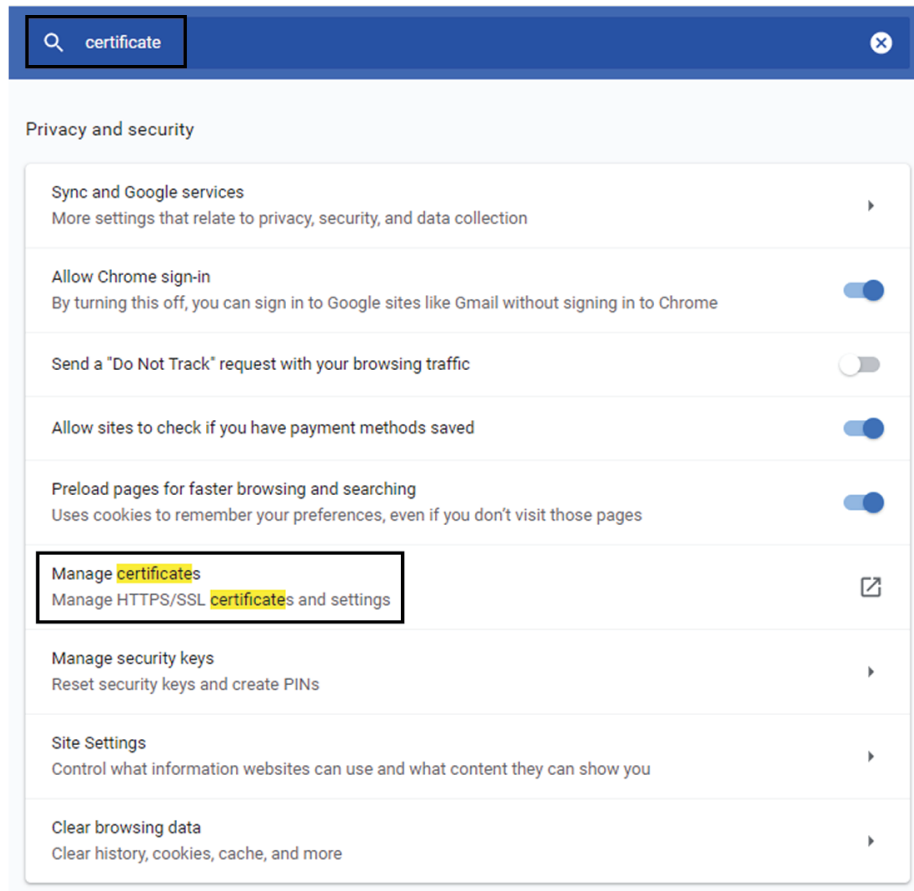
- Step 1** Open your browser.
- Step 2** Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.
The certificate is downloaded.
- Step 3** Save the certificate on your computer.

Step 4 In the browser, access the settings.

