Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.1.0

First Published: 2021-01-01

Last Modified: 2021-01-01

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

CONTENTS

CHAPTER 1

About this documentation

Document purpose

Amazon VirtualPrivate Cloud (Amazon VPC) enables you to launch Amazon WebServices (AWS) resources into a virtual network that you define. This virtual network closely resembles a traditional network that might operate in your own data center, 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 4.1.0**.

Warnings and notices

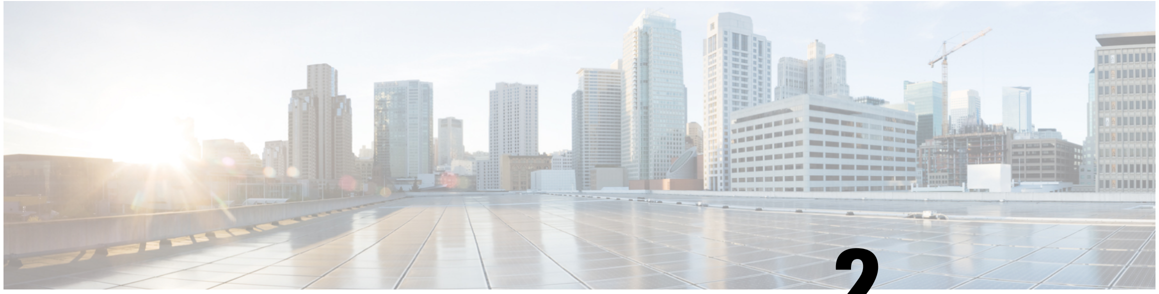
This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

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

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 AMI available for Cisco Cyber Vision instance.
- 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
- Center with sync
- Global Center

Limitations

The following features or hardwares are not supported:

- Dual interface Centers.
- Sensors using the sensor management extension.
- Cisco IC3000 ssh access from Center.

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

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.

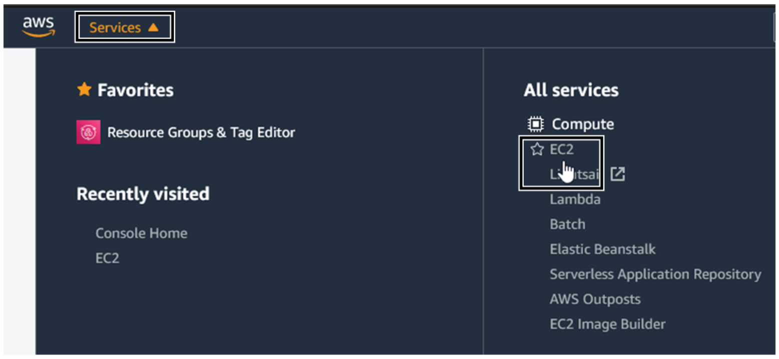
Refer to https://aws.amazon.com/documentation/gettingstarted/ for more information.

Create Elastic IPs

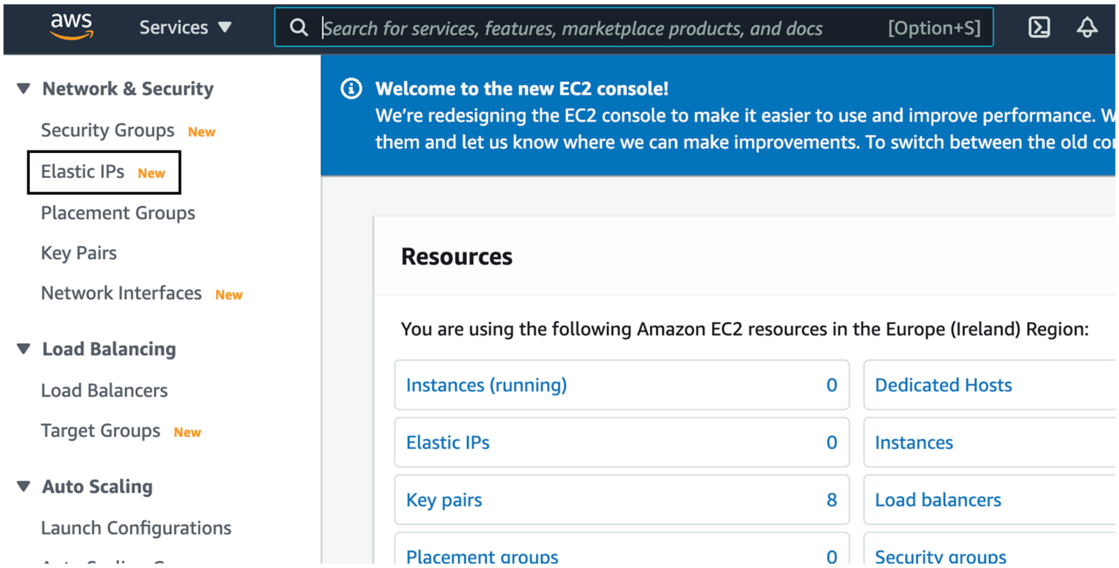
When an instance is created, a public IP address is associated with the instance. That public IP address changes automatically when you stop and start the instance. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. Elastic IPs are reserved public 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.



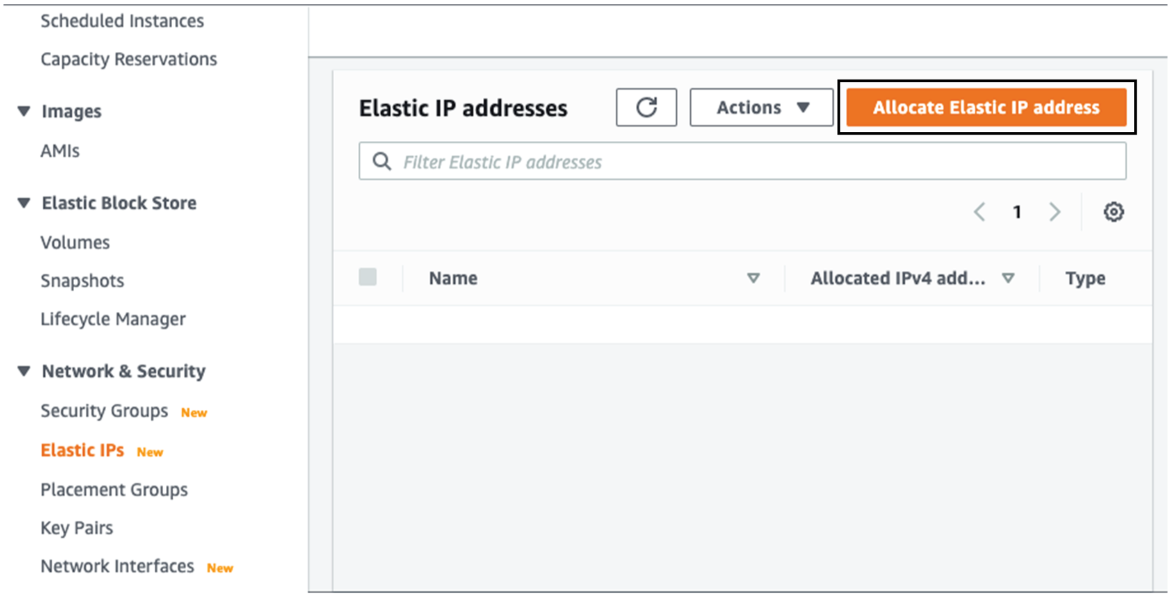
Welcome to the new EC2 console!
We're redesigning the EC2 console to make it easier to use and improve performance. W
them and let us know where we can make improvements. To switch between the old co

Resources

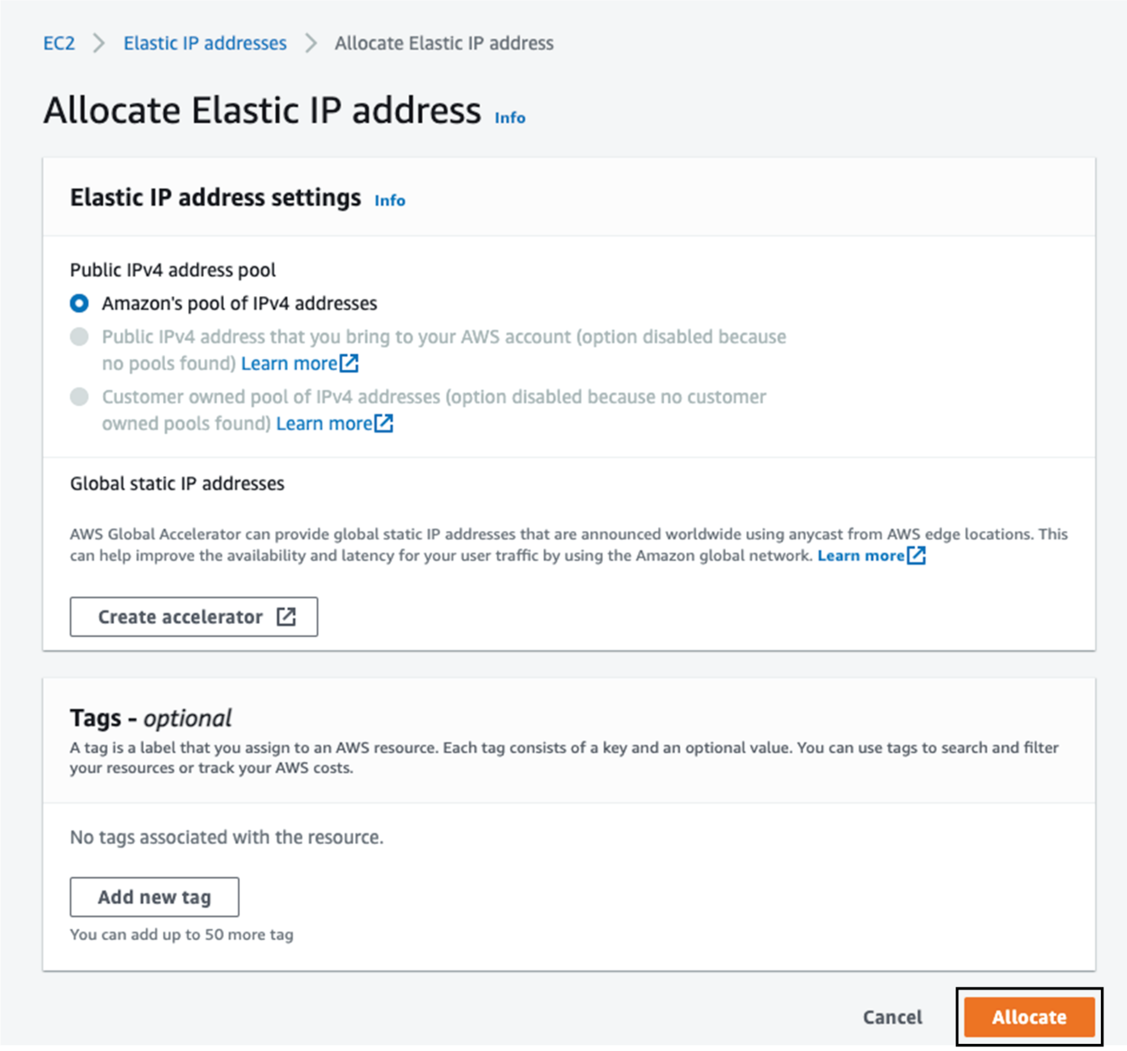
You are using the following Amazon EC2 resources in the Europe (Ireland) Region:

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

4. Click Allocate Elastic IP address.



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.

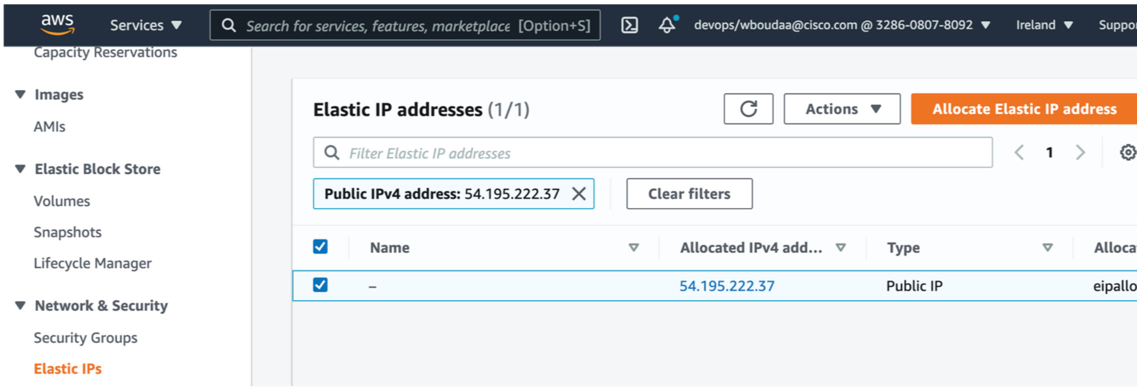
No tags associated with the resource.

Add new tag

You can add up to 50 more tag

Cancel Allocate

6. Check the new Elastic IP out.



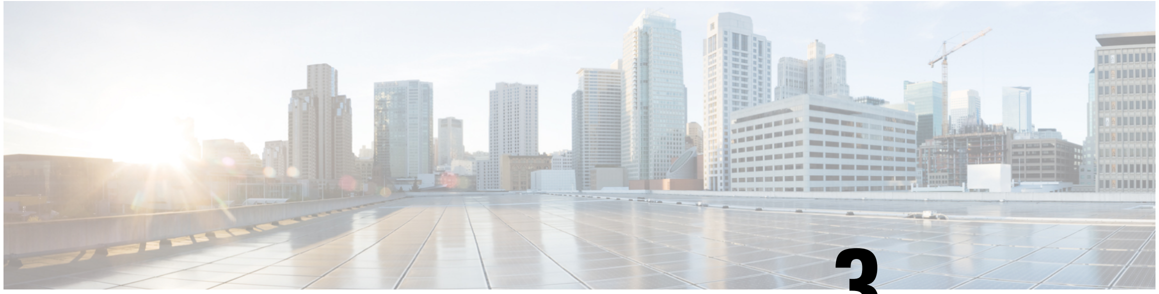
Elastic IP addresses (1/1)

Actions ▼ Allocate Elastic IP address

Filter Elastic IP addresses

Public IPv4 address: 54.195.222.37 Clear filters

☑	Name	Allocated IPv4 add...	Type	Alloca
☑	–	54.195.222.37	Public IP	eipallo

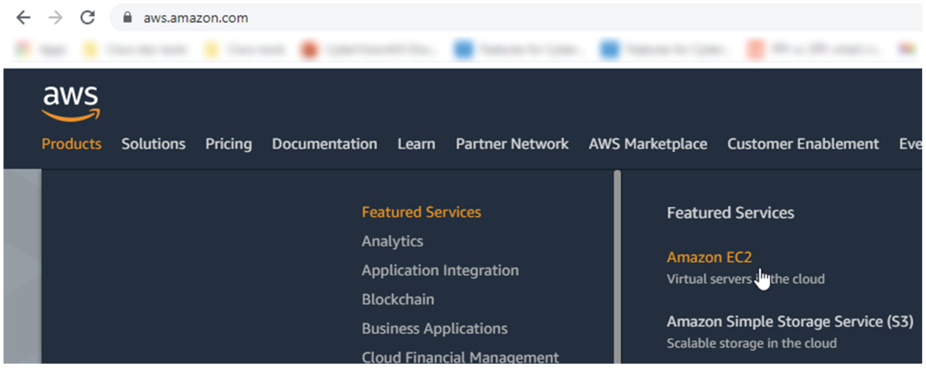


CHAPTER 3

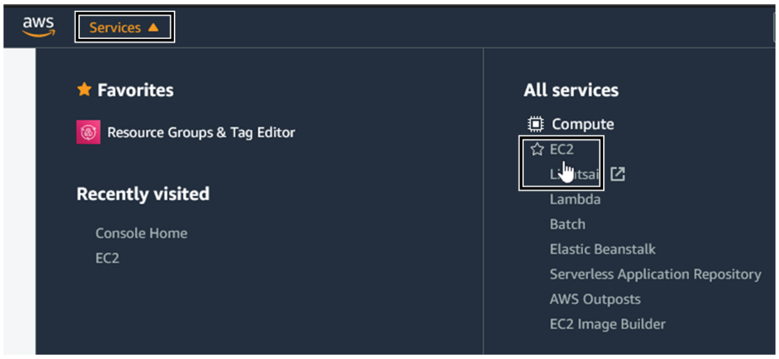
Deploy the Cisco Cyber Vision Center

Create and configure the instance

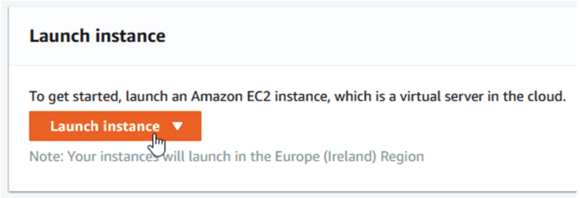
1. Go to https://aws.amazon.com Amazon Web Services and sign in.



2. Navigate to Services > EC2.



3. Click Launch Instance.

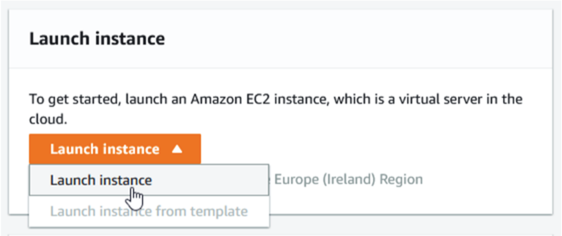


Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Europe (Ireland) Region

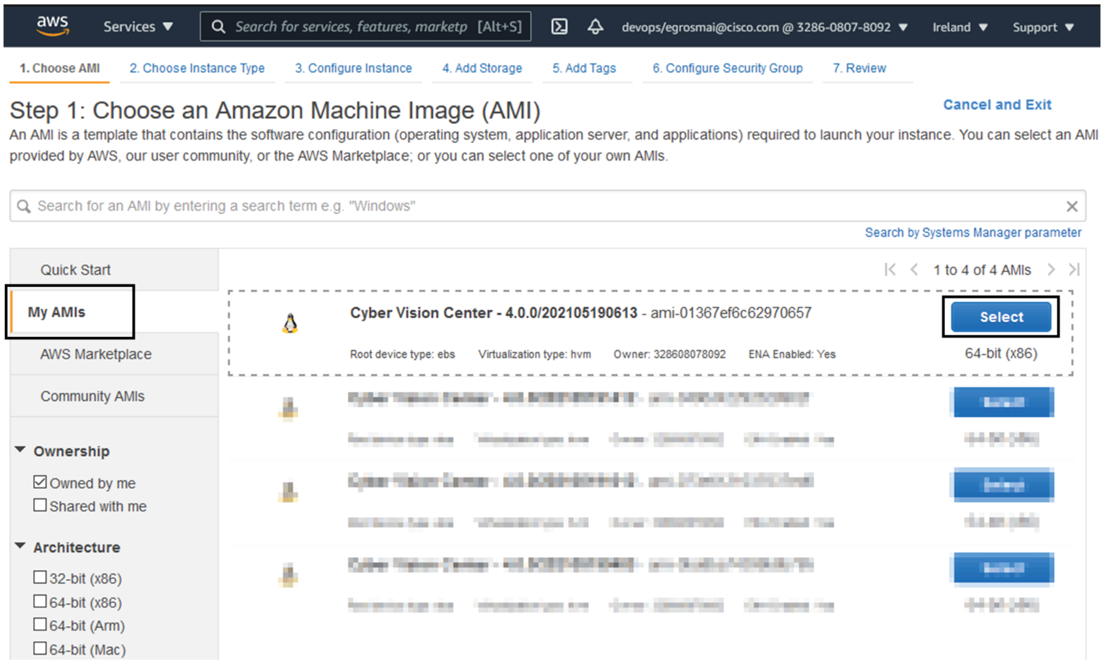
4. Click Launch Instance again.



Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

5. Choose your Cisco Cyber Vision AMI from the AWS Marketplace and click Select.



Step 1: Choose an Amazon Machine Image (AMI)

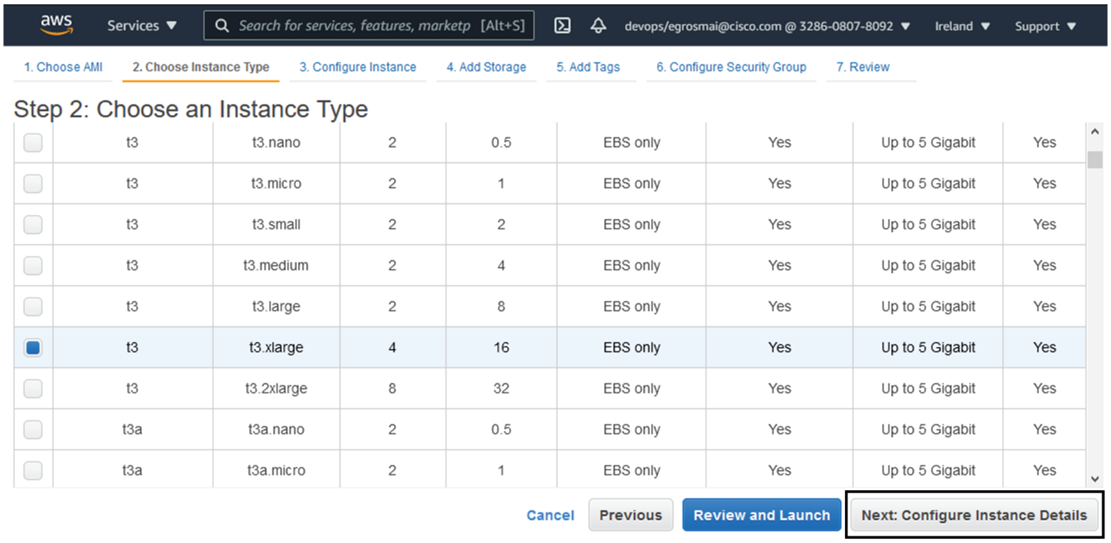
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Cyber Vision Center - 4.0.0/202105190613 - ami-01367ef6c62970657

Root device type: ebs Virtualization type: hvm Owner: 328608078092 ENA Enabled: Yes 64-bit (x86)

Note In the example above, the image is mapped with sample AMIs. Those images are for internal use. You will find the image in the AWS marketplace using the keyword "Cisco Cyber Vision". The correct version to use should appear.