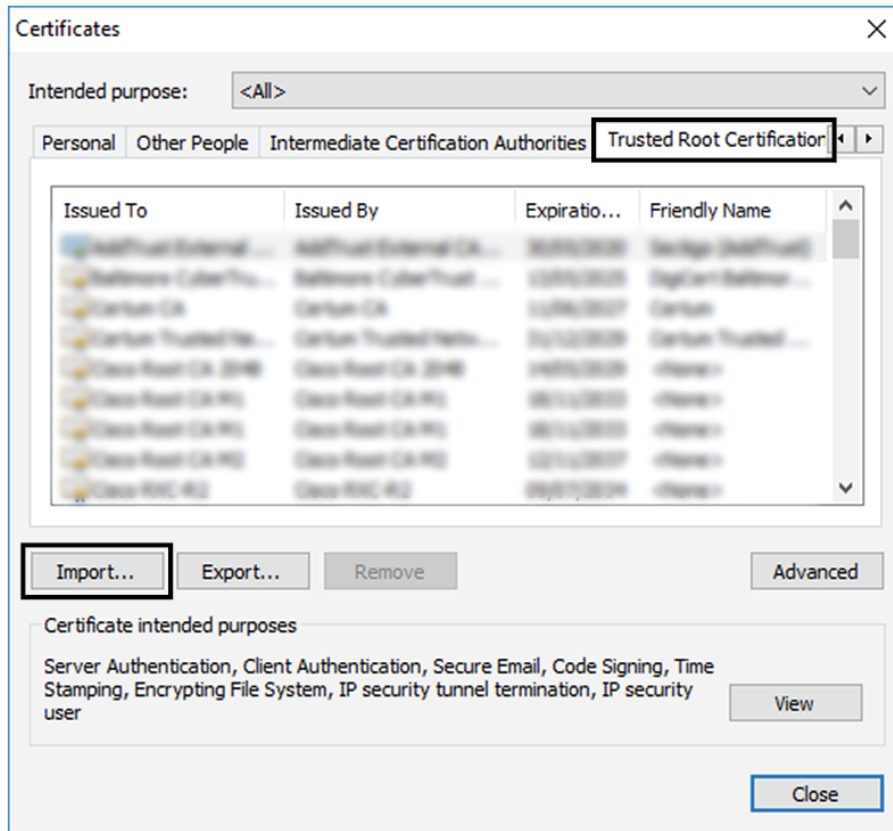
Example: Chrome



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



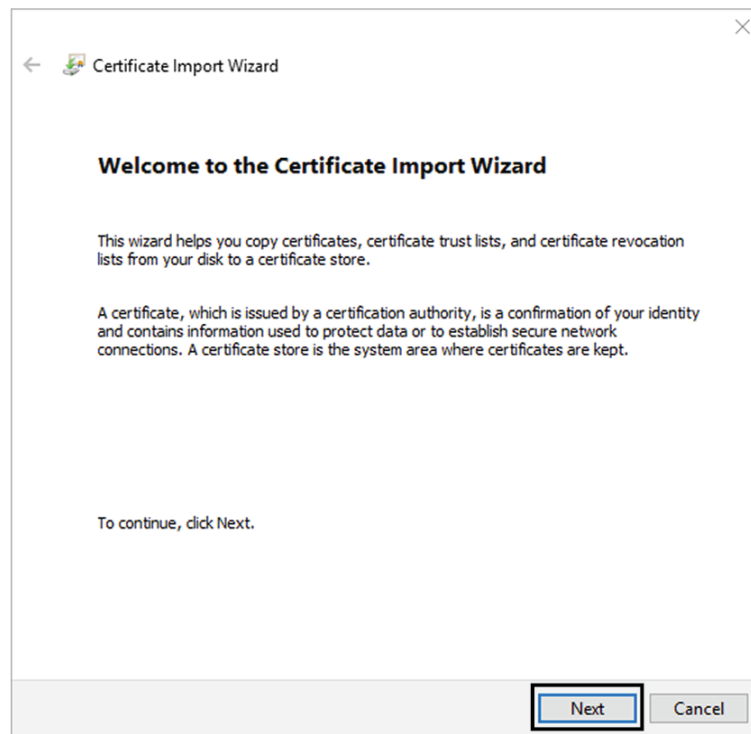
Step 6 Access the Trusted Root Certification tab and click Import.



A certificate importation wizard opens.

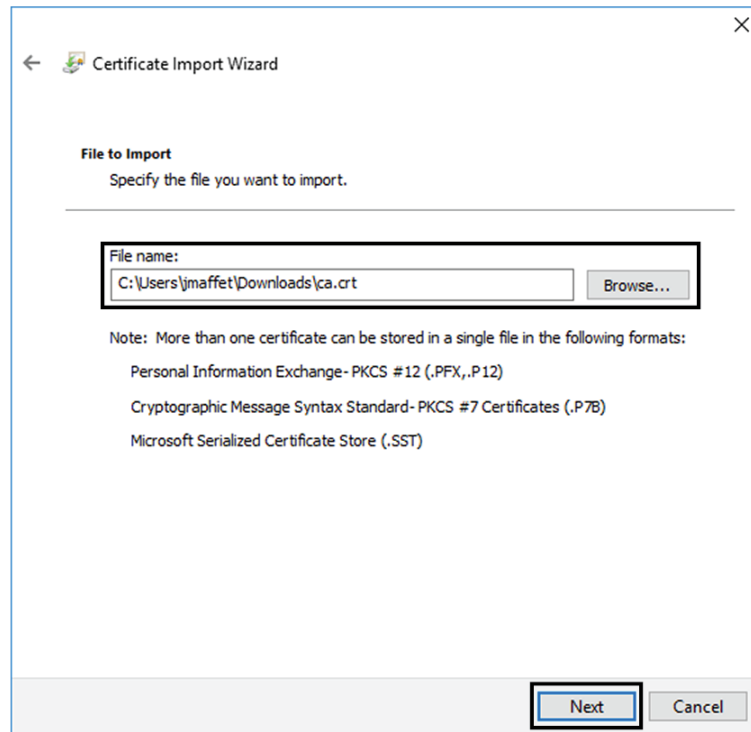
Step 7

Go to the next step.

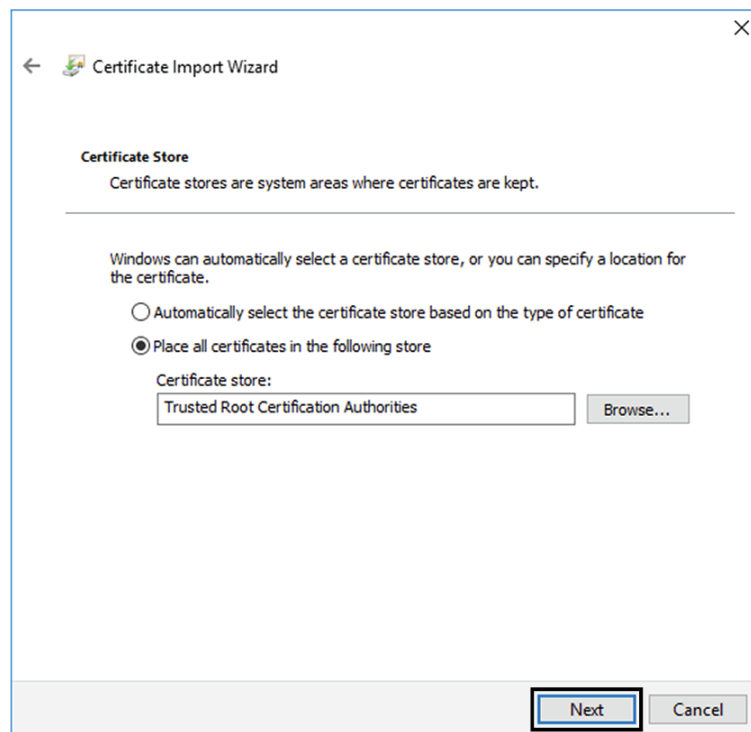


Step 8 Search for the certificate you downloaded earlier.

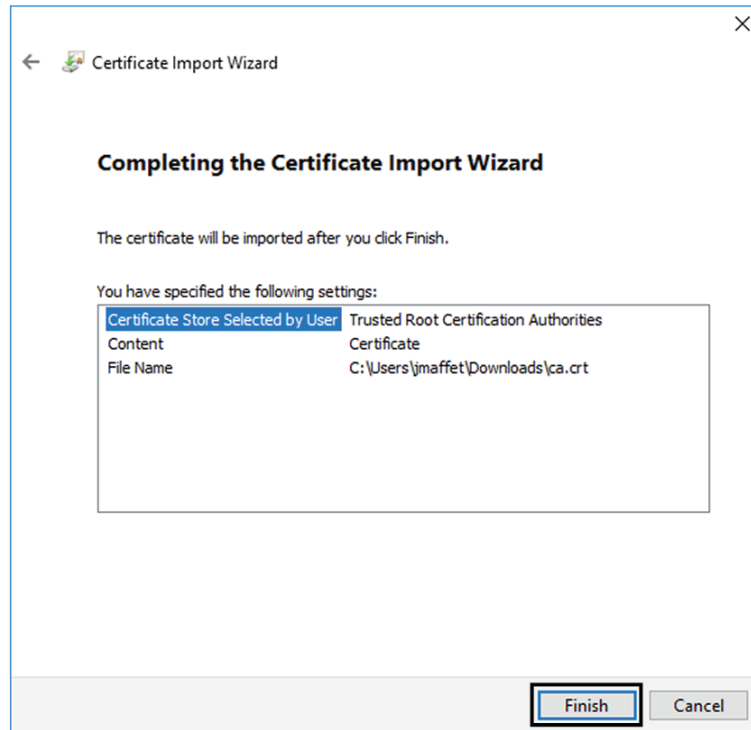
Step 9 Go to the next step.