6. Choose the instance type from the available list and click Next.



Step 2: Choose an Instance Type

☐	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
☑	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Supported instance families

- 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

VM sizing

Minimum – up to 500 components:

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

Recommended:

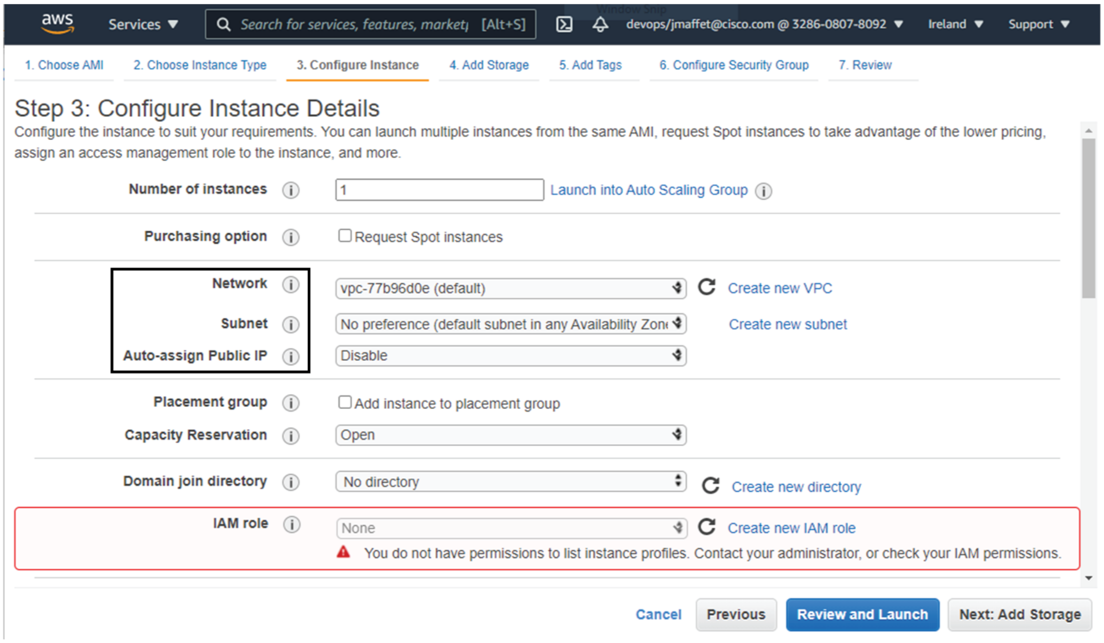
For 10,000 components w/o Center DPI:

- 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

1. Configure instance details.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-77b96d0e (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Zon — Create new subnet

Auto-assign Public IP: Disable

Placement group: □ Add instance to placement group

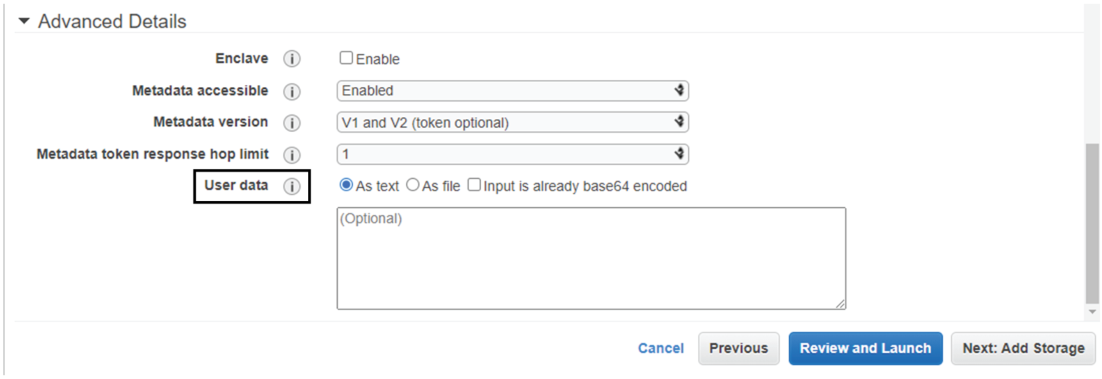
Capacity Reservation: Open

Domain join directory: No directory — Create new directory

IAM role: None — Create new IAM role

You do not have permissions to list instance profiles. Contact your administrator, or check your IAM permissions.

2. Choose the VPC and the subnet network.
3. The public IP address should be disabled. An Elastic IP will be associated to the Cisco Cyber Vision instance to avoid any Dynamic public IP issues. The Public IP address association will be described later in this section.
4. Depending on the Center type you can fill the Advanced Details > User data part at the bottom of Configure Instance Details menu.



Advanced Details

Enclave ⓘ □ Enable

Metadata accessible ⓘ Enabled

Metadata version ⓘ V1 and V2 (token optional)

Metadata token response hop limit ⓘ 1

User data ⓘ ● As text ○ As file □ Input is already base64 encoded

(Optional)

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:

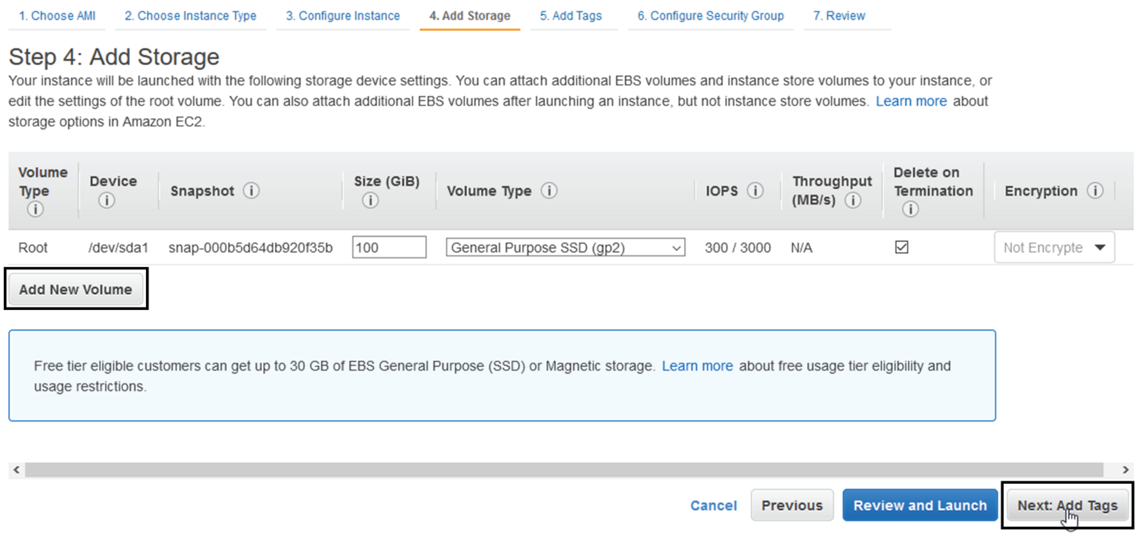
  {

  "center-type": "Global Center",

  }

  For all json parameters, refer to Annex – Setup Center json file.

5. Click Next: Add Storage.
6. If needed, click the button to add a new volume.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-000b5d64db920f35b	100	General Purpose SSD (gp2)	300 / 3000	N/A	☑	Not Encrypte

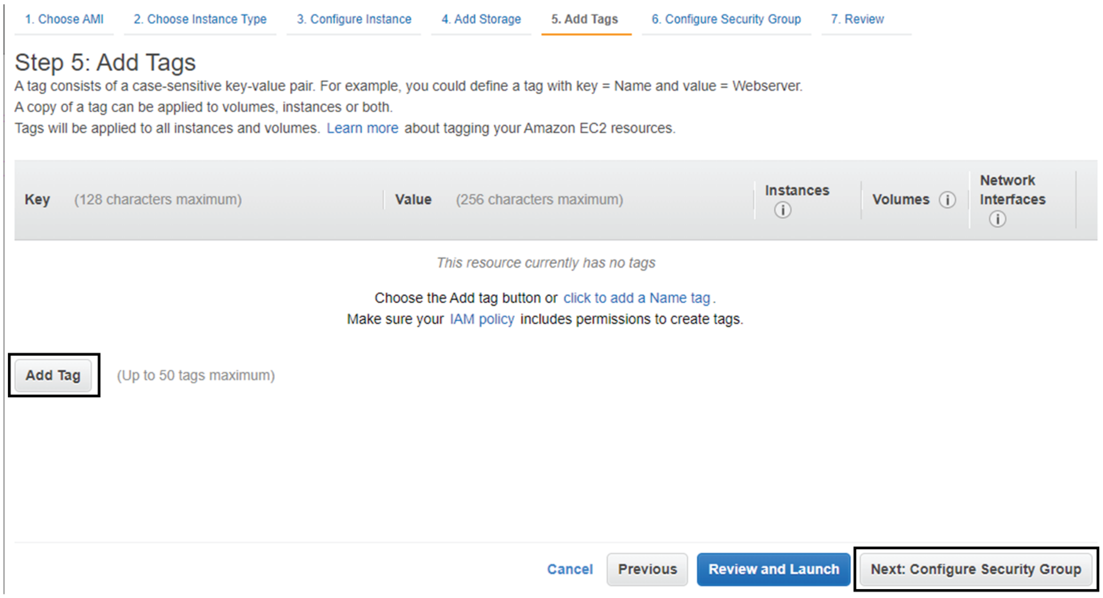
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

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.

7. You can add tags to identify resources internally on AWS.



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ	Network Interfaces ⓘ

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

8. 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

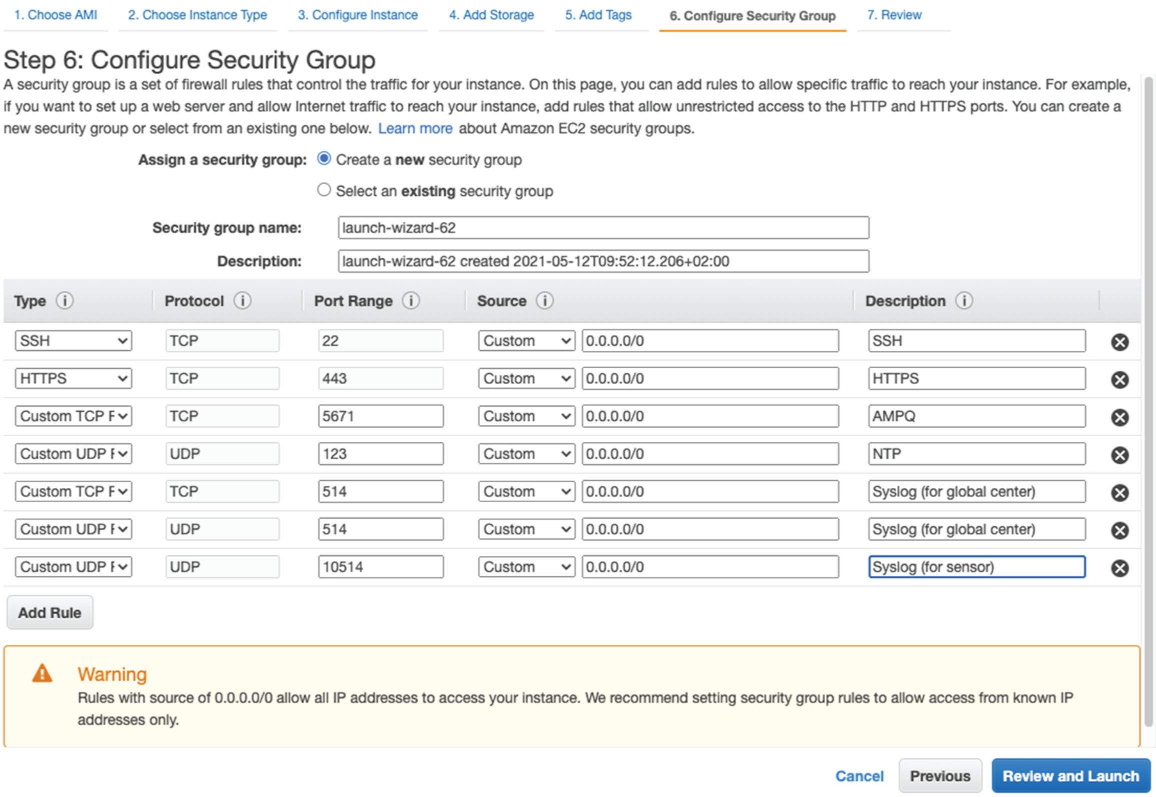
Protocol	Port
HTTPS	TCP/443
SSH	TCP/22
NTP	UDP/123

For Sensor à Center communication

Protocol	Port
AMPQ	TCP/5671

Protocol	Port
Syslog	UDP/10514

Example of a security configuration:



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: launch-wizard-62

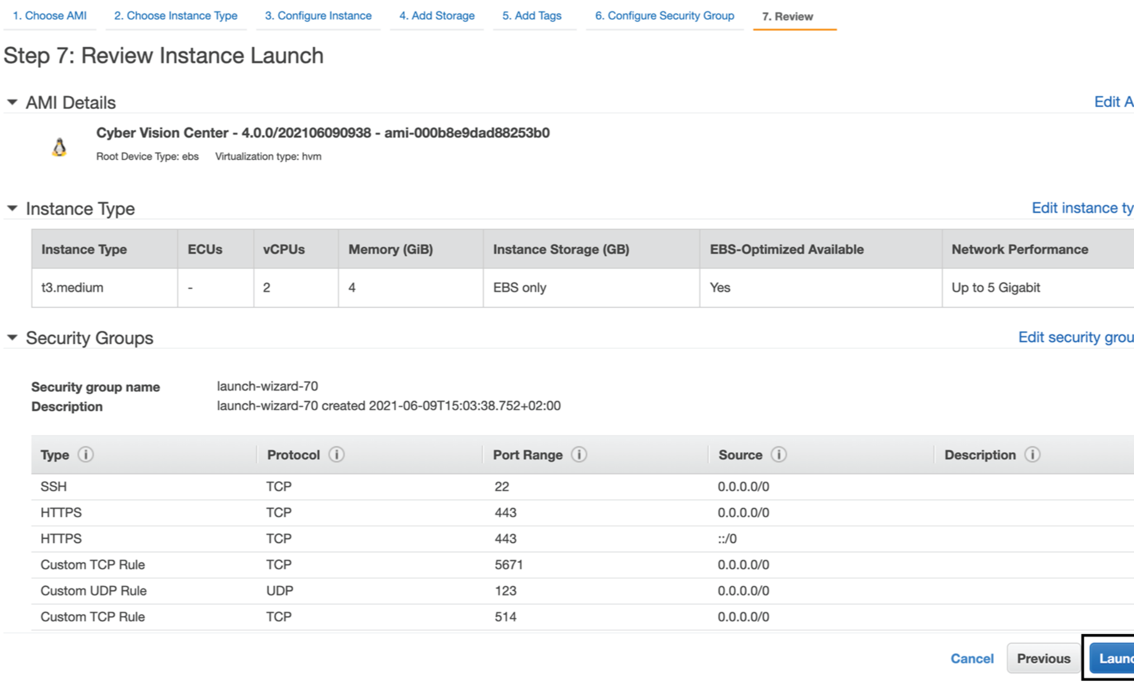
Description: launch-wizard-62 created 2021-05-12T09:52:12.206+02:00

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	SSH
HTTPS	TCP	443	Custom	0.0.0.0/0	HTTPS
Custom TCP F	TCP	5671	Custom	0.0.0.0/0	AMPQ
Custom UDP F	UDP	123	Custom	0.0.0.0/0	NTP
Custom TCP F	TCP	514	Custom	0.0.0.0/0	Syslog (for global center)
Custom UDP F	UDP	514	Custom	0.0.0.0/0	Syslog (for global center)
Custom UDP F	UDP	10514	Custom	0.0.0.0/0	Syslog (for sensor)

⚠ Warning

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.

1. Review your settings and click Launch.



1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 7: Review Instance Launch

▾ AMI Details — Edit A

Cyber Vision Center - 4.0.0/202106090938 - ami-000b8e9dad88253b0

Root Device Type: ebs   Virtualization type: hvm

▾ Instance Type — Edit instance ty

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t3.medium	-	2	4	EBS only	Yes	Up to 5 Gigabit

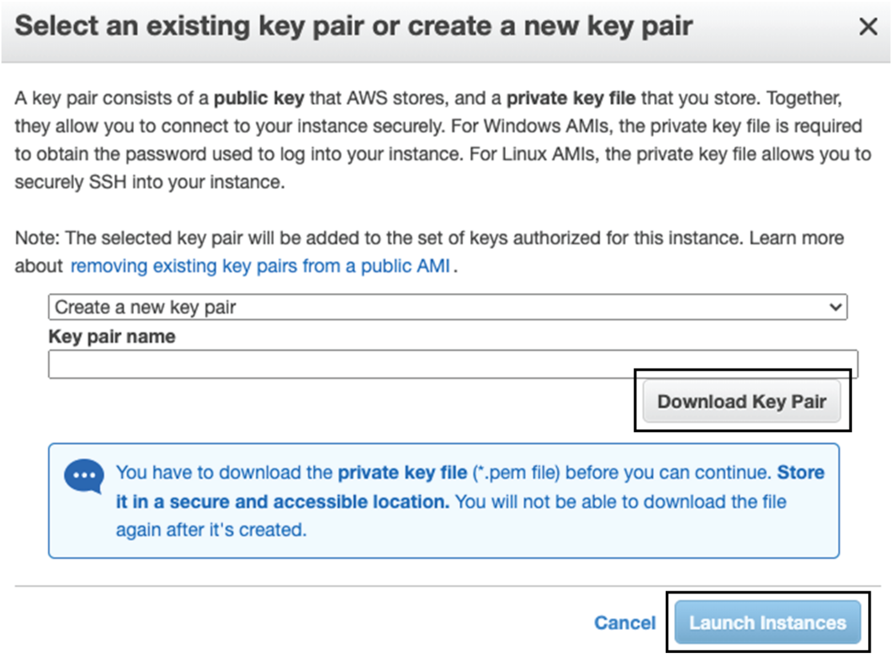
▾ Security Groups — Edit security grou

Security group name: launch-wizard-70

Description: launch-wizard-70 created 2021-06-09T15:03:38.752+02:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	
HTTPS	TCP	443	::/0	
Custom TCP Rule	TCP	5671	0.0.0.0/0	
Custom UDP Rule	UDP	123	0.0.0.0/0	
Custom TCP Rule	TCP	514	0.0.0.0/0	

2. Select or create a new key pair for the SSH connection.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

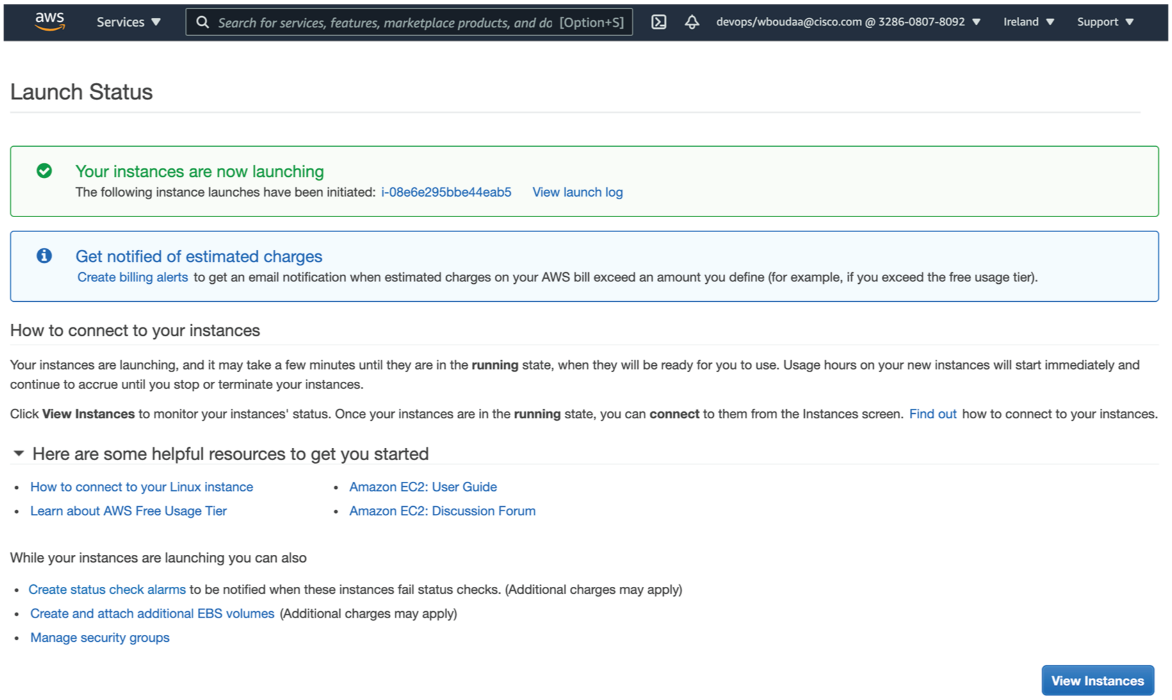
You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

3. Click Download Key Pair. A file called YOURKEYPAIRNAME.pem will be downloaded.

4. Then, click Launch Instance.

Allocate an Elastic IP to the instance

1. Click View Instances.



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

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-08e6e295bbe44eab5 View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

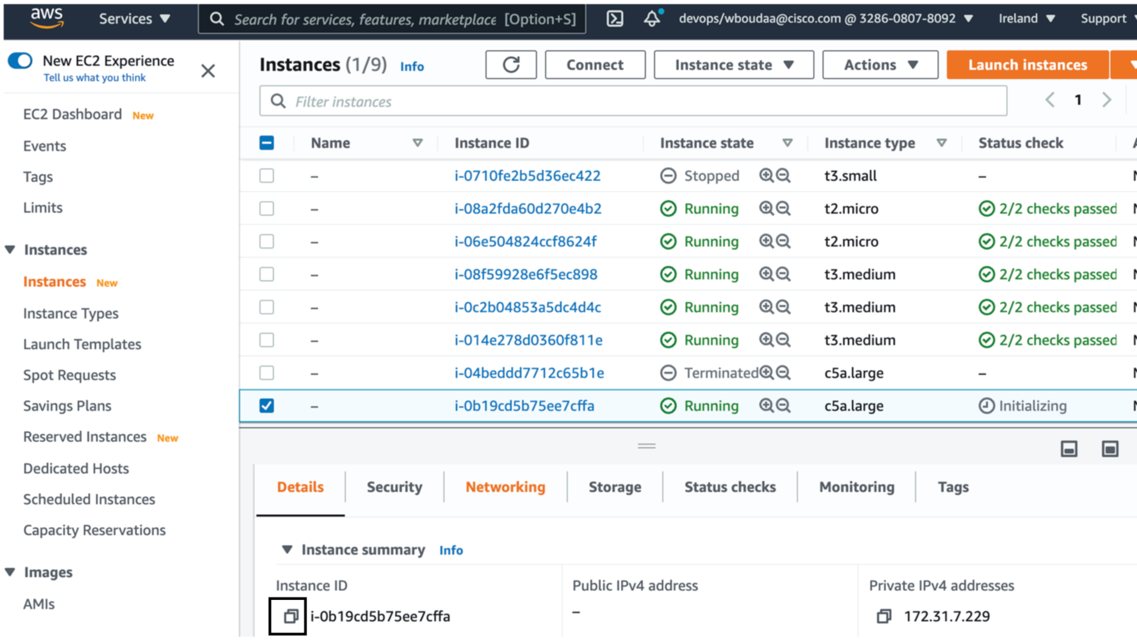
Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

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



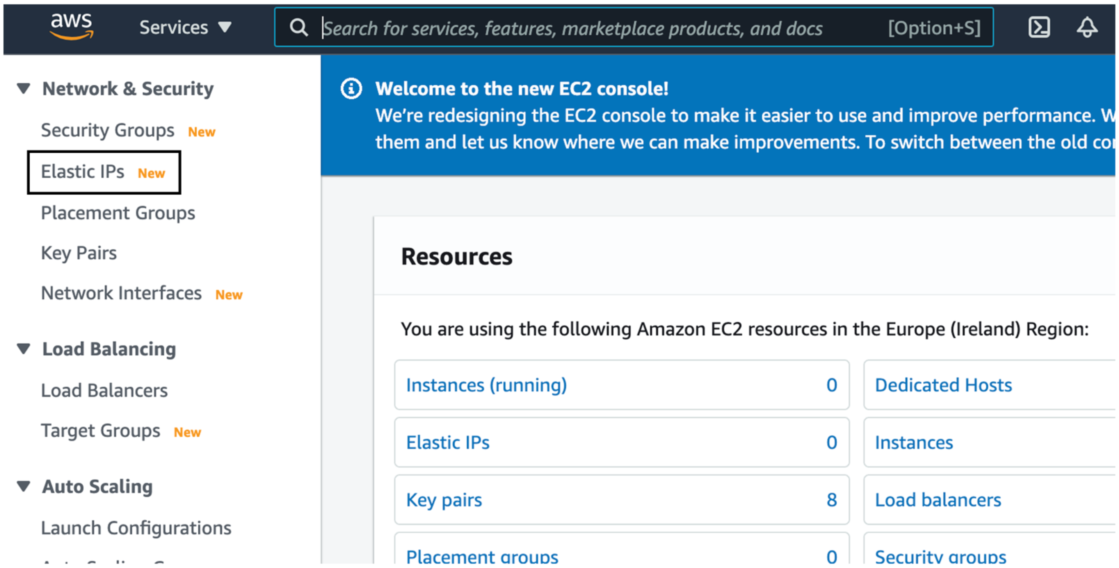
Instances (1/9) Info

	Name	Instance ID	Instance state	Instance type	Status check
□	–	i-0710fe2b5d36ec422	Stopped	t3.small	–
□	–	i-08a2fda60d270e4b2	Running	t2.micro	2/2 checks passed
□	–	i-06e504824ccf8624f	Running	t2.micro	2/2 checks passed
□	–	i-08f59928e6f5ec898	Running	t3.medium	2/2 checks passed
□	–	i-0c2b04853a5dc4d4c	Running	t3.medium	2/2 checks passed
□	–	i-014e278d0360f811e	Running	t3.medium	2/2 checks passed
□	–	i-04beddd7712c65b1e	Terminated	c5a.large	–
☑	–	i-0b19cd5b75ee7cffa	Running	c5a.large	Initializing