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



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



What to do next

[Install Cisco Cyber Vision, on page 35](#)

Install Cisco Cyber Vision

Access the Cisco Cyber Vision 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 Cisco Cyber Vision 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

👤 Create the first user 📄 Agree to the license terms ✅ Done

Firstname : Lastname :
 Email :
 Password : Confirm password :
 Suggested password:
 SkvIH2Qq*odz90fj0E3  

[Create](#)

Step 4**Step 5**

Enter the information required.

Note Email will be asked for login access.

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

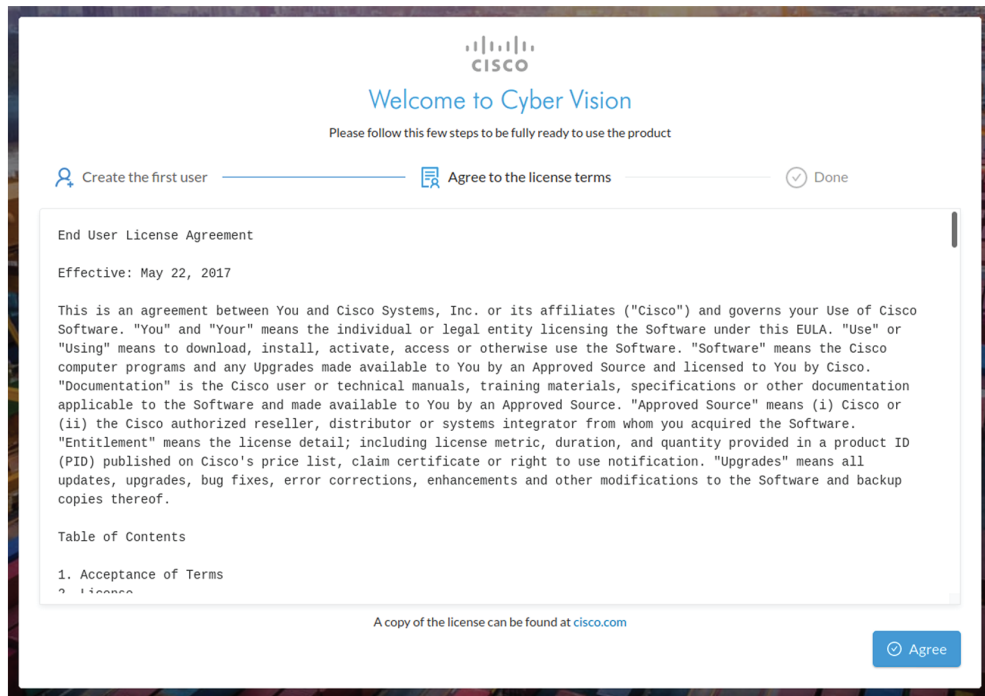
- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#\$%&'()*+,-./:;<=>?@[^_{}.

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

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

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

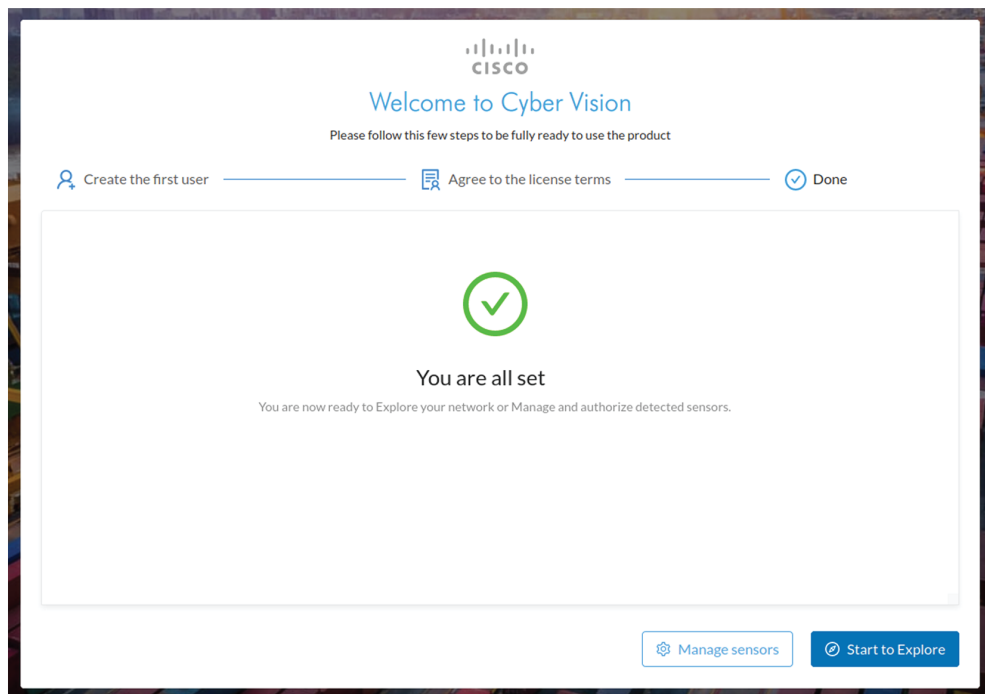
Step 6 **Accept the software license agreement:**

**Step 7****Step 8 Finish the installation:**

The Center is now correctly installed and 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 47](#).

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 52](#).

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

Step 1

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

The screenshot shows the 'Center web server certificate' configuration page in the Cisco Cyber Vision Admin console. The left sidebar contains a navigation menu with 'Center certificate' selected. The main content area shows the following information:

- 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.
- Current Certificate Details:**
 - 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):** [Text input field]
- Upload Area:** A box with the text 'Please import a PKCS#12 file' and an upload icon. Below it, it says '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

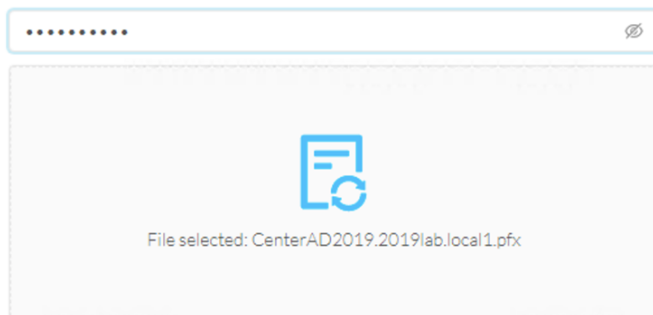
Click Please import a PKCS12 file and choose you pfx or p12 file generated from your certification server.

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)



Save

Step 4 Click Save.

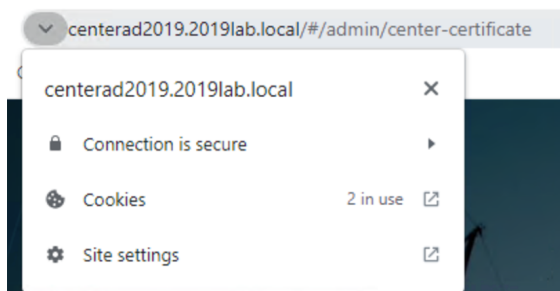
The following message appears:



Step 5 Click Reload.

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

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



What to do next

If you are installing a Global Center or a synchronized Center, proceed with [Configure Center data synchronization, on page 52](#).

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

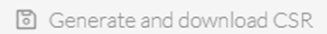
Procedure

Step 1 Select Generate a CSR.

Update with a new web server certificate:

Upload a .p12 Generate a CSR (RSA 2048)

Enter your FQDN

 Generate and download CSR

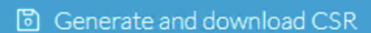
Step 2 Enter the Center FQDN as registered on your DNS server.

Step 3 Click the Generate and download CSR button.

Update with a new web server certificate:

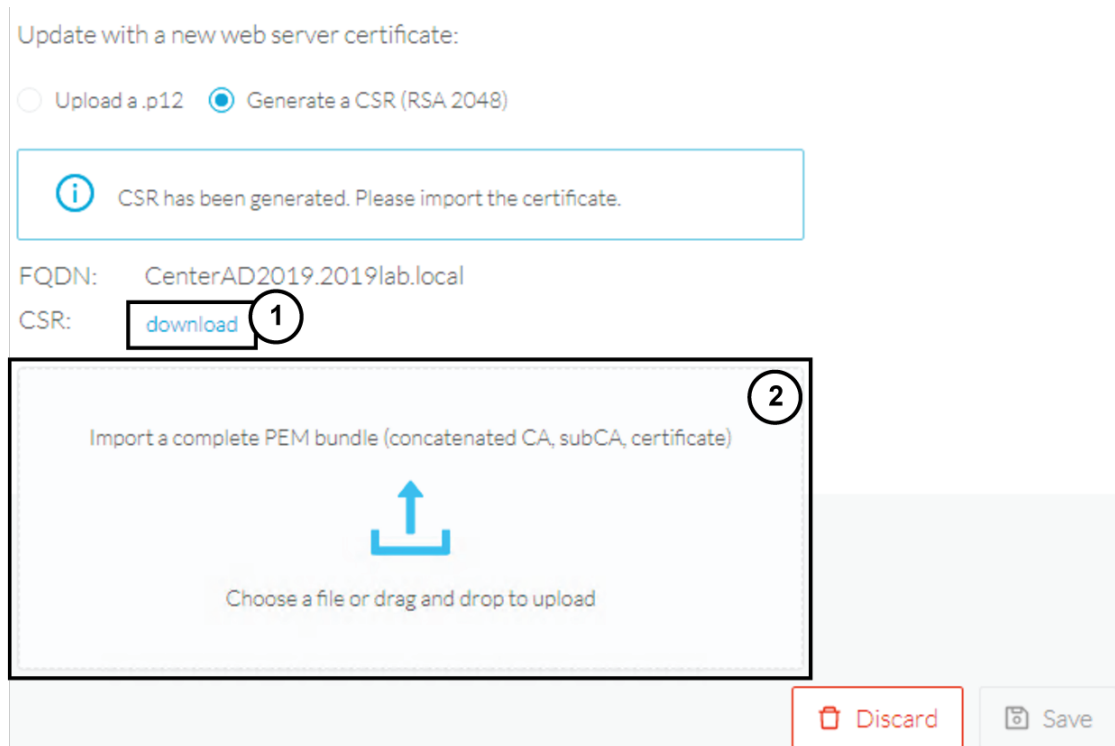
Upload a .p12 Generate a CSR (RSA 2048)