▼ Instance summary Info

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

3. Go to Elastic IP.



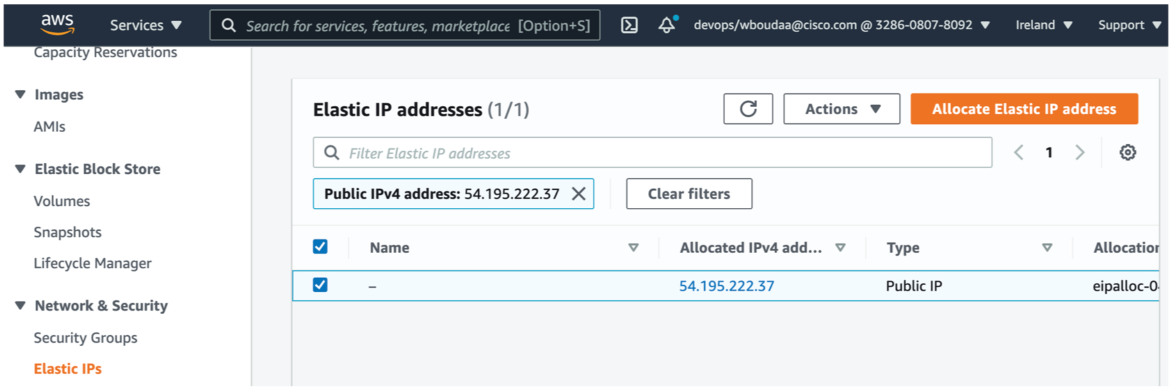
Welcome to the new EC2 console!
We're redesigning the EC2 console to make it easier to use and improve performance. W
them and let us know where we can make improvements. To switch between the old co

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)

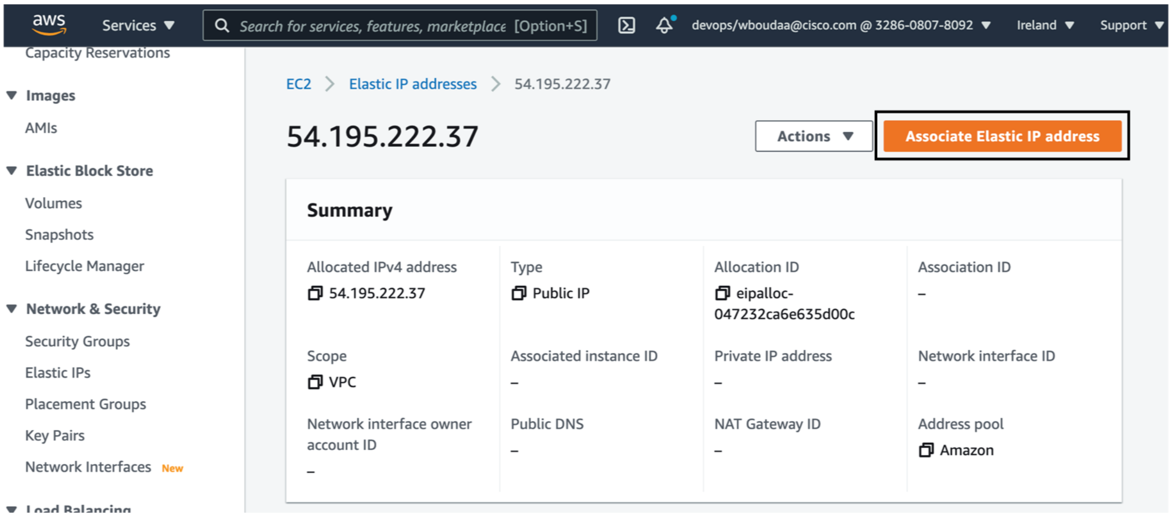
Actions ▼ Allocate Elastic IP address

Filter Elastic IP addresses

Public IPv4 address: 54.195.222.37 ✕ Clear filters

☑	Name	Allocated IPv4 add...	Type	Allocation
☑	–	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

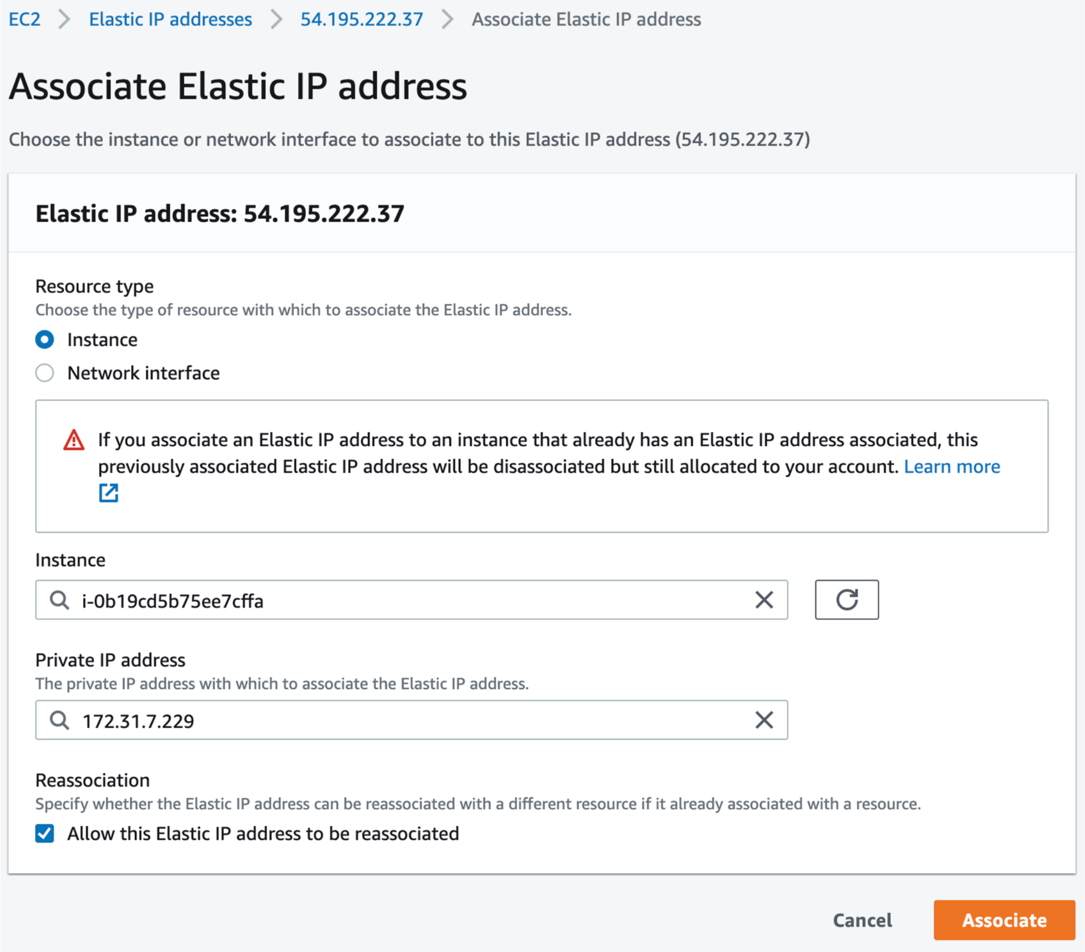
54.195.222.37

Actions ▼ Associate Elastic IP address

Summary

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

6. Tick Instance.
7. Paste the instance ID previously copied.
8. Type 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
i-0b19cd5b75ee7cffa

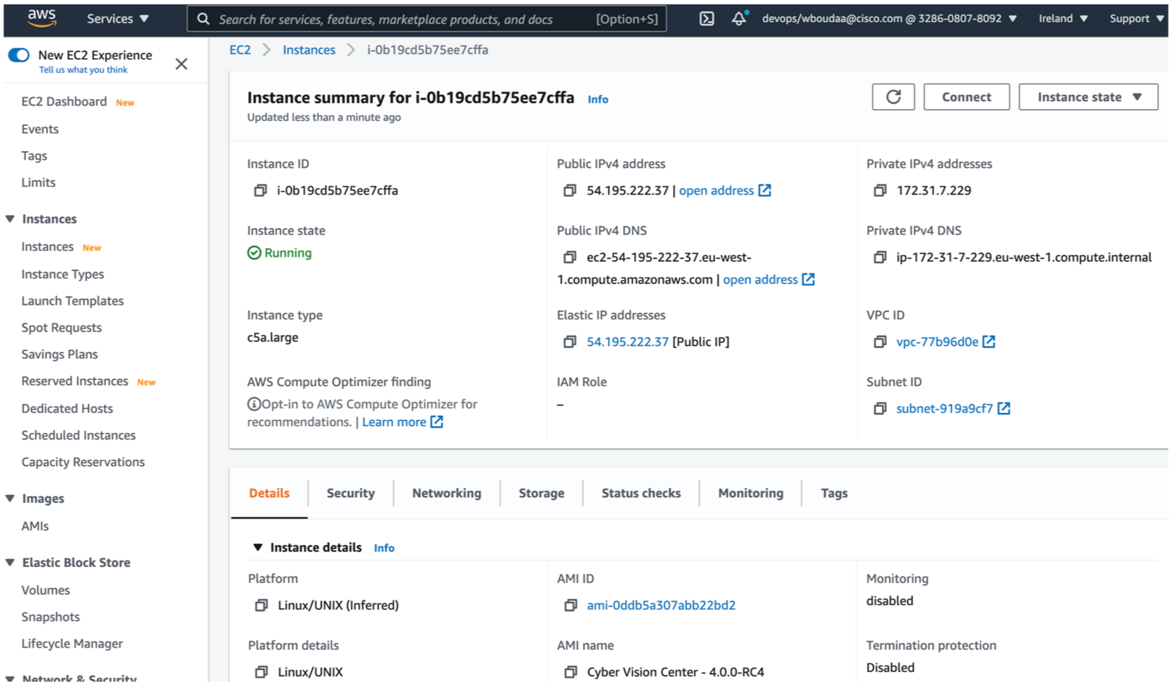
Private IP address
The private IP address with which to associate the Elastic IP address.
172.31.7.229

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

Cisco Cyber Vision Center setup

Open an SSH connection from AWS

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



Instance summary for i-0b19cd5b75ee7cffa Info

Updated less than a minute ago

Instance ID: i-0b19cd5b75ee7cffa

Public IPv4 address: 54.195.222.37 | open address

Private IPv4 addresses: 172.31.7.229

Instance state: Running

Public IPv4 DNS: ec2-54-195-222-37.eu-west-1.compute.amazonaws.com | open address

Private IPv4 DNS: ip-172-31-7-229.eu-west-1.compute.internal

Instance type: c5a.large

Elastic IP addresses: 54.195.222.37 [Public IP]

VPC ID: vpc-77b96d0e

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role: –

Subnet ID: subnet-919a9cf7

▼ Instance details Info

Platform: Linux/UNIX (Inferred)

AMI ID: ami-0ddb5a307abb22bd2

Monitoring: disabled

Platform details: Linux/UNIX

AMI name: Cyber Vision Center - 4.0.0-RC4

Termination protection: Disabled

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

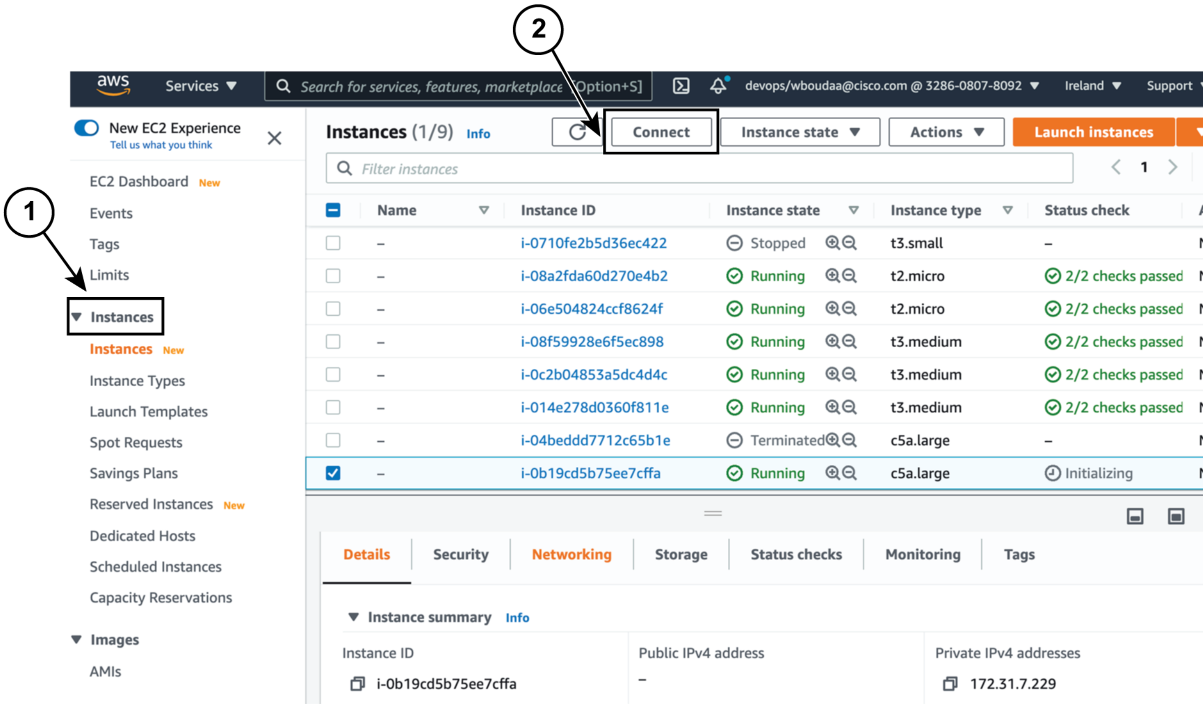
Note It is possible to add multiple keys on that file if an access is needed from another device that is not using the same certificates than the installed one.

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)**.

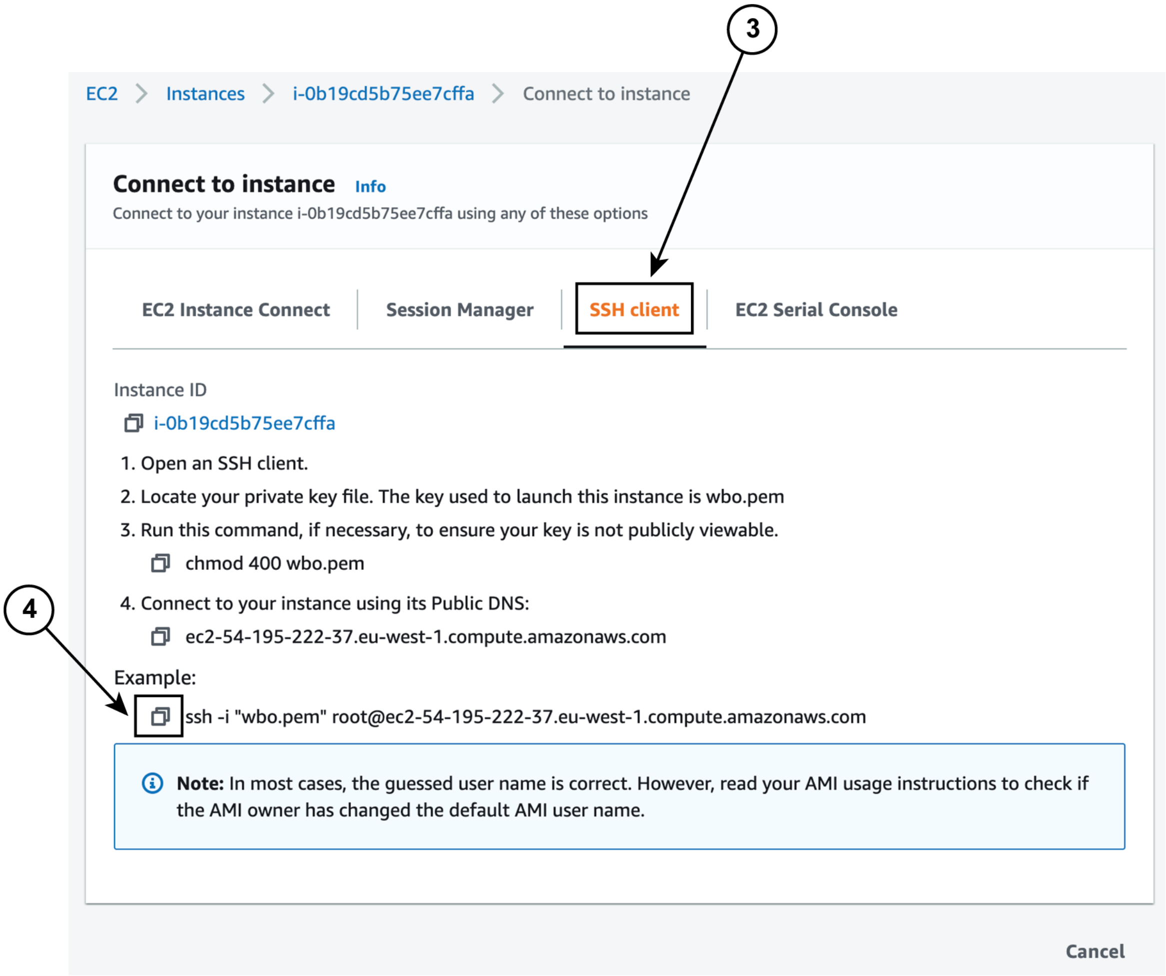
3. Choose the needed instance and click the Connect button **(2)**.



	Name	Instance ID	Instance state	Instance type	Status check
□	–	i-0710fe2b5d36ec422	Stopped	t3.small	–
□	–	i-08a2fda60d270e4b2	Running	t2.micro	2/2 checks passed
□	–	i-06e504824ccf8624f	Running	t2.micro	2/2 checks passed
□	–	i-08f59928e6f5ec898	Running	t3.medium	2/2 checks passed
□	–	i-0c2b04853a5dc4d4c	Running	t3.medium	2/2 checks passed
□	–	i-014e278d0360f811e	Running	t3.medium	2/2 checks passed
□	–	i-04beddd7712c65b1e	Terminated	c5a.large	–
☑	–	i-0b19cd5b75ee7cffa	Running	c5a.large	Initializing

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

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



Connect to instance

Connect to your instance i-0b19cd5b75ee7cffa using any of these options

Instance ID

i-0b19cd5b75ee7cffa

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is wbo.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.

```
chmod 400 wbo.pem
```

4. Connect to your instance using its Public DNS:

```
ec2-54-195-222-37.eu-west-1.compute.amazonaws.com
```

Example:

```
ssh -i "wbo.pem" root@ec2-54-195-222-37.eu-west-1.compute.amazonaws.com
```

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

5. Copy and paste the example **(4)** into the ssh client and replace the 'root' with 'cv-admin', like below:

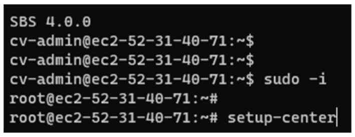
   ssh -i wbo.pem cv-admin@ec2-54-195-222-376.eu-west-1.compute.amazonaws.com

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
```

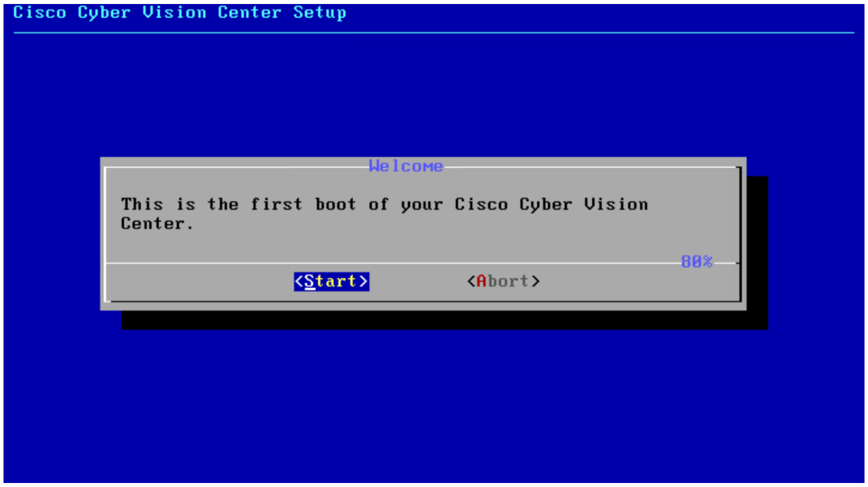
8. Press enter.

   The basic Center configuration appears.

Basic Center configuration

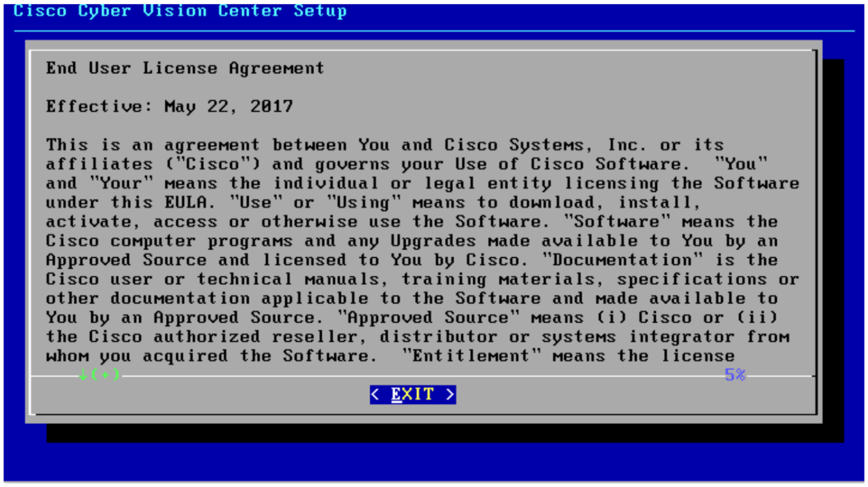
Access the basic Center configuration

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

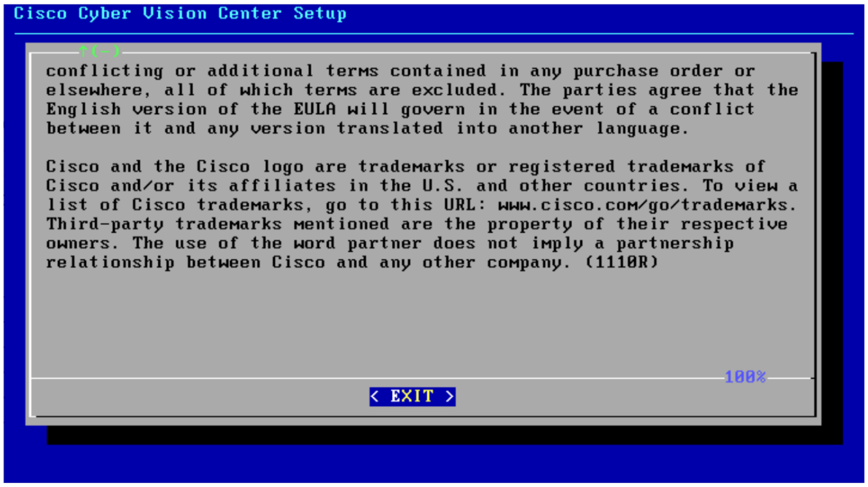


```
Cisco Cyber Vision Center Setup

                         Welcome

 This is the first boot of your Cisco Cyber Vision
 Center.
                                                  80%
             <Start>            <Abort>
```

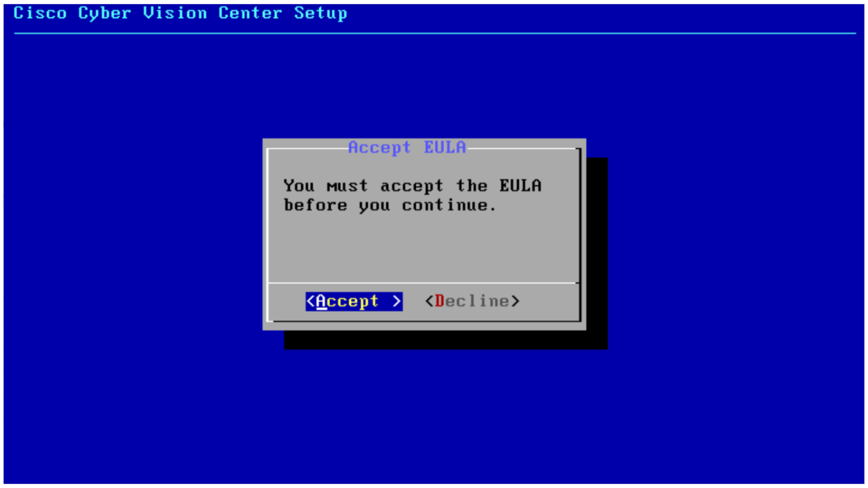
Accept the End User License Agreement



```
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
    ↓(+)                                                       5%
                              < EXIT >
```



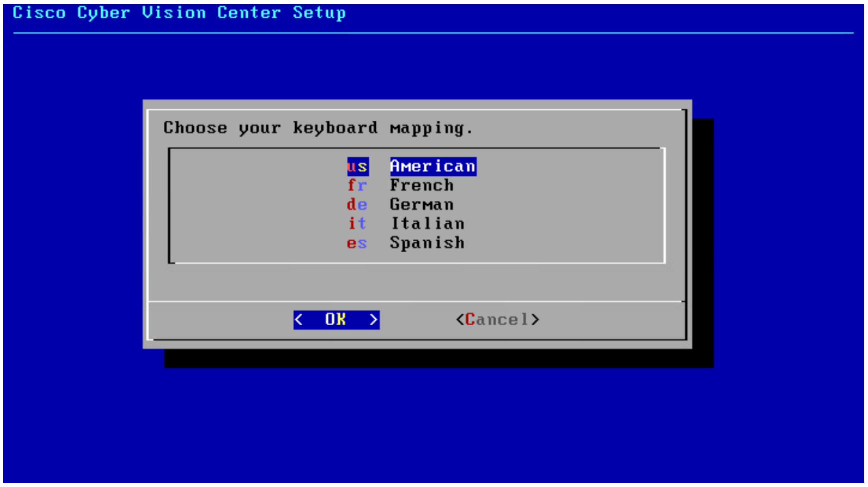
```
Cisco Cyber Vision Center Setup

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

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

                                                              100%
                          < EXIT >
```



```
Cisco Cyber Vision Center Setup

                 Accept EULA
    You must accept the EULA
    before you continue.