CenterAD2019.2019lab.local

 Generate and download CSR

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

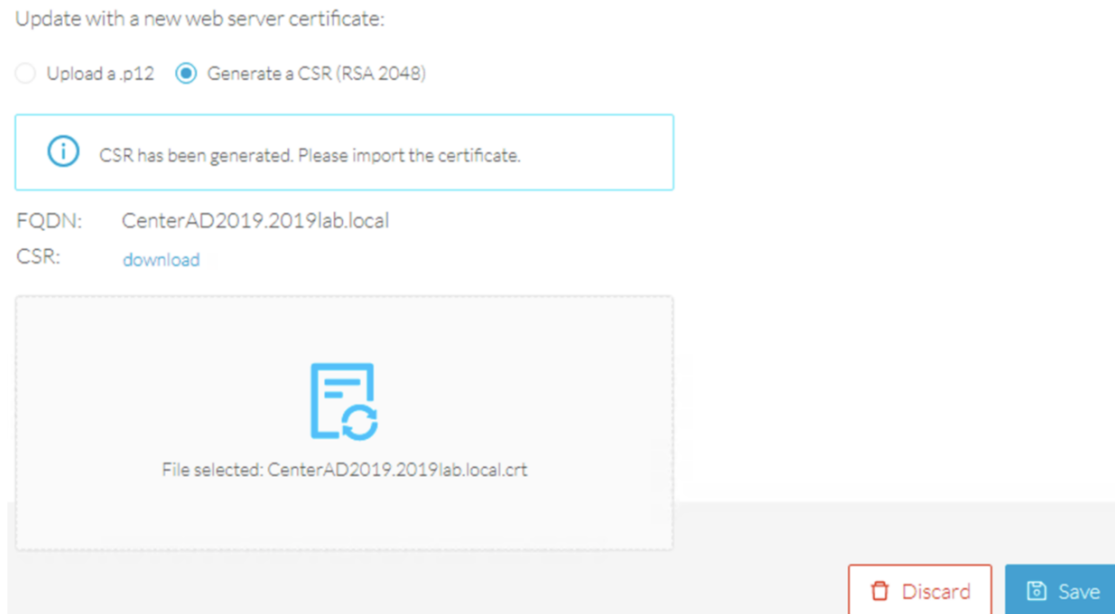
Step 4 Click the download button (1).



A <FQDN>.csr file is downloaded.

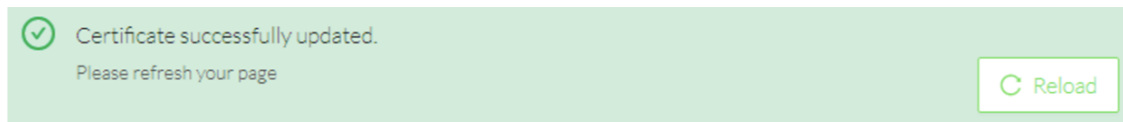
Step 5 Use the <FQDN>.csr file to generate a pem certificate from your enterprise Certification Authority.

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



Step 7 Click Save.

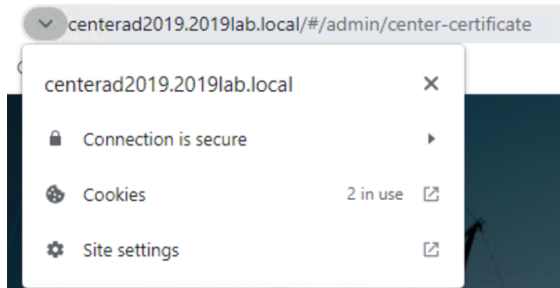
The following message appears:



Step 8 Click Reload.

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

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



What to do next

If you are installing a Global Center or a synchronized Center, proceed with [Configure Center data synchronization, on page 52](#).

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.

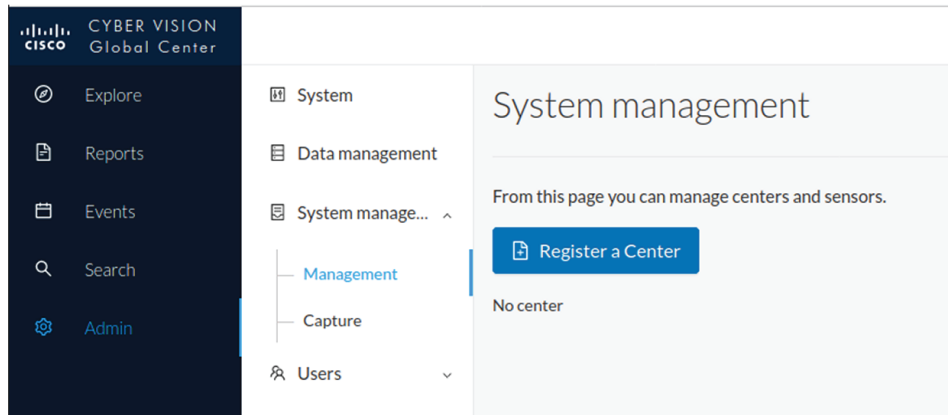


Note To differentiate each user interface, check the top left corner of Cisco Cyber Vision's "Global Center" or "Center".

Procedure

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

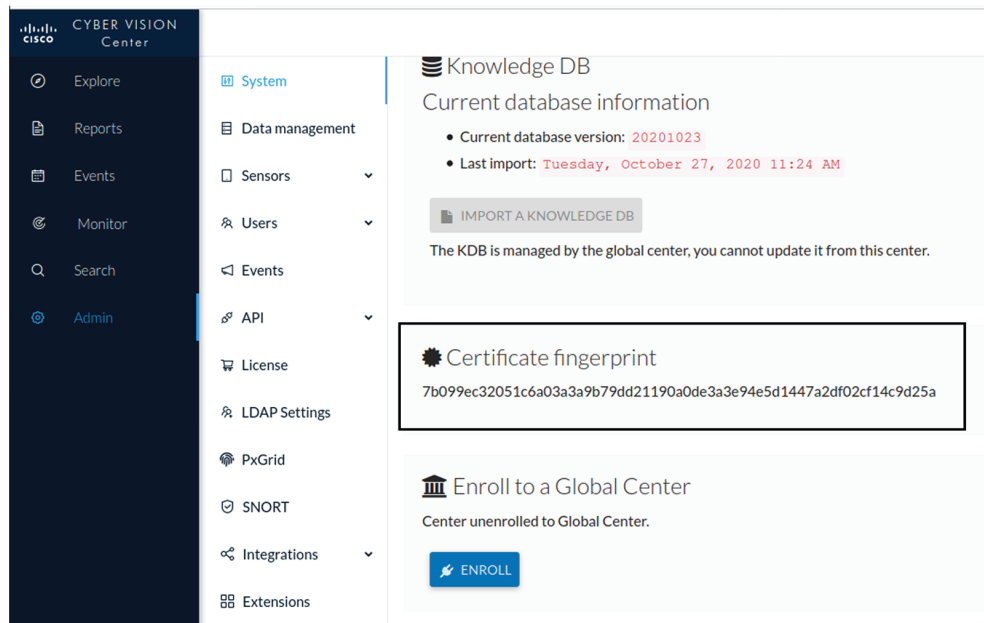
Step 2 Click the **Register a Center** button.



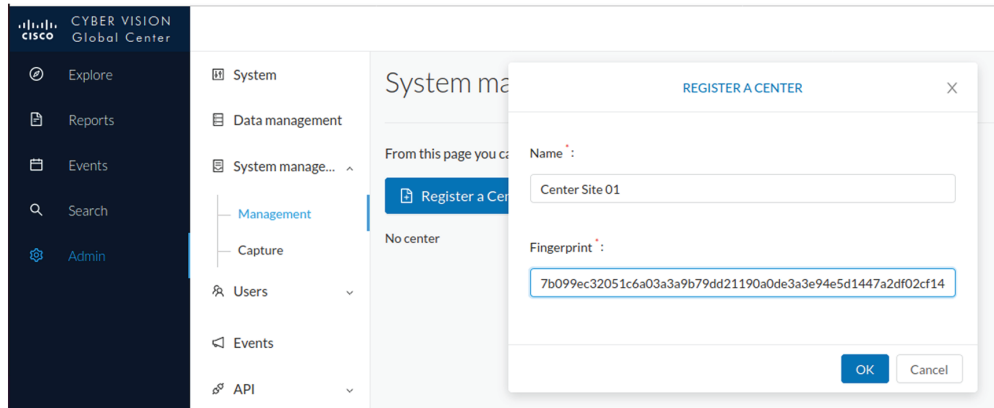
The window "Register a Center" pops up, ready to be filled. Now you must access the Center's GUI to retrieve its fingerprint.

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

Step 4 Scroll down to Certificate fingerprint and copy it.



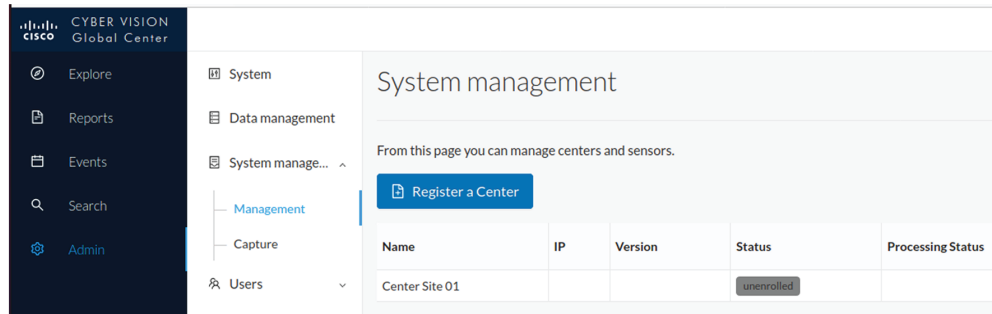
Step 5 In the Global Center's GUI, give a name to the Center, and paste the Center's fingerprint into the corresponding



field

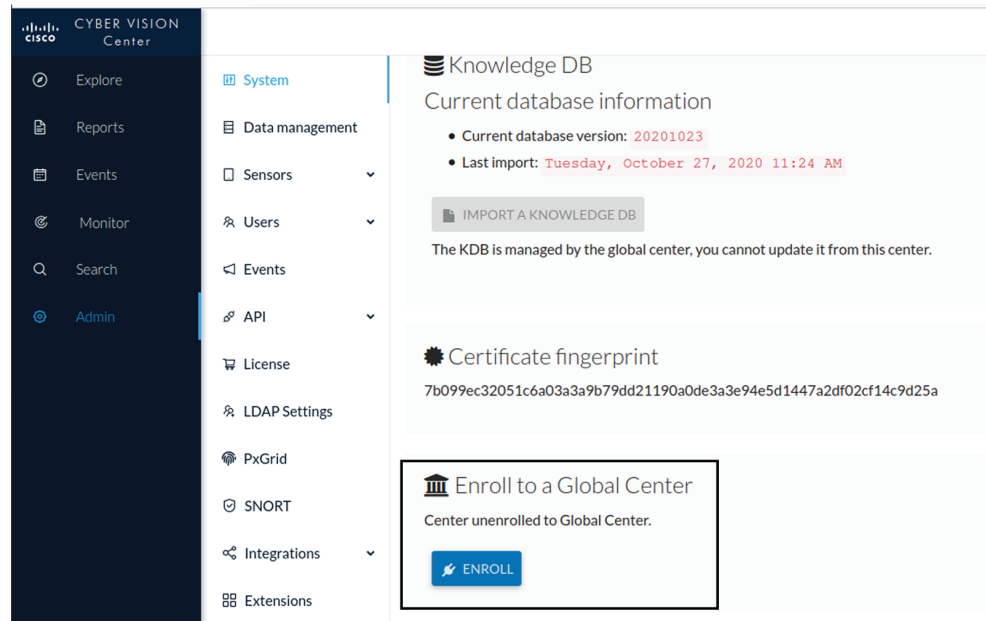
Step 6 Click **OK**.

The Center appears in the list as unenrolled.



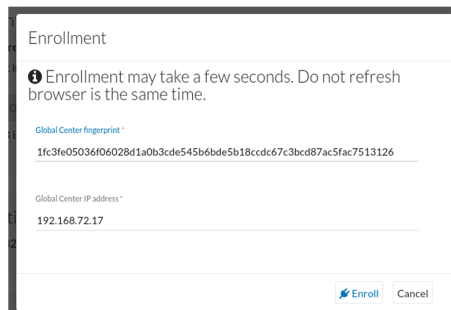
At this point you must switch to the Center's GUI and enroll it to the Global Center.

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



The Enrollment window pops up.

- Step 8** Copy the Global Center's fingerprint from its GUI's System administration page (same location as the Center's).
- Step 9** Enter the Global Center's IP address and click **Enroll**.



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



CHAPTER 6

Deploy sensors

- [Deploy sensors, on page 57](#)

Deploy sensors

On standard conditions:

- No tunnels are configured.
- Both switches and sensors have internet access.