    <Accept >   <Decline>
```

Select the language to match your keyboard

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



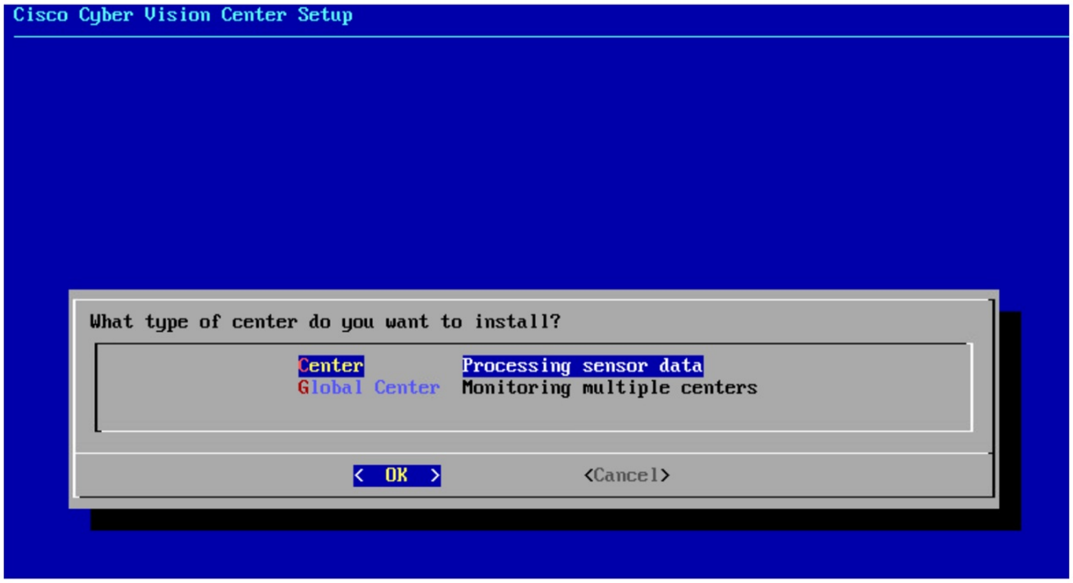
```
Cisco Cyber Vision Center Setup

Choose your keyboard mapping.

   us   American
   fr   French
   de   German
   it   Italian
   es   Spanish

      <  OK  >        <Cancel>
```

Select the Center type

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

- A **Center** receives metadata from sensors and store them into an internal database (Postrgresql). This Center could be standalone or with synchronization with Global Center, 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 your system to start enrollment and start pushes events to it. .
- A **Global Center** introduces a centralized architecture which collects all industrial insights and events from Centers with Global Center and aggregate it on a single global point of view. It will also allow you to manage the knowledge database (KDB) and upgrade the whole platform.

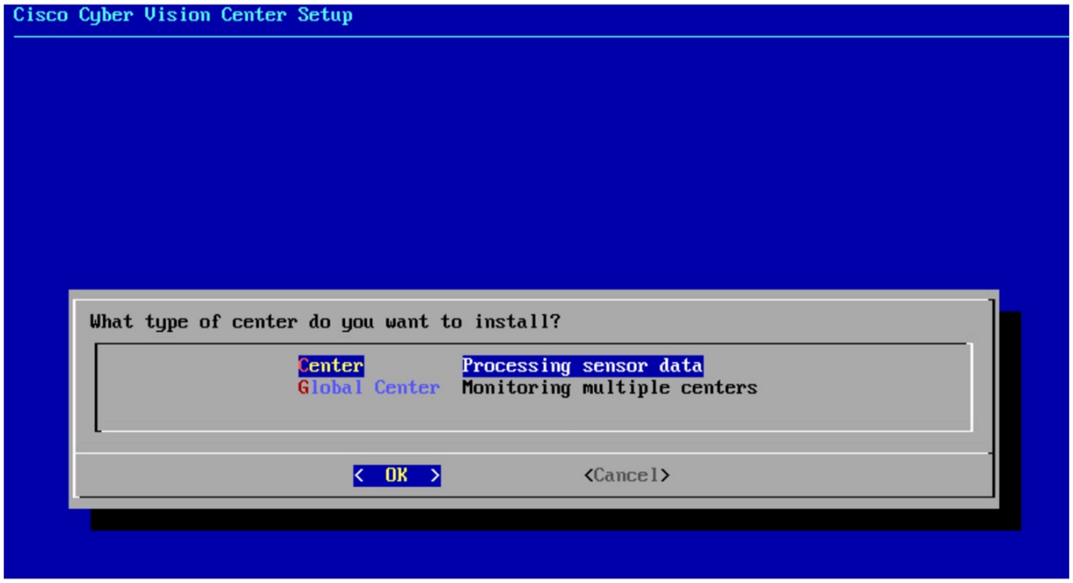
Select the type of Center you want to install.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

   Center            Processing sensor data
   Global Center     Monitoring multiple centers

      <  OK  >              <Cancel>
```

Center

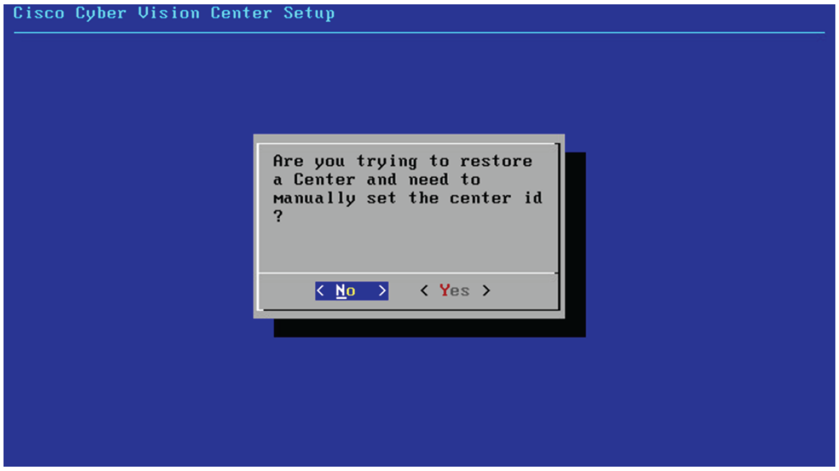
If installing a Center, select the first option.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

Center          Processing sensor data
Global Center   Monitoring multiple centers

< OK >          <Cancel>
```

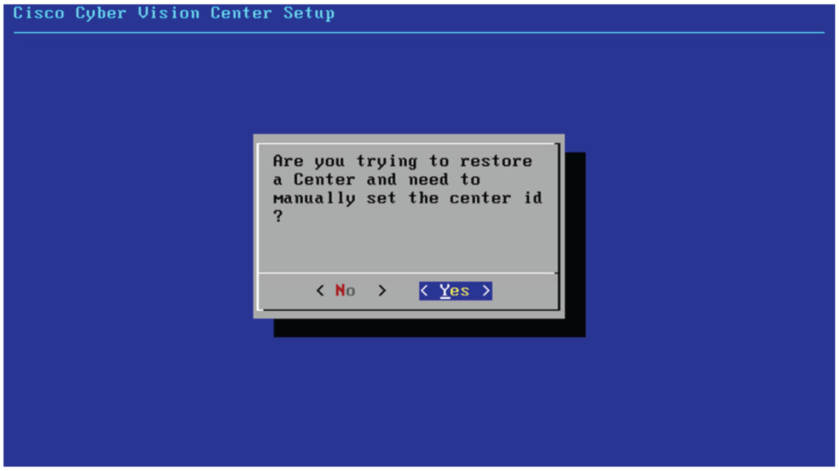
Then you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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



```
Cisco Cyber Vision Center Setup

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

< No >   < Yes >
```

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



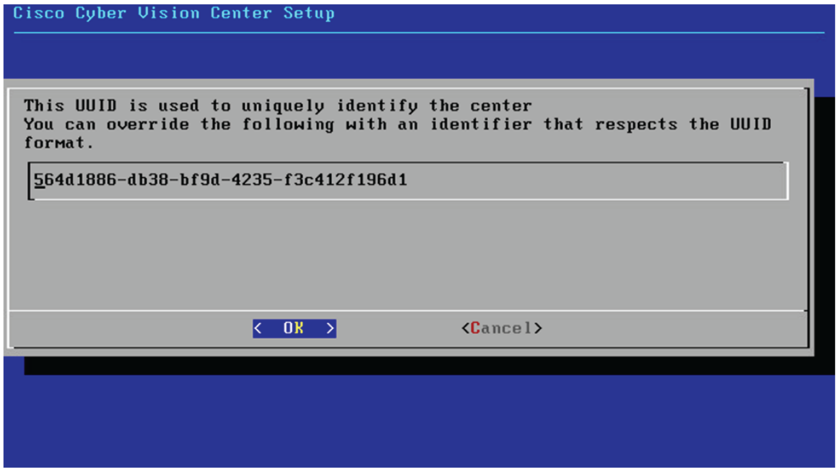
Cisco Cyber Vision Center Setup

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

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

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

Type the id into the basic Center configuration UUID field.



Cisco Cyber Vision Center Setup

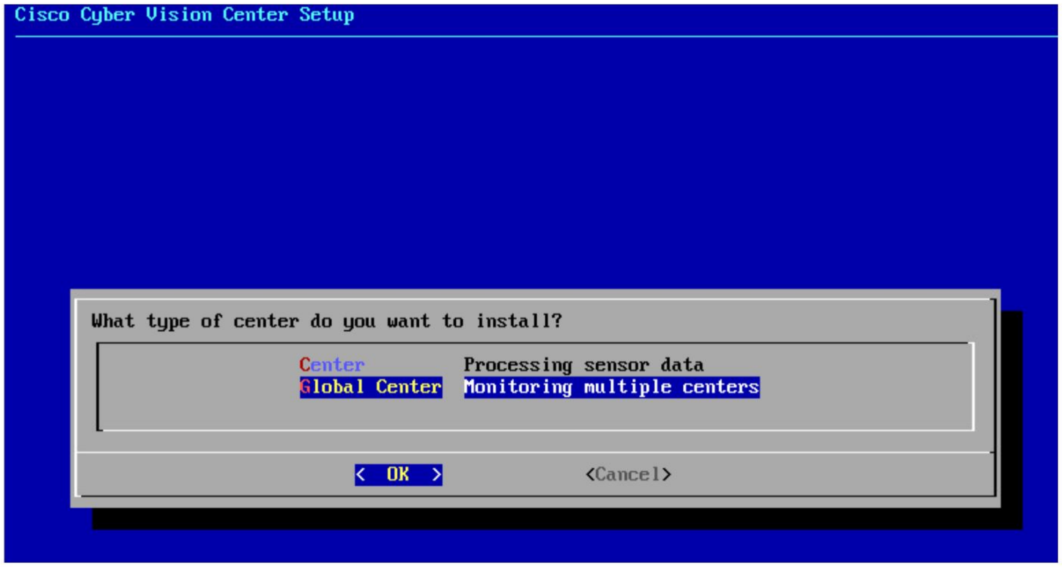
This UUID is used to uniquely identify the center
You can override the following with an identifier that respects the UUID format.

564d1886-db38-bf9d-4235-f3c412f196d1

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

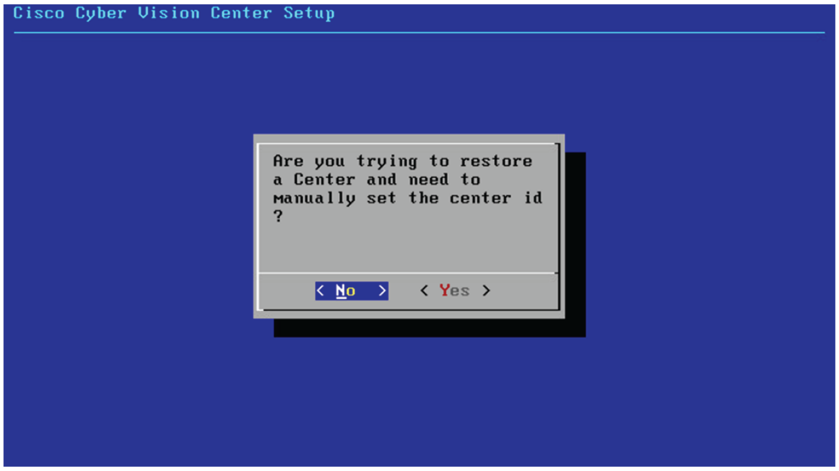
Global Center

If installing a Global Center, select the second option.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

    Center            Processing sensor data
    Global Center     Monitoring multiple centers

        <  OK  >              <Cancel>
```

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

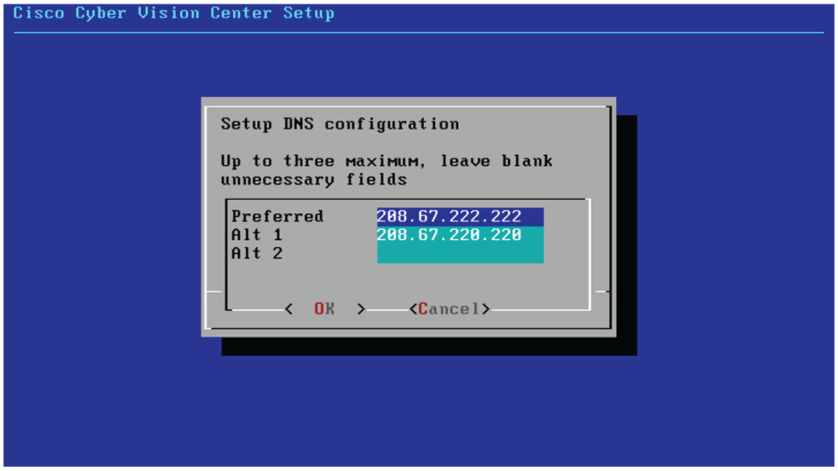


```
Cisco Cyber Vision Center Setup

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

    < No >    < Yes >
```

You will be directed to the next step.

Configure the Center's DNS

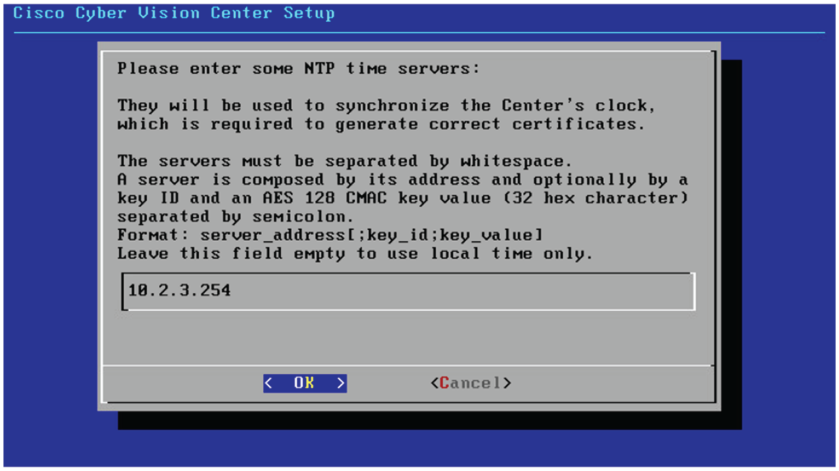
Type a DNS server address and optional fallbacks.



```
Cisco Cyber Vision Center Setup

Setup DNS configuration

Up to three maximum, leave blank
unnecessary fields

Preferred      208.67.222.222
Alt 1          208.67.220.220
Alt 2

          <  OK  >    <Cancel>
```

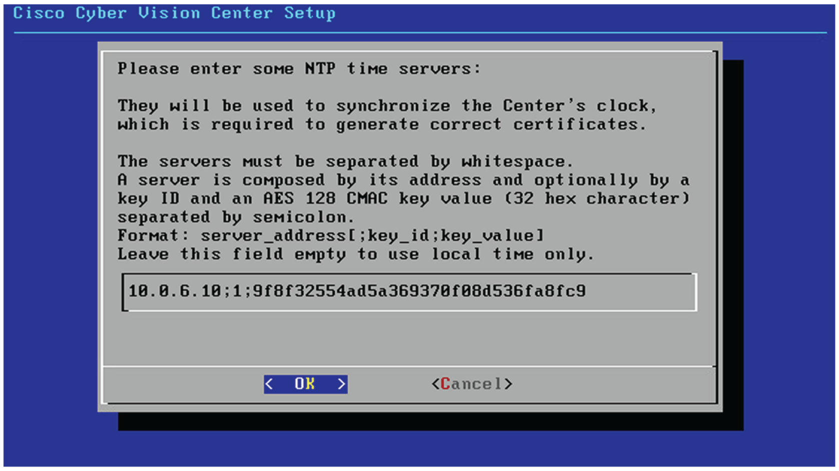
Synchronize the Center and the sensors to NTP servers

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



```
Cisco Cyber Vision Center Setup

Please enter some NTP time servers:

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

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

10.2.3.254

               <  OK  >          <Cancel>
```

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

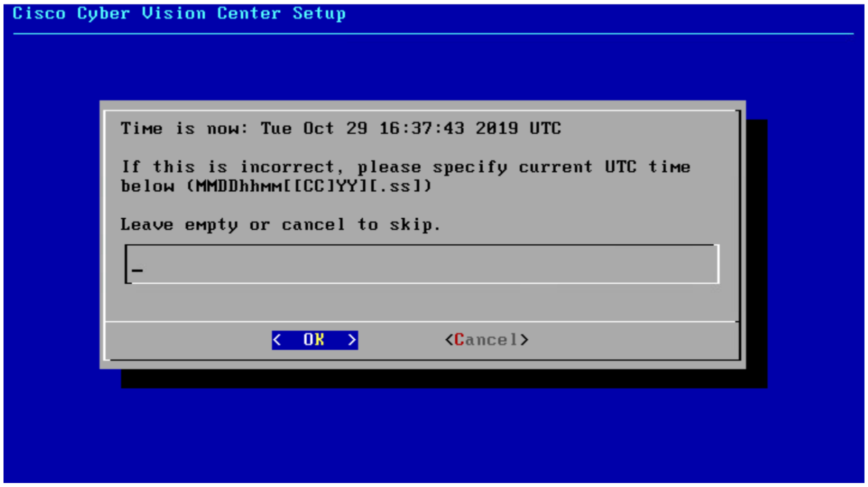


```
Cisco Cyber Vision Center Setup

Please enter some NTP time servers:

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

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

10.0.6.10;1;9f8f32554ad5a369370f08d536fa8fc9
```

The synchronization takes a few seconds.

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

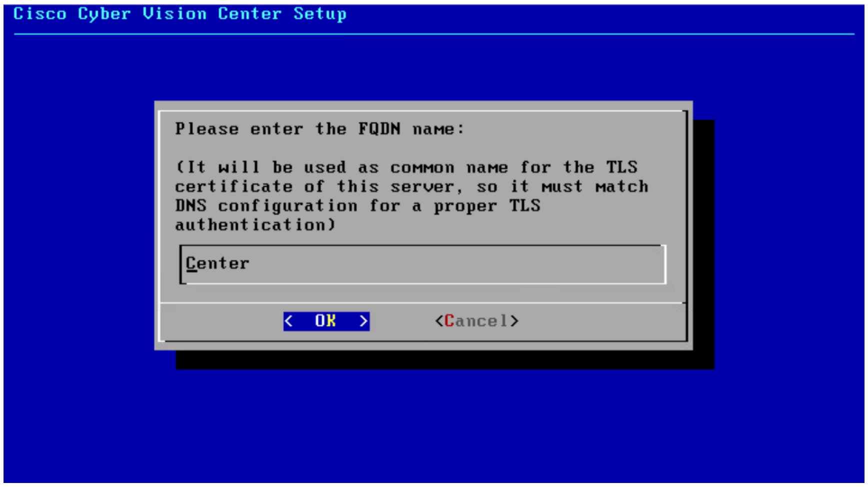
Note The time is set in the UTC standard.



```
Cisco Cyber Vision Center Setup

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

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

Leave empty or cancel to skip.
```

Give the Center a name

Note This name will be used in the Center certificate.



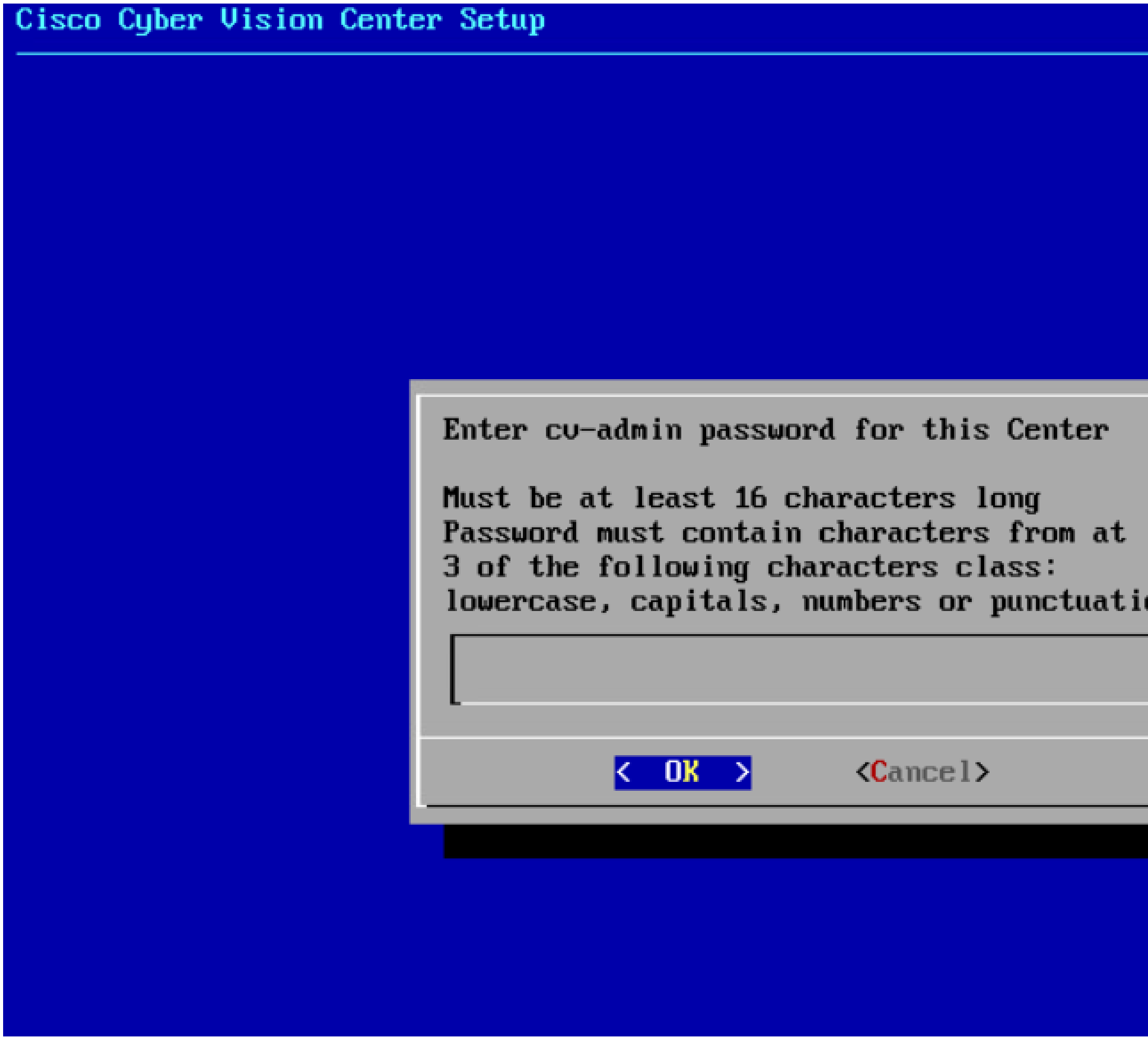
```
Cisco Cyber Vision Center Setup

Please enter the FQDN name:

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

Center

< OK >          <Cancel>
```

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

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

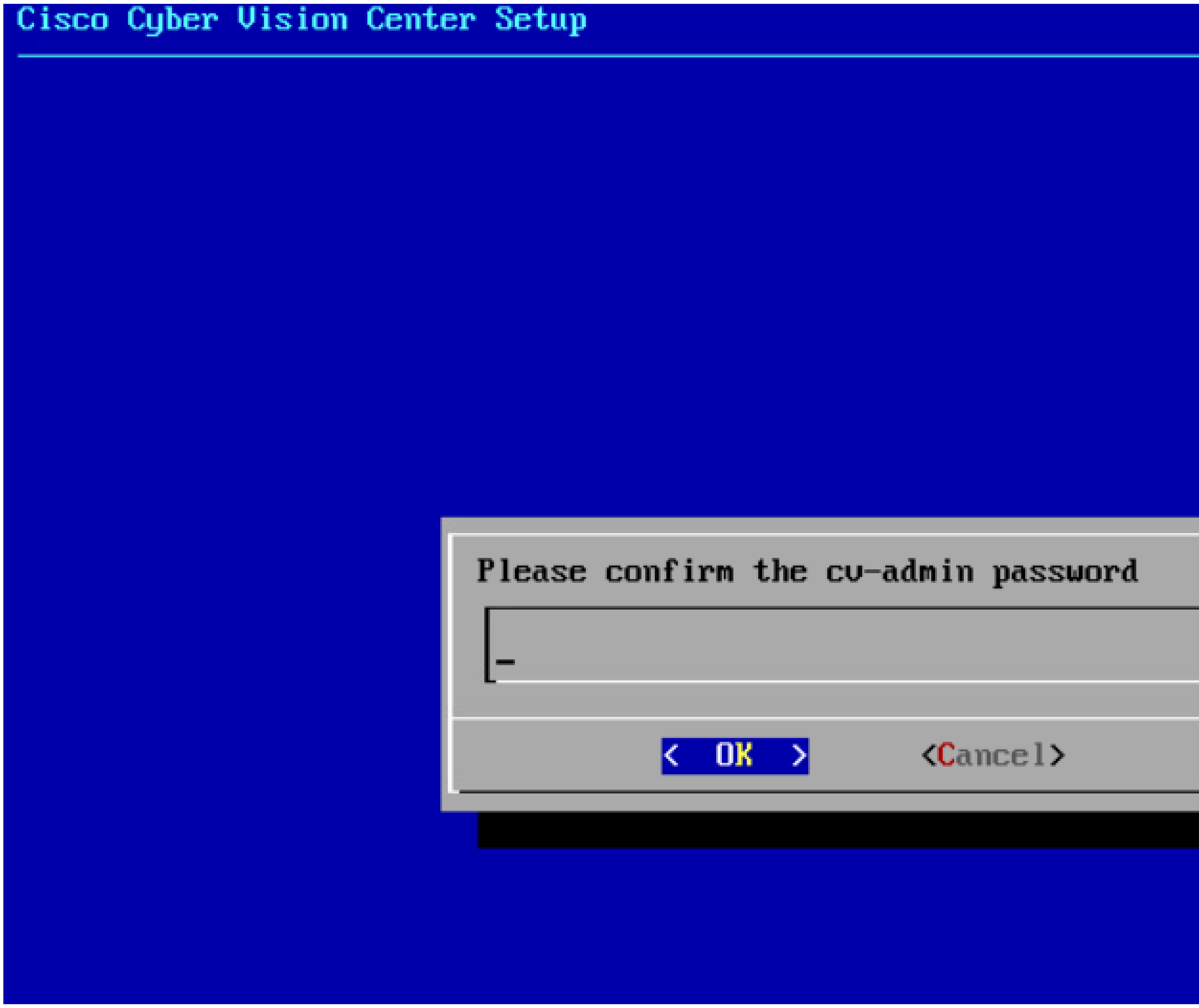
Set the Center's password

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



```
Cisco Cyber Vision Center Setup

Enter cv-admin password for this Center

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

Confirm the password.



Cisco Cyber Vision Center Setup

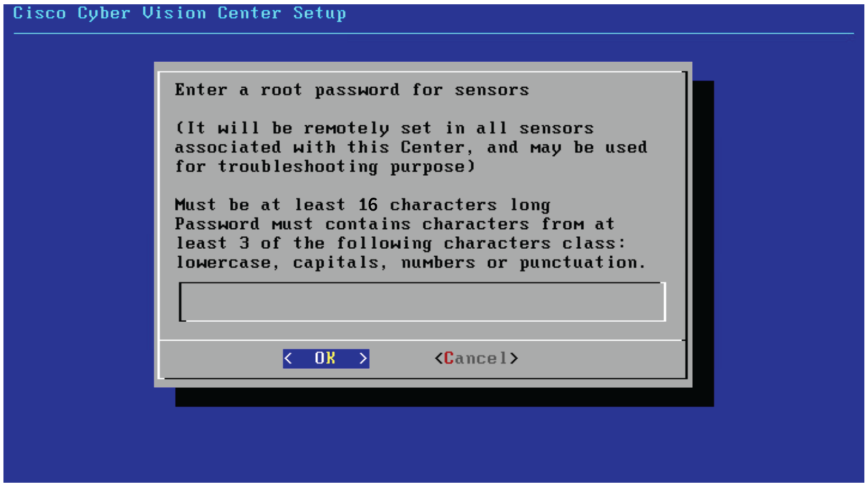
Please confirm the cv-admin password

Configure the sensors' password

As this step does not apply when installing a Global Center, the following screens won't be displayed. Instead, you'll be directed to Authorize networks.

Although, if you're installing a Center, proceed as below.

The sensors' root password must be set for security reasons.



Cisco Cyber Vision Center Setup

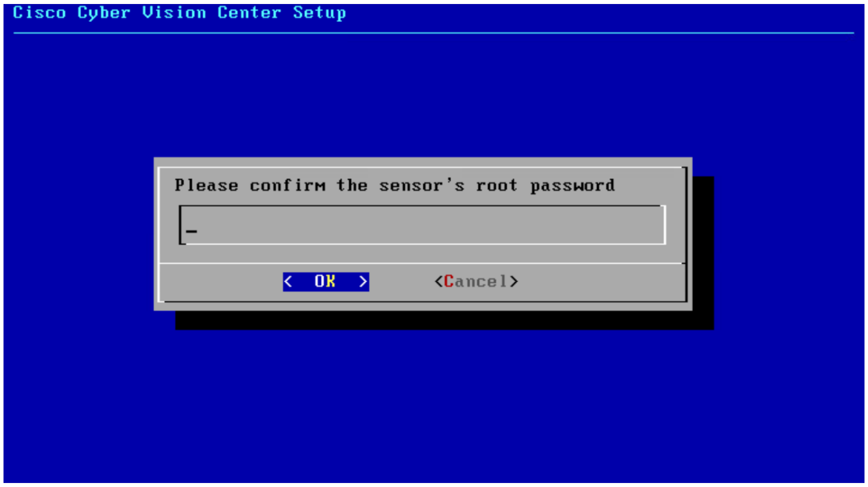
Enter a root password for sensors

(It will be remotely set in all sensors associated with this Center, and may be used for troubleshooting purpose)

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

This password will be assigned once you will have enrolled the sensors on the Center. You will need this password for troubleshooting, diagnostics, and updates.

Confirm the password.

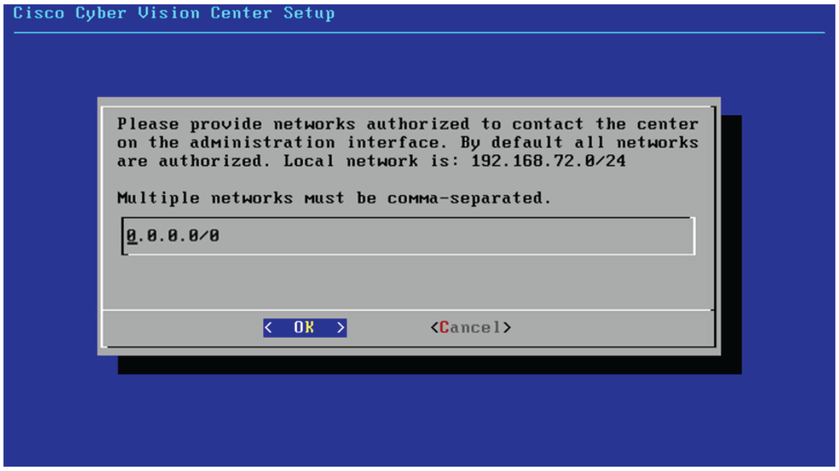


Cisco Cyber Vision Center Setup

Please confirm the sensor's root password

Authorize networks

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

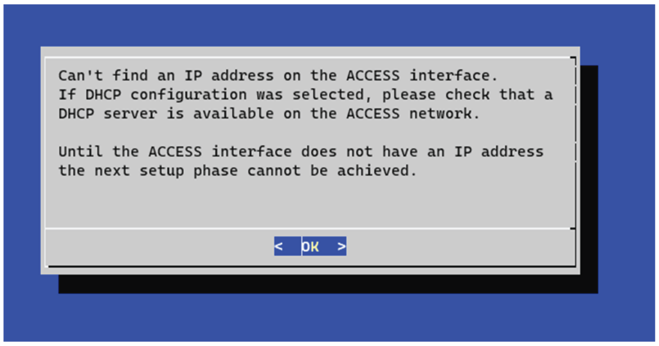


```
Cisco Cyber Vision Center Setup

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

Multiple networks must be comma-separated.

0.0.0.0/0
```

Set DHCP

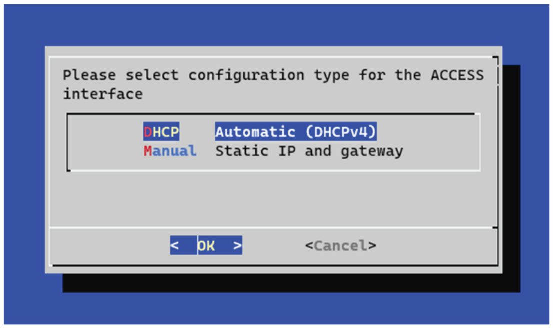
Procedure

Step 1 If the following message appears, select OK.



```
Can't find an IP address on the ACCESS interface.
If DHCP configuration was selected, please check that a
DHCP server is available on the ACCESS network.

Until the ACCESS interface does not have an IP address
the next setup phase cannot be achieved.
```

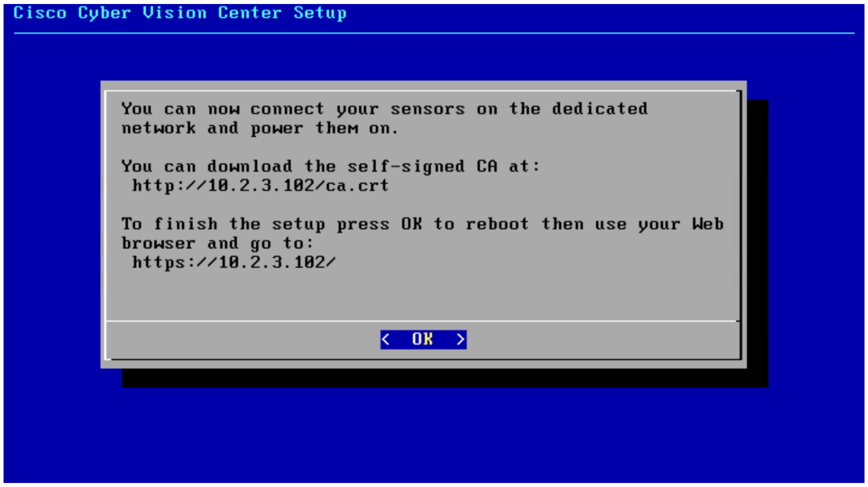
Step 2 Select DHCP.



```
Please select configuration type for the ACCESS
interface

        DHCP     Automatic (DHCPv4)
        Manual   Static IP and gateway
```

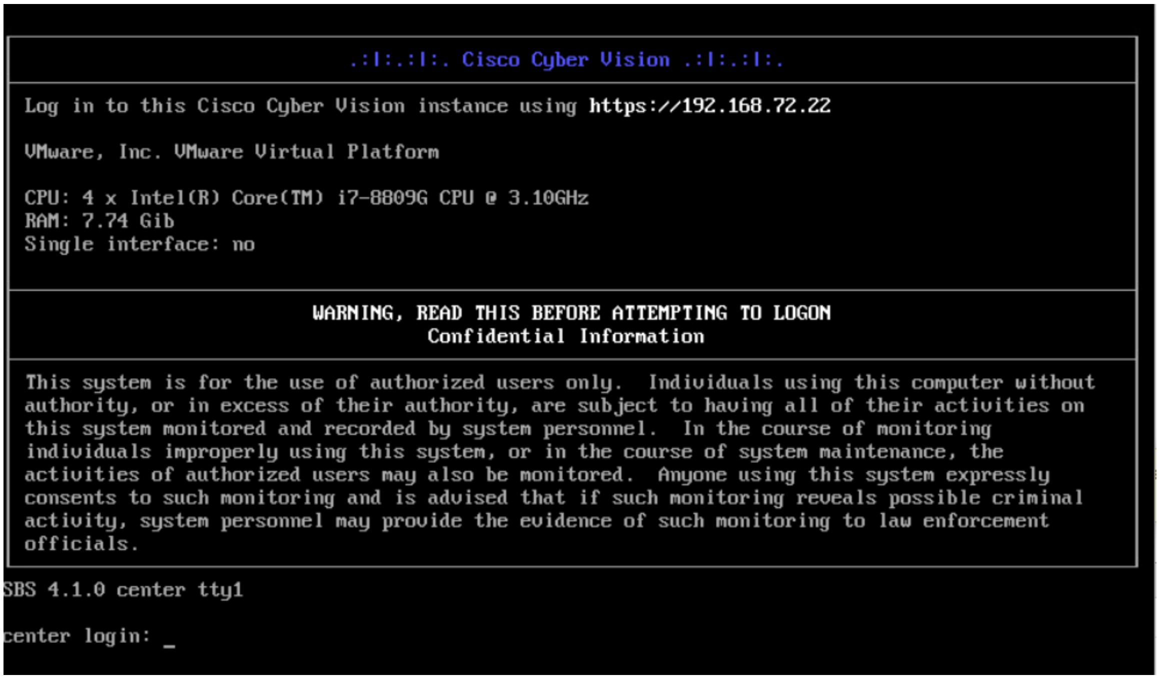
Complete the basic Center configuration

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 Cyber 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.