The deployment procedure is the same as described on the sensors installation guides. The only difference is that the Center's public IP address must be specified in the menu below:

Manual sensor installation

The manual sensor installation is provided to install Cisco IOx Sensor, Cisco IC3000 Industrial Compute Gateway and sensors that are not allowed to access the Center's DHCP server for automatic configuration. Please fill the fields below to configure your sensor and generate a provisioning package.

① This package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up or added in the right location of your IOx Application.

Select a hardware model: Cisco IOx Application ▼

Sensor configuration

Serial number : *

Sensor's serial number as printed on the side panel

FCW2445P6X5

Center IP:

Optional, leave blank to use current Center IP address

Gateway:

Optional

Capture mode:

Optional

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

Create Sensor

Cancel



CHAPTER 7

Configure the Cisco Cyber Vision Center synchronization

- [Global Center Configuration, on page 59](#)

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.

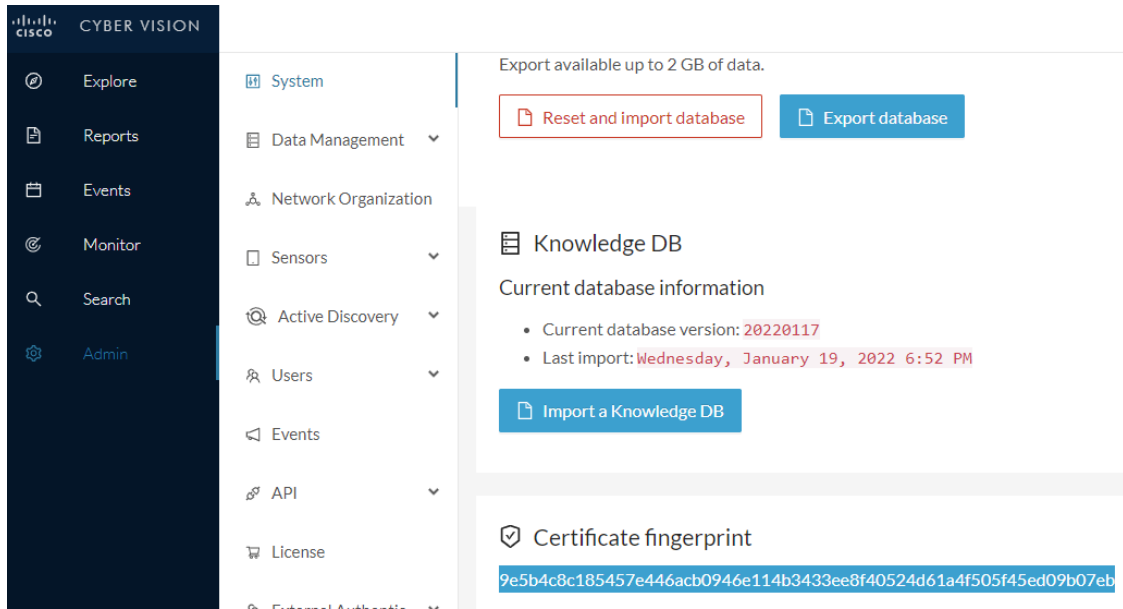
Center enrollment

Before you begin

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

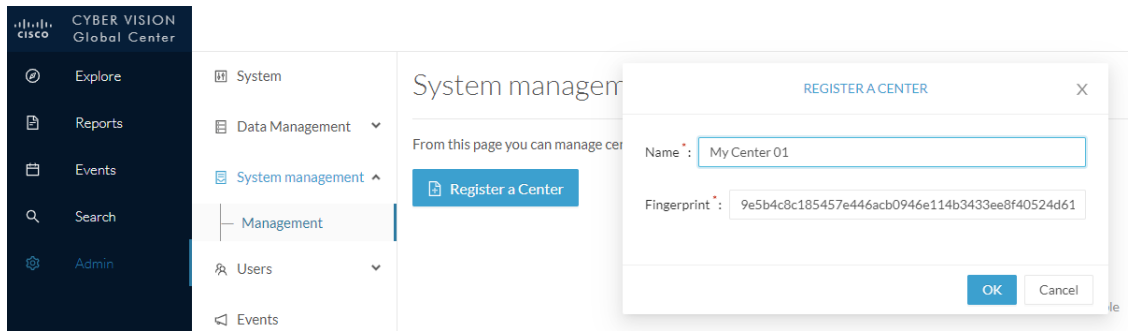
Procedure

- 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.

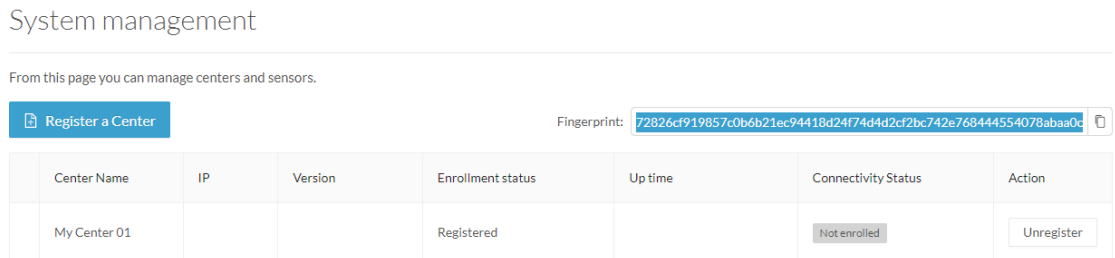


Step 2 Move to the Global Center user interface, Admin menu, in the **System management**, navigate to the **Management** menu. Click on the button **Register a Center** and:

- a) Fill the **Name** field with the name you would like to have for this center
- b) Paste the **Certificate fingerprint** copied above