```
                    .:|:.:|:. 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: _
```

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

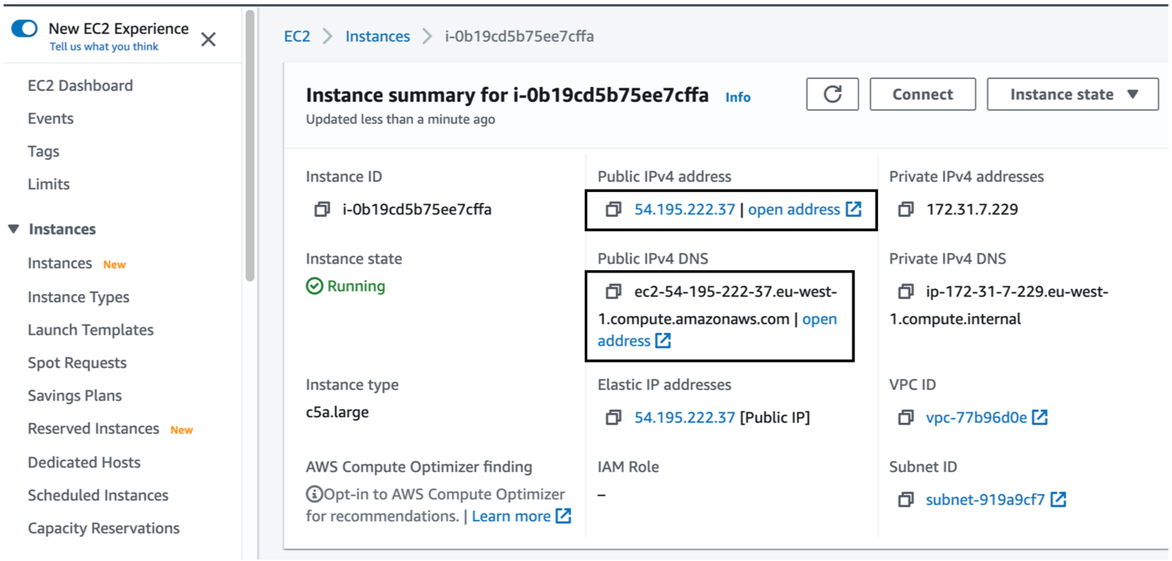
Connect to the Center

You can connect to the Center:

- Using the Using the GUI.
- Using the Using the console.

Using the GUI

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



Instance summary for i-0b19cd5b75ee7cffa

Updated less than a minute ago

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

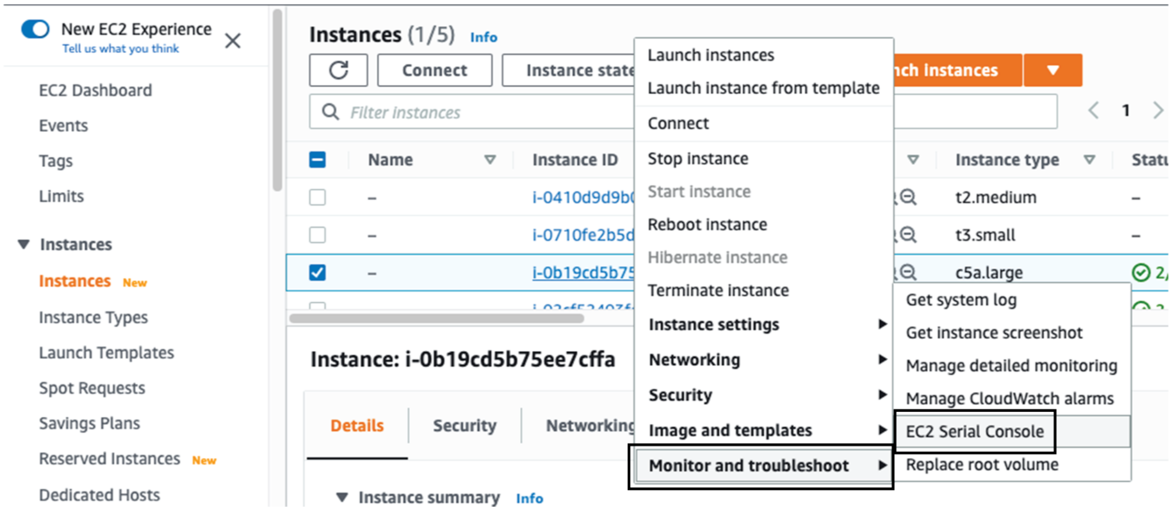
   You can proceed with Install Cisco Cyber Vision.

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 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

Access the Cisco Cyber Vision installation wizard:

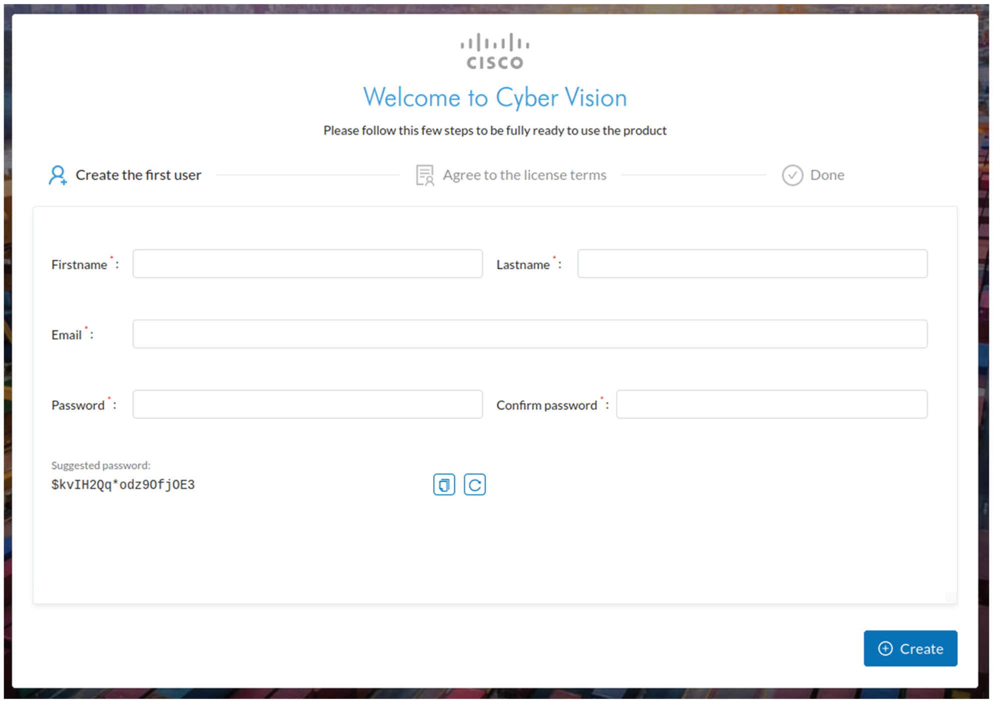
Procedure

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:
$kvIH2Qq*odz90fjOE3

Step 4

Step 5 Enter the information required.

Note Email will be asked for login access.

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

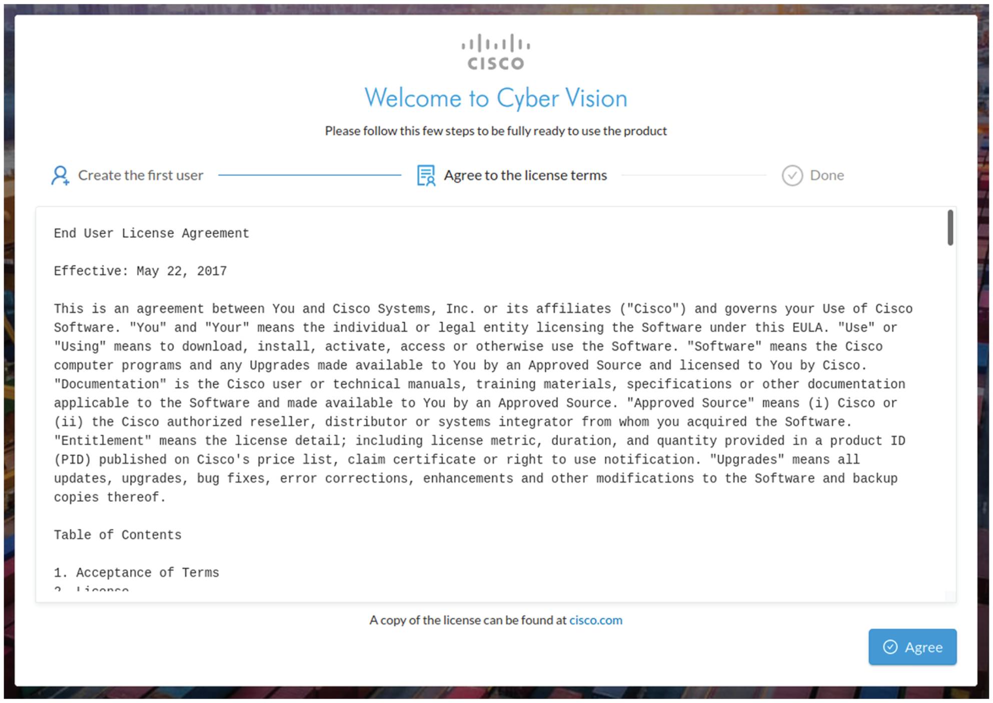
- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

Passwords should be changed regularly to ensure the 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

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

Table of Contents

1. Acceptance of Terms

2. License

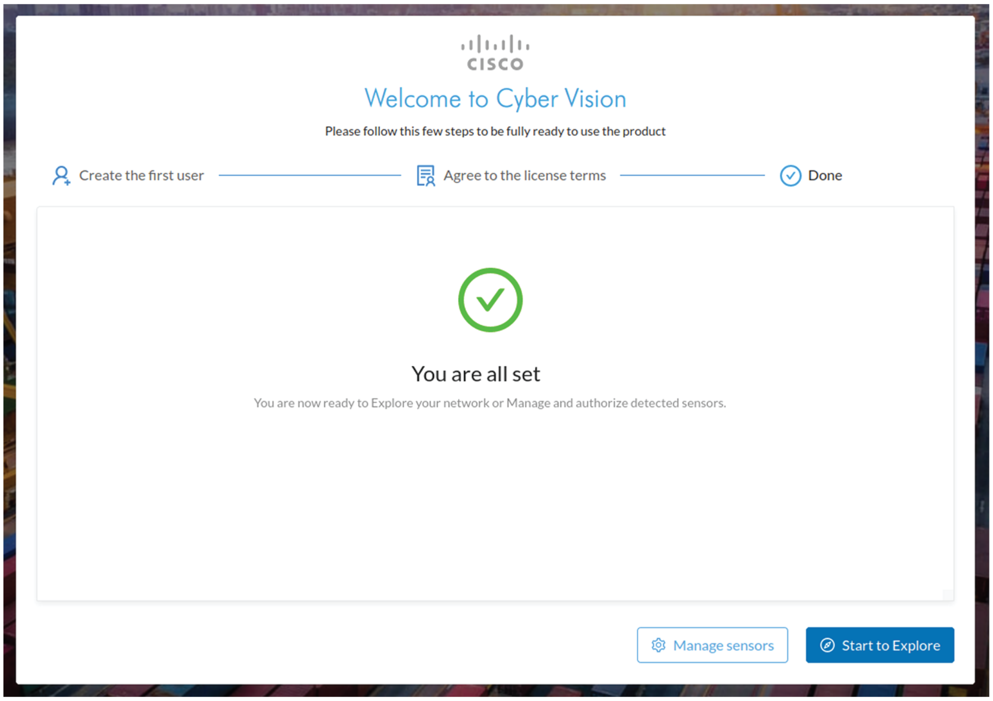
A copy of the license can be found at cisco.com

Step 7

Step 8 **Finish the installation:**

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

Step 9 Click Start to Explore.



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

You are all set

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

Manage sensors
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 56.

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 61.

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 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 43.

Procedure

Step 1 Open your browser.

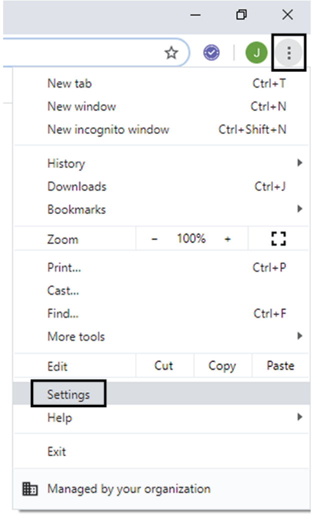
Step 2 Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.

The certificate is downloaded.

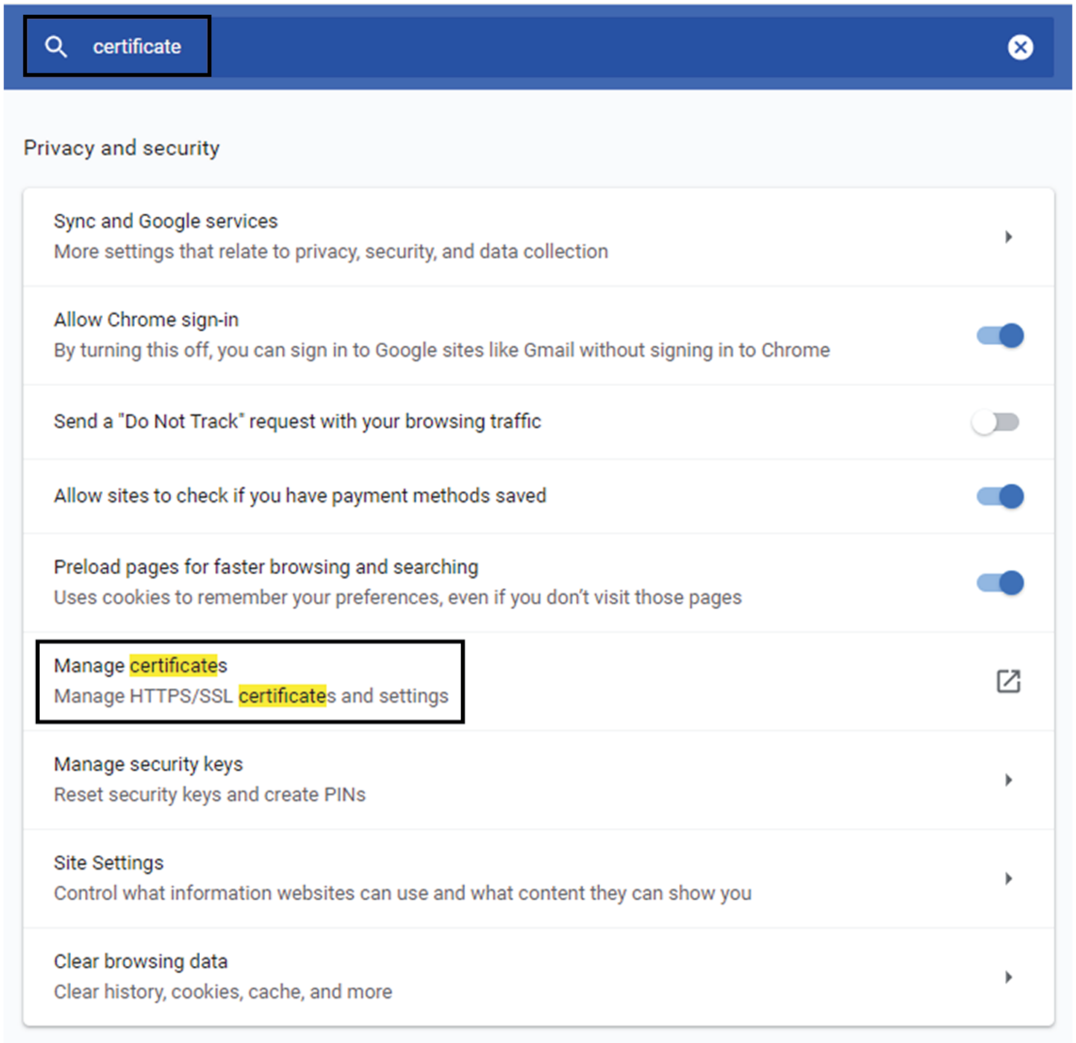
Step 3 Save the certificate on your computer.

Step 4 In the browser, access the settings.

Example: Chrome



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



certificate

Privacy and security

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

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

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

Allow sites to check if you have payment methods saved

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

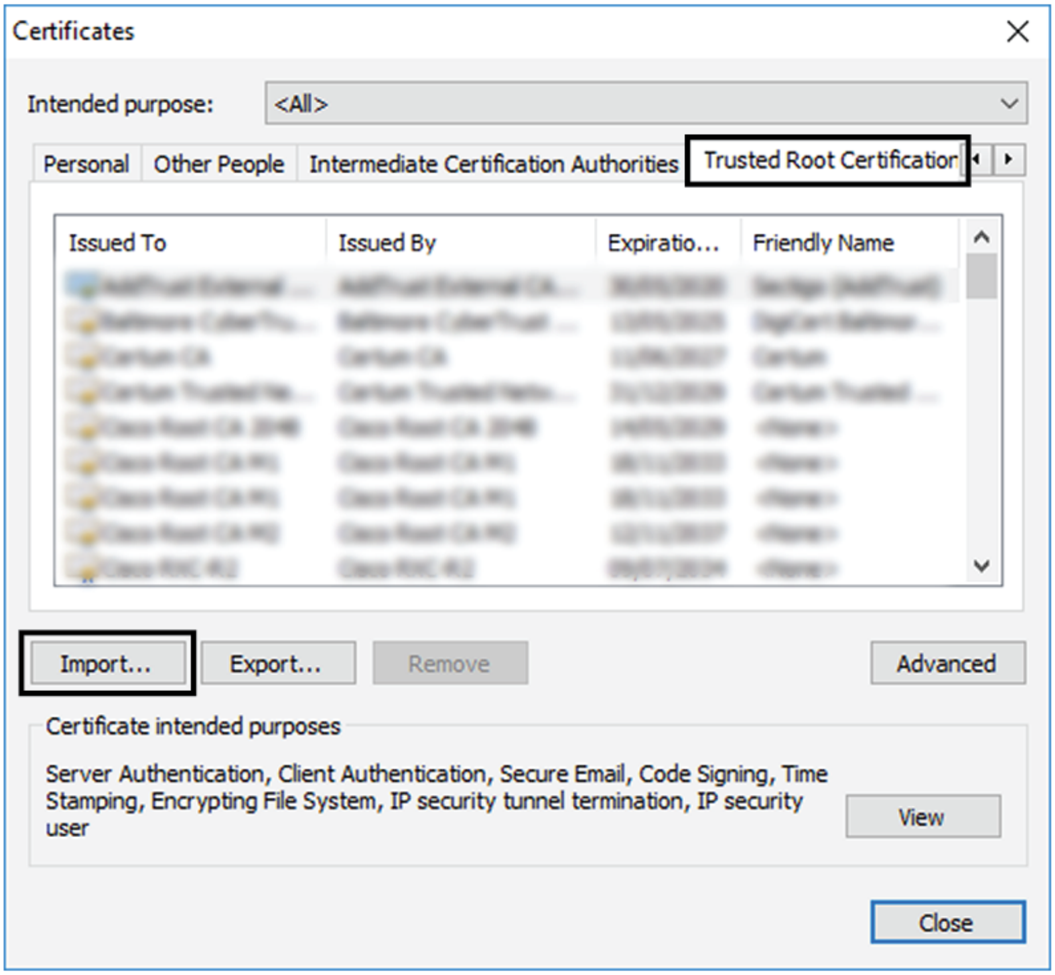
Manage certificates
Manage HTTPS/SSL certificates and settings

Manage security keys
Reset security keys and create PINs

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

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

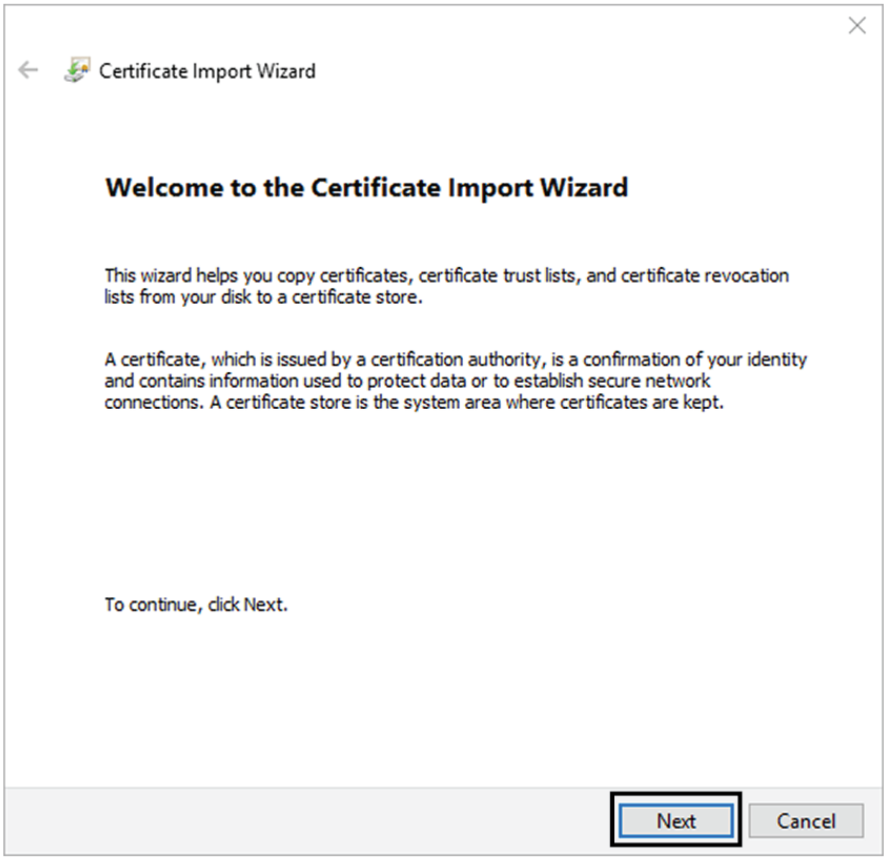
Step 6 Access the Trusted Root Certification tab and click Import.



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

A certificate importation wizard opens.

Step 7 Go to the next step.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

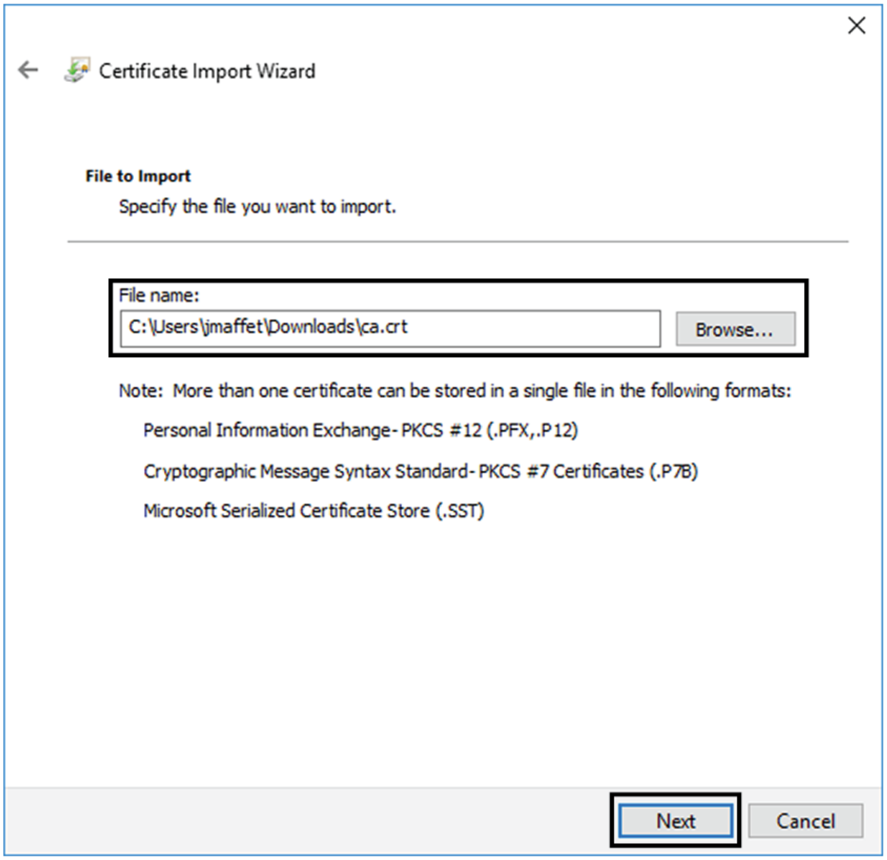
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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

To continue, click Next.

Step 8 Search for the certificate you downloaded earlier.

Step 9 Go to the next step.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

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

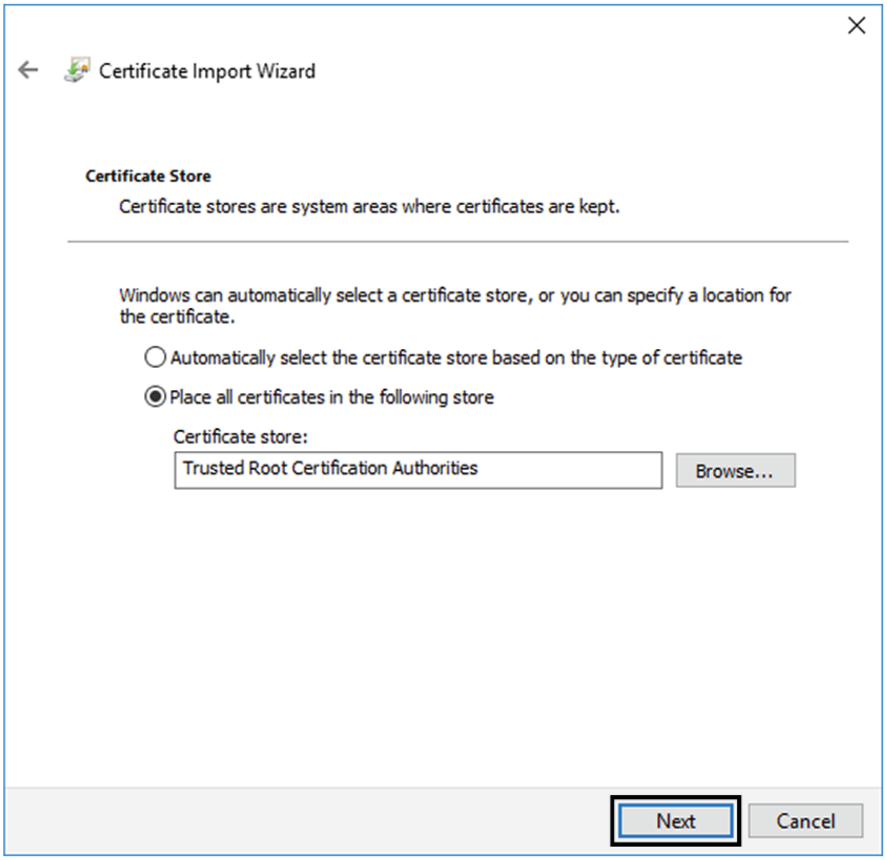
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

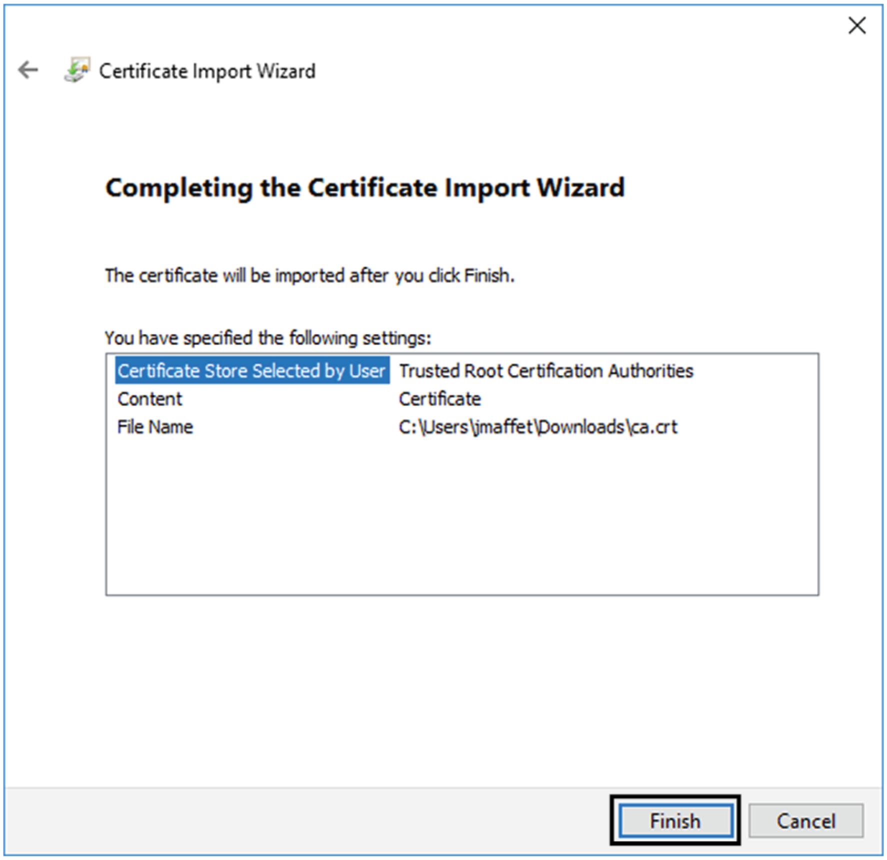
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

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



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

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

What to do next

Install Cisco Cyber Vision, on page 43

Install Cisco Cyber Vision

Access the Cisco Cyber Vision installation wizard:

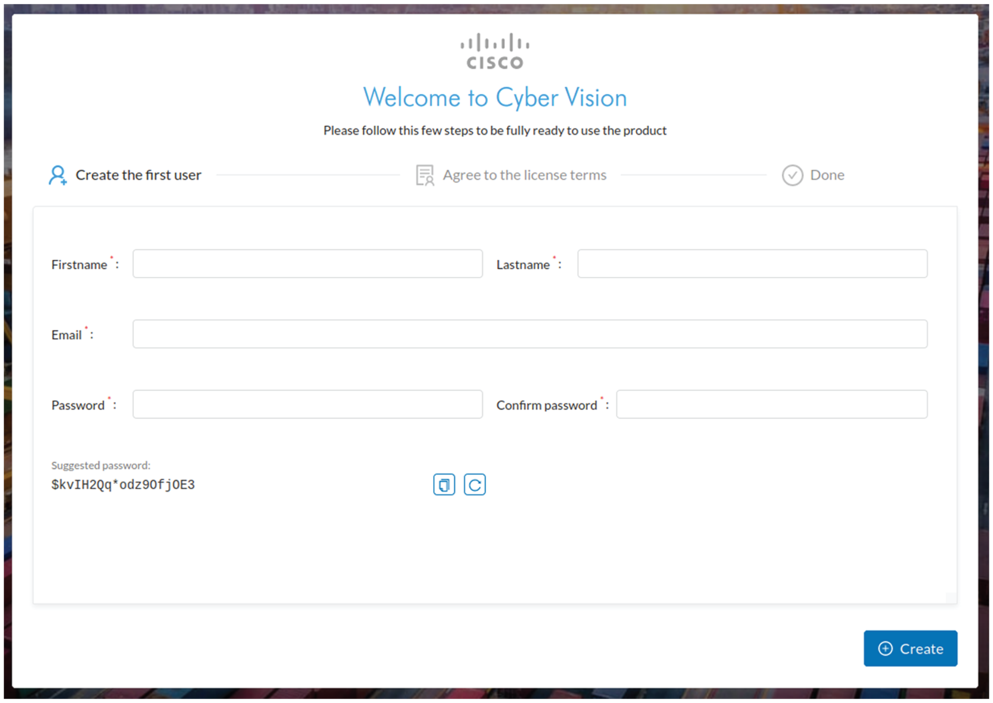
Procedure

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

Suggested password:
$kvIH2Qq*odz90fjOE3

Step 4

Step 5 Enter the information required.

Note Email will be asked for login access.

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

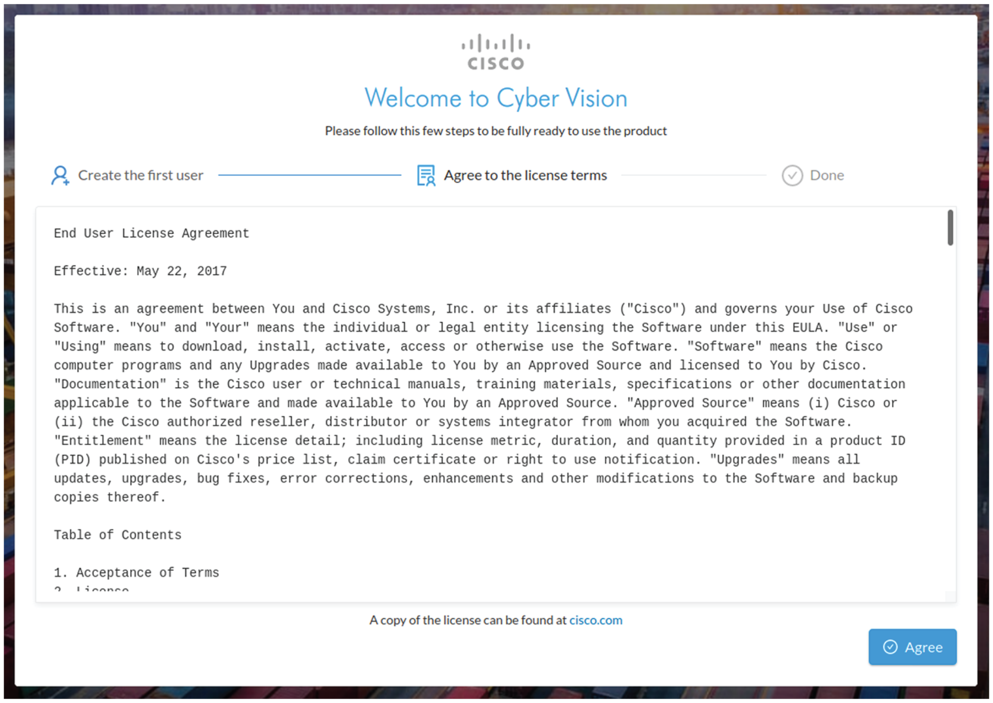
- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#$%&’()*+,-./:;<=>?@[]^_{|}.