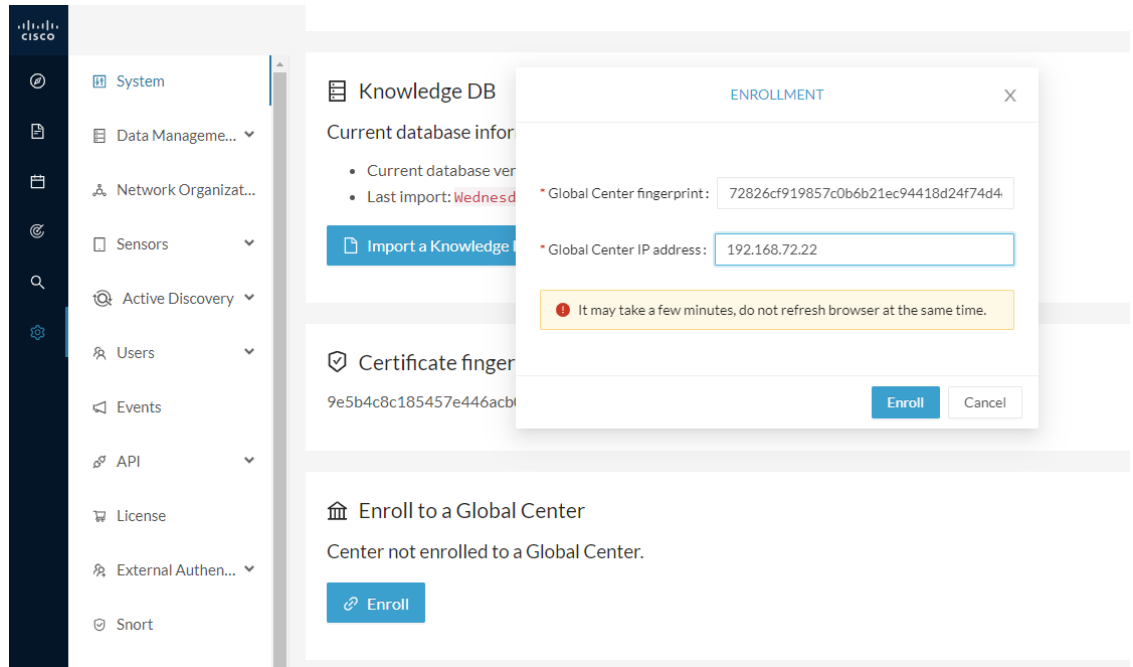


Step 3 Stay in the Global Center, on the same menu (Admin - System management - Management) and copy the **Fingerprint** of the Global Center.

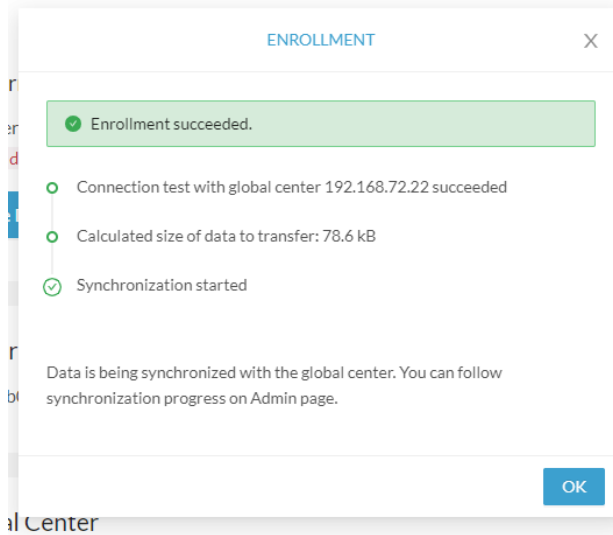


Step 4 On the Center, in the Admin menu, System page, click on the button **Enroll** and:

- a) add the **Global Center fingerprint** (paste it with the value copied above in the Global Center)
- b) add the **Global Center IP address**
- c) press on **Enroll**



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



What to do next

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

System management

From this page you can manage centers and sensors.

Register a Center 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

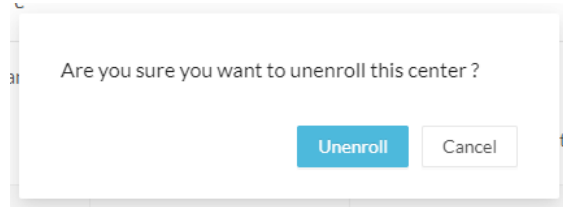
From this page you can manage centers and sensors.

Register a Center 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.



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.

Register a Center Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

Force the unenrollment 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 synchronization 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.

Register a Center 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

Force the unenrollement of a Center



CHAPTER 8

Annex – Setup Center json file

- [Annex – Setup Center json file, on page 65](#)

Annex – Setup Center json file

- keys:
SSH public keys to add in the authorized keys.
- dns:
DNS used by Cisco Cyber Vision. If not specified, Cisco Umbrella is used by default:
<https://docs.umbrella.com/mssp-deployment/docs/point-dns-to-cisco-umbrella>.
- dhcpd-enabled:
Enable or not DHCPD on the Collection network interface. Accepts "true" or "false" as string.
- single-interface:
Deploy Cisco Cyber Vision in single interface mode as default mode.
- center-type:
Type of Cisco Cyber Vision Center to deploy: Standalone (default), Local Center or Global Center.
- center-id:
Specify Center ID. If not provided, a new one is generated at first boot.
- fqdn:
FQDN to access the Cisco Cyber Vision web application. Public IPv4 DNS is used by default.
- ipset:
Configure allowed networks. 169.254.0.0/16 and 0.0.0.0/0 (all networks) are used by default.

Examples:

- To deploy a standalone Center, leave the textbox empty.
- To deploy a Local Center, the minimal configuration is:
{

```
"center-type": "Local Center",  
}
```

- To deploy a Global Center, the minimal configuration is:

```
{  
  "center-type": "Global Center",  
}
```



CHAPTER 9

Center Backup and Restore

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

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

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

- [Backup and Restore Constraints, on page 67](#)
- [Backup Cyber Vision Center, on page 68](#)
- [Restore Cyber Vision Center, on page 68](#)
- [Automate the Backup of the Cyber Vision Center, on page 69](#)
- [Bash Script, on page 70](#)
- [Cron, on page 70](#)

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 which 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 can 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 extension 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 = ZcQ1awWIsn3NprBf0mFEb4cwE1MYHXcJ-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 below::

- `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>
```