Passwords should be changed regularly to ensure the 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

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

Table of Contents

1. Acceptance of Terms
2. Licence

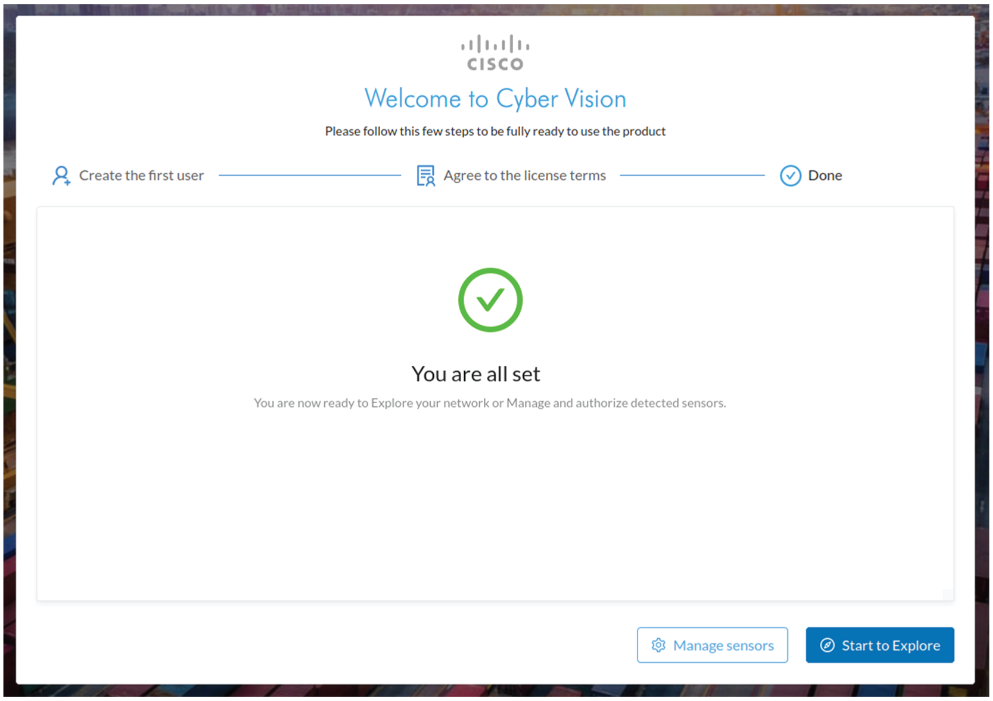
A copy of the license can be found at cisco.com

Step 7

Step 8 **Finish the installation:**

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

Step 9 Click Start to Explore.


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

You are all set

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

Manage sensors
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 56.

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 61.

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

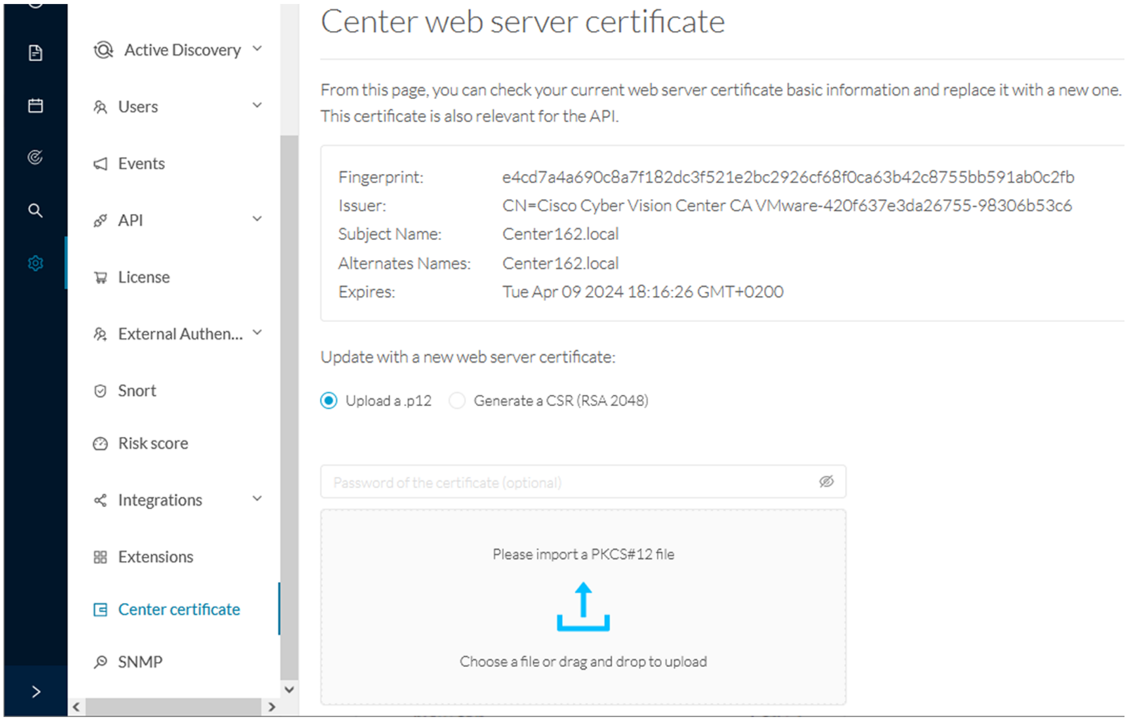
This section explains how to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

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.



Center web server certificate

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

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

Update with a new web server certificate:

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

Password of the certificate (optional)

Please import a PKCS#12 file

Choose a file or drag and drop to upload

Step 2 You can Upload a p12 orGenerate a CSR.

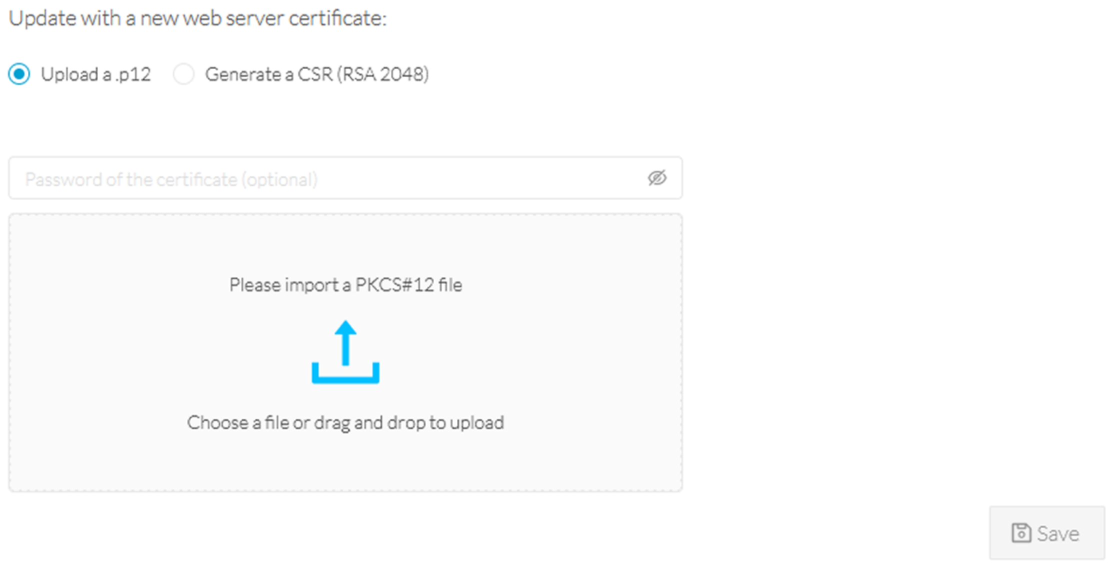
Upload a p12

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:

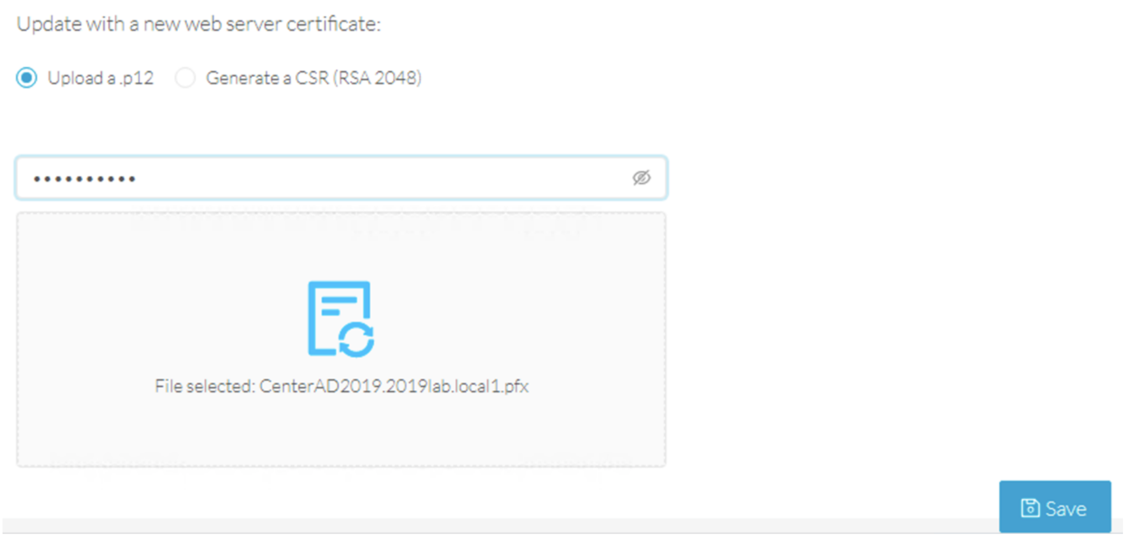
● Upload a .p12 ○ Generate a CSR (RSA 2048)

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

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

Step 2 Type the certificate password.

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



Update with a new web server certificate:

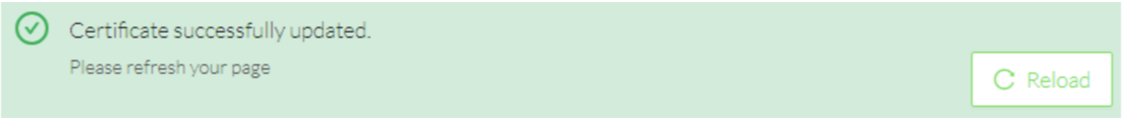
● Upload a .p12 ○ Generate a CSR (RSA 2048)

•••••••••••

File selected: CenterAD2019.2019lab.local1.pfx

Step 4 Click Save.

The following message appears:



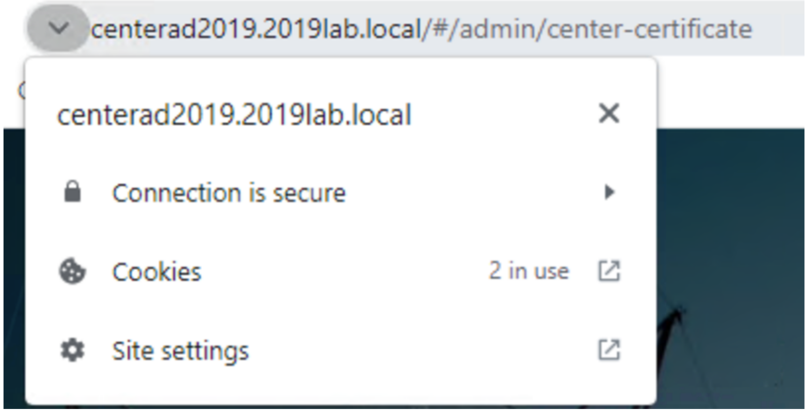
Certificate successfully updated.

Please refresh your page

Step 5 Click Reload.

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

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



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

centerad2019.2019lab.local

Connection is secure

Cookies 2 in use

Site settings

What to do next

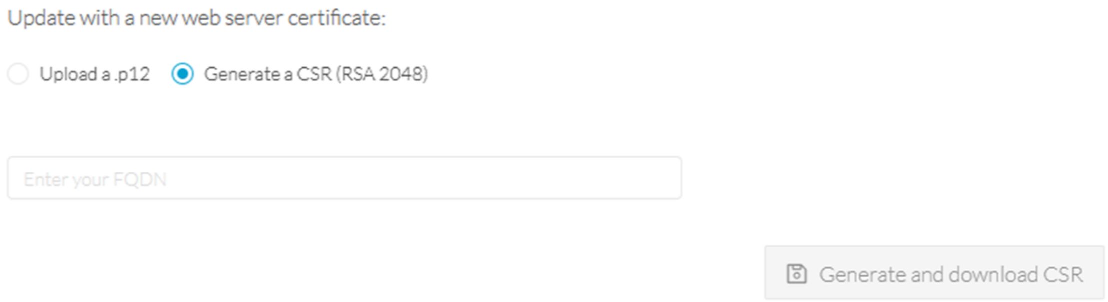
If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 61.

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.



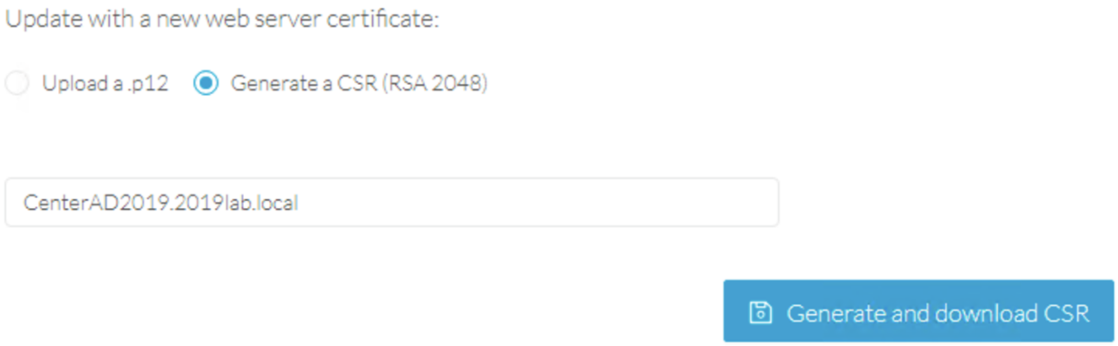
Update with a new web server certificate:

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

Enter your FQDN

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

Step 3 Click the Generate and download CSR button.



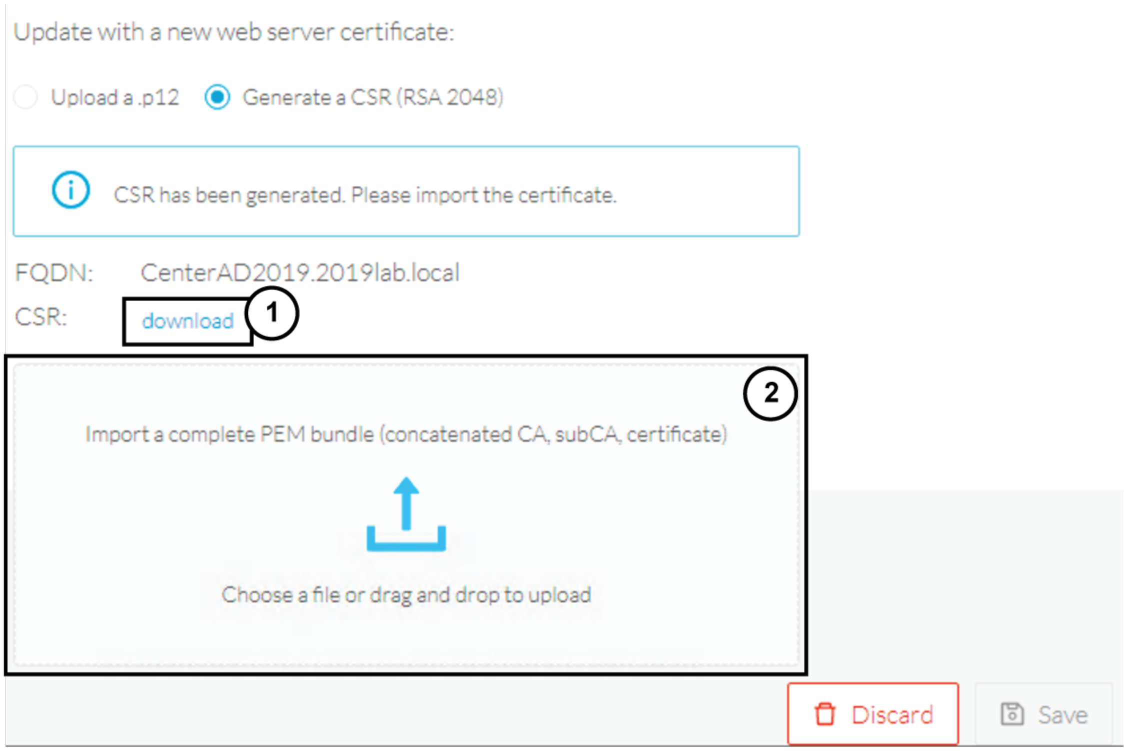
Update with a new web server certificate:

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

CenterAD2019.2019lab.local

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

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



Update with a new web server certificate:

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

CSR has been generated. Please import the certificate.

FQDN: CenterAD2019.2019lab.local

CSR: download

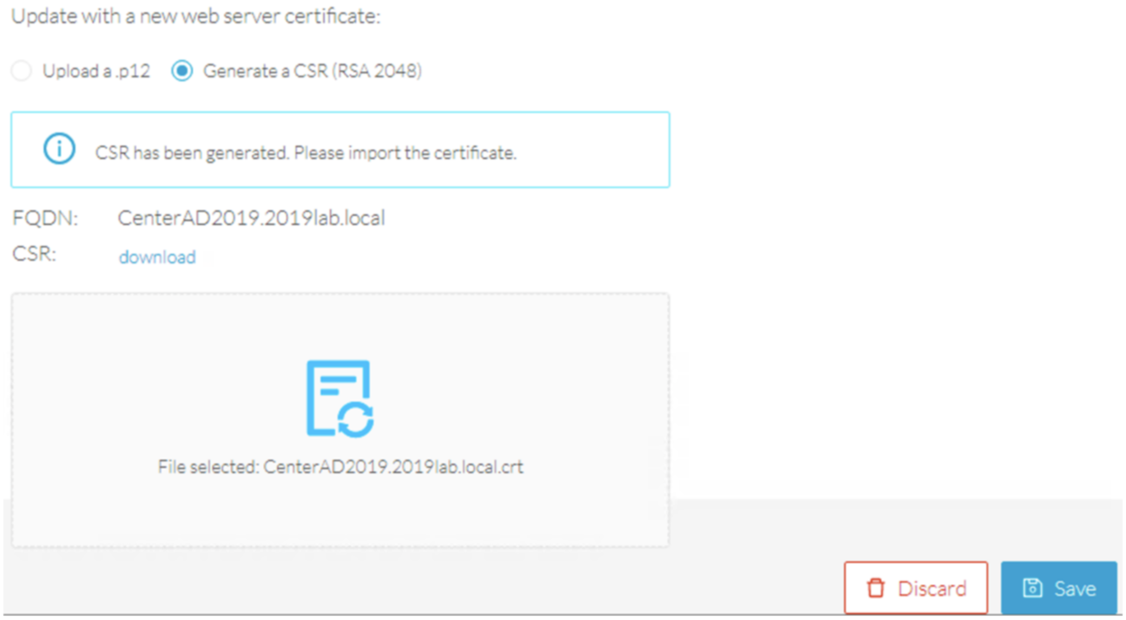
Import a complete PEM bundle (concatenated CA, subCA, certificate)

Choose a file or drag and drop to upload

A <FQDN>.csr file is downloaded.

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

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



Update with a new web server certificate:

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

CSR has been generated. Please import the certificate.

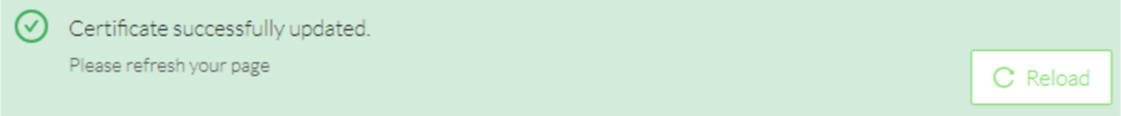
FQDN: CenterAD2019.2019lab.local

CSR: download

File selected: CenterAD2019.2019lab.local.crt

Step 7 Click Save.

The following message appears:



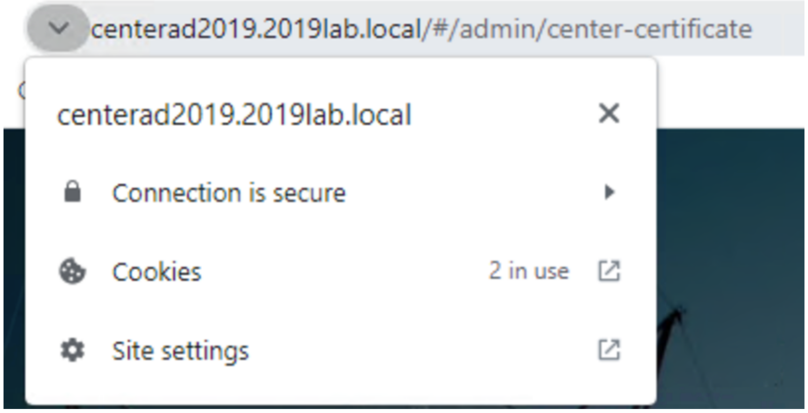
Certificate successfully updated.

Please refresh your page

Step 8 Click Reload.

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

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



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

centerad2019.2019lab.local

Connection is secure

Cookies 2 in use

Site settings

What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 61.

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

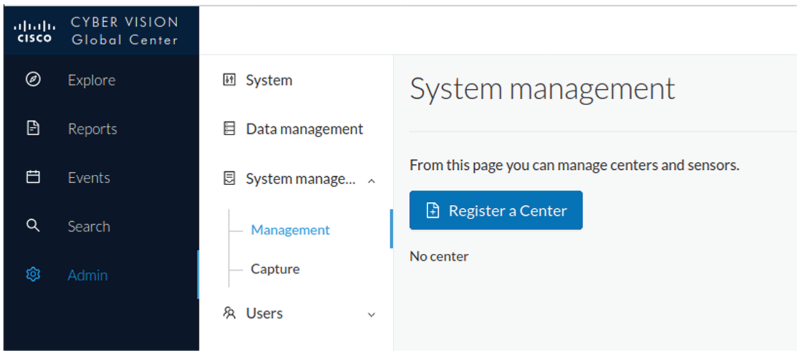
This step is applicable to the Global Center and its synchronized Centers.

Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists in 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".

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

Click the Register a Center button.



System management

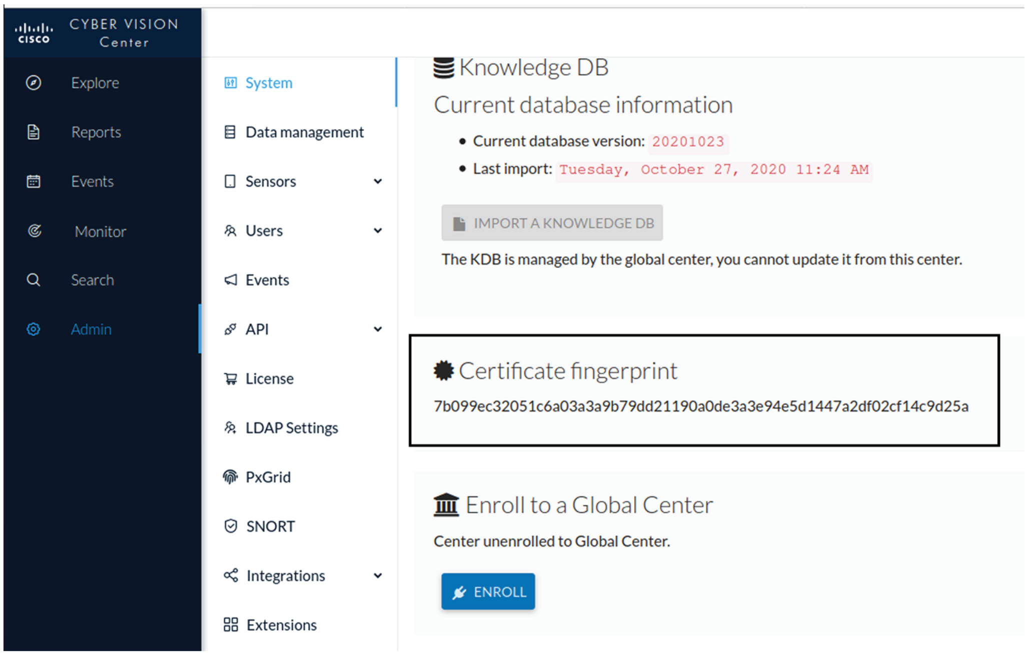
From this page you can manage centers and sensors.

No center

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

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

Scroll down to Certificate fingerprint and copy it.



Knowledge DB

Current database information

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

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

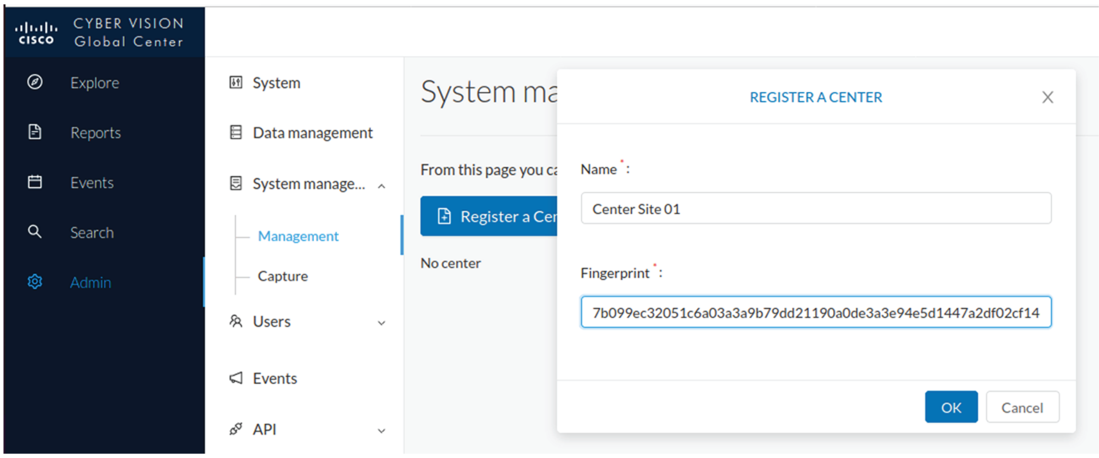
Certificate fingerprint

7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14c9d25a

Enroll to a Global Center

Center unenrolled to Global Center.

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



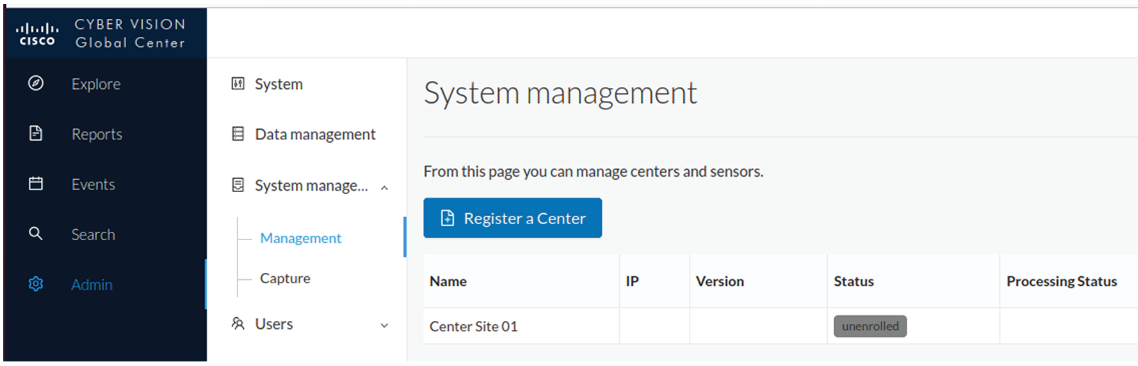
REGISTER A CENTER

Name * : Center Site 01

Fingerprint * : 7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14

Click OK.

The Center appears in the list as unenrolled.



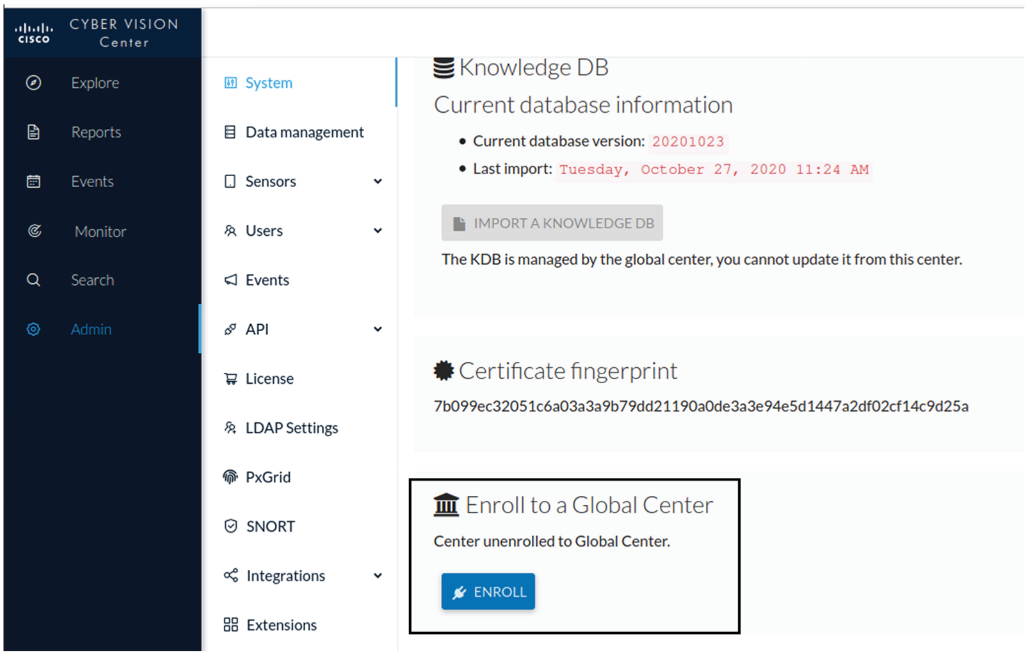
System management

From this page you can manage centers and sensors.

Name	IP	Version	Status	Processing Status
Center Site 01			unenrolled	

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

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



Knowledge DB

Current database information

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

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

Certificate fingerprint

7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14c9d25a

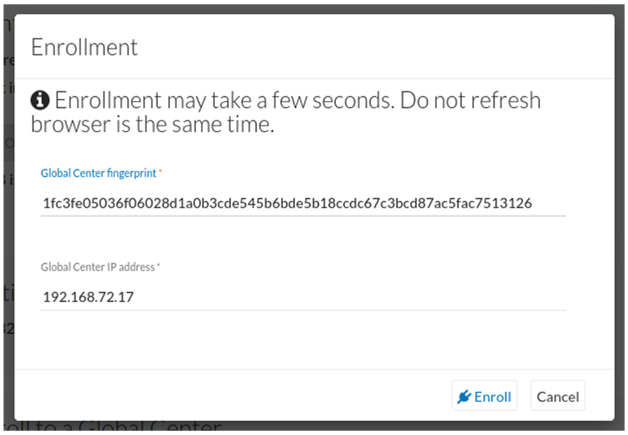
Enroll to a Global Center

Center unenrolled to Global Center.

The Enrollment window pops up.

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

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



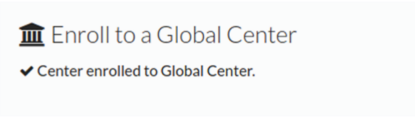
Enrollment

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

Global Center fingerprint *: 1fc3fe05036f06028d1a0b3cde545b6bde5b18ccdc67c3bcd87ac5fac7513126

Global Center IP address *: 192.168.72.17

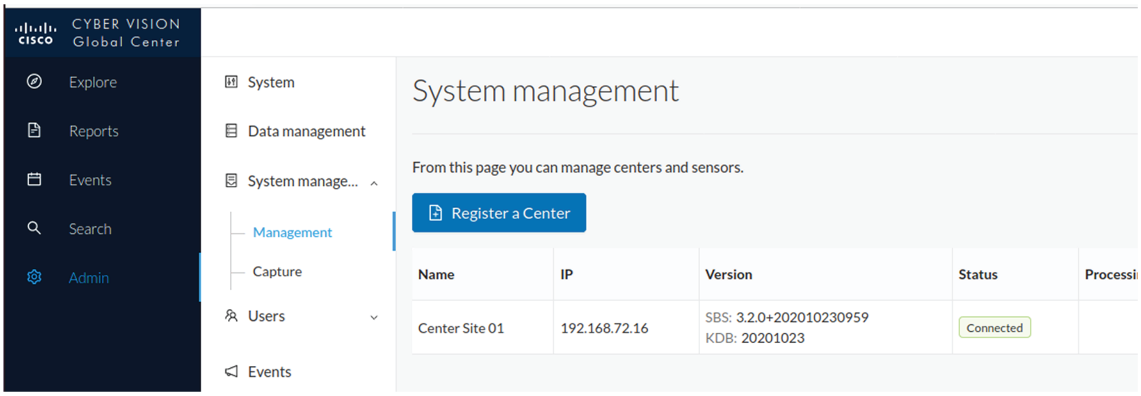
Once the synchronization is on, it is indicated that the Center is enrolled to the Global Center.



Enroll to a Global Center

✓ Center enrolled to Global Center.

In the Global Center's GUI, the Center status changes to Connected.



System management

From this page you can manage centers and sensors.

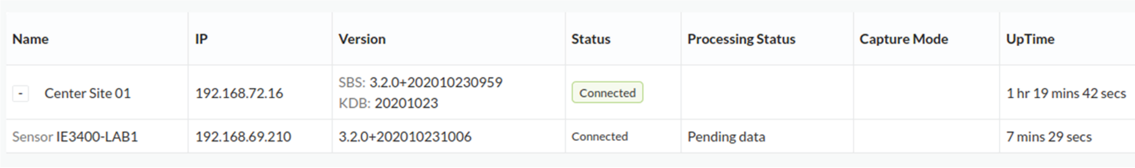
Name	IP	Version	Status	Processi
Center Site 01	192.168.72.16	SBS: 3.2.0+202010230959 KDB: 20201023	Connected	

The Global Center and the Center are successfully connected.

Repeat the previous steps as many times as necessary to connect other Centers.

The next step will be to install and enroll the sensors. To do so, refer to the corresponding Cisco Cyber Vision Sensors Installation Guides.

Once a sensor will be connected it will appear in the Global Center's GUI as below:



Name	IP	Version	Status	Processing Status	Capture Mode	UpTime
- Center Site 01	192.168.72.16	SBS: 3.2.0+202010230959 KDB: 20201023	Connected			1 hr 19 mins 42 secs
Sensor IE3400-LAB1	192.168.69.210	3.2.0+202010231006	Connected	Pending data		7 mins 29 secs

CHAPTER 6

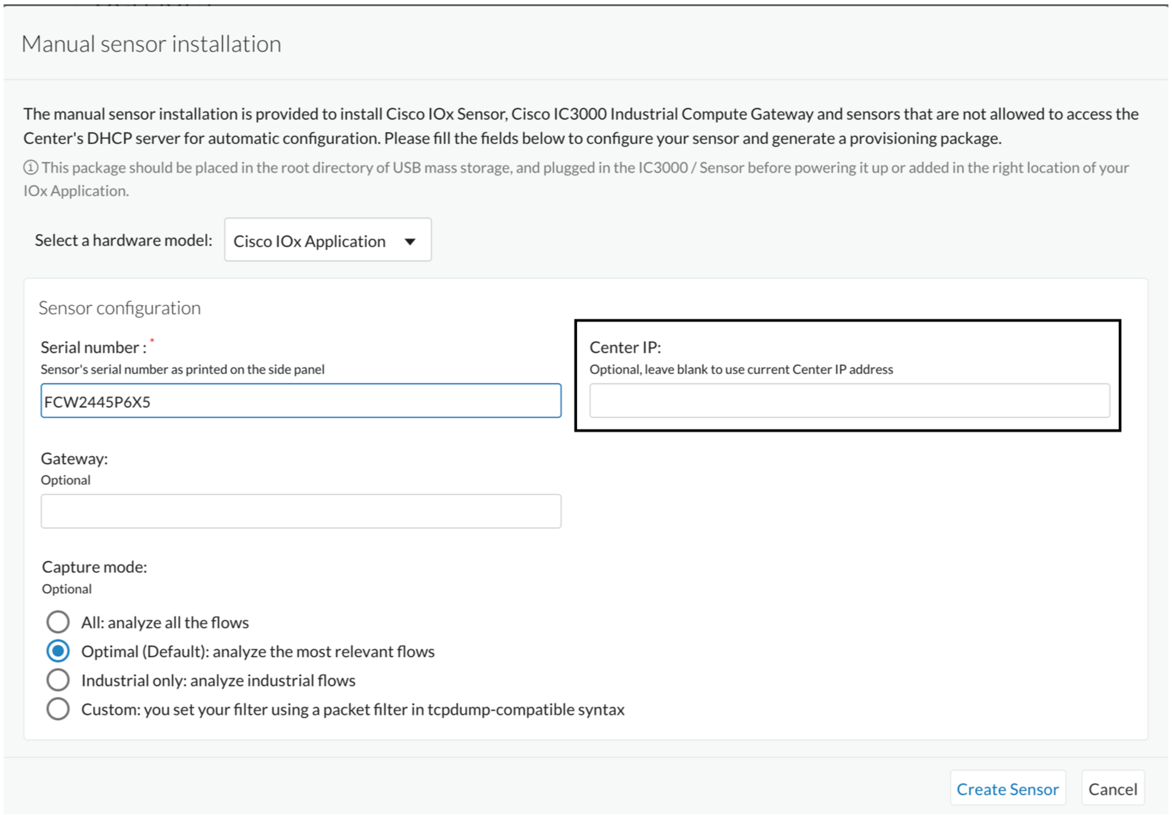
Deploy sensors

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.

ⓘ 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

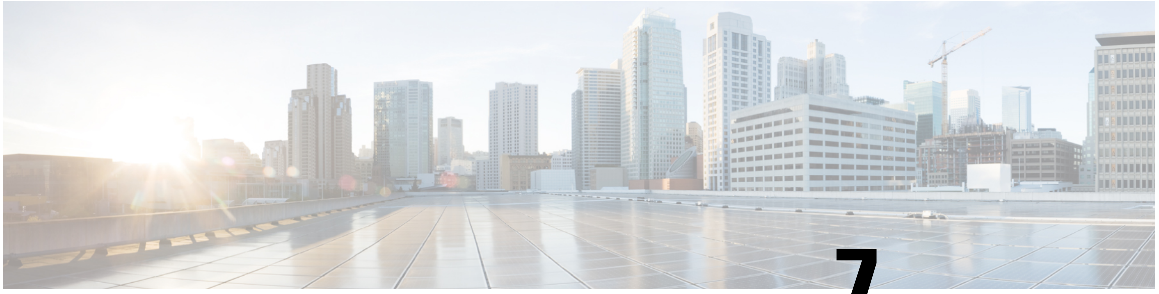
Serial number : *
Sensor's serial number as printed on the side panel
FCW2445P6X5

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



CHAPTER 7

Configure the Cisco Cyber Vision Center synchronization

Global Center Configuration

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

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

Enrollment and unenrollement will be described below.

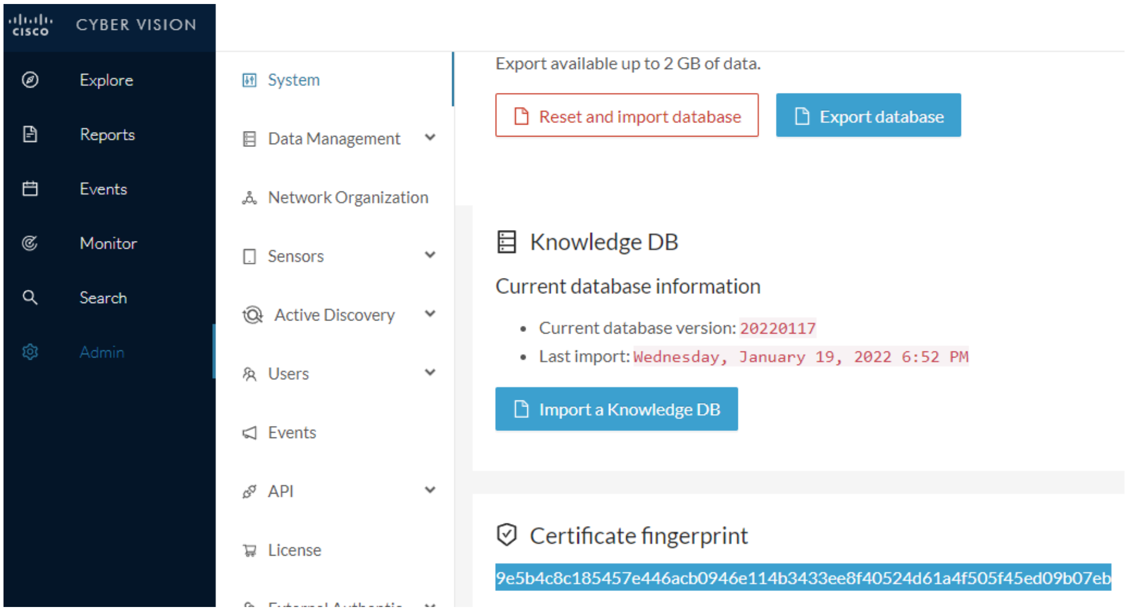
Center enrollment

Before you begin

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

Procedure

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



Export available up to 2 GB of data.

Knowledge DB

Current database information

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

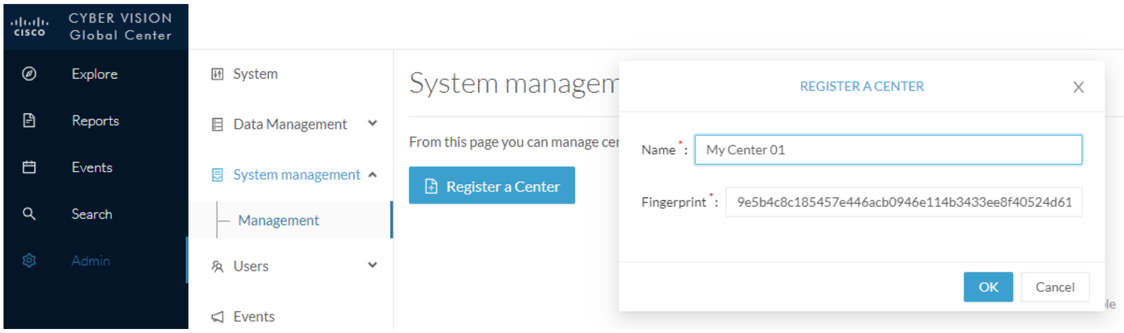
Certificate fingerprint

9e5b4c8c185457e446acb0946e114b3433ee8f40524d61a4f505f45ed09b07eb

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

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

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



System managem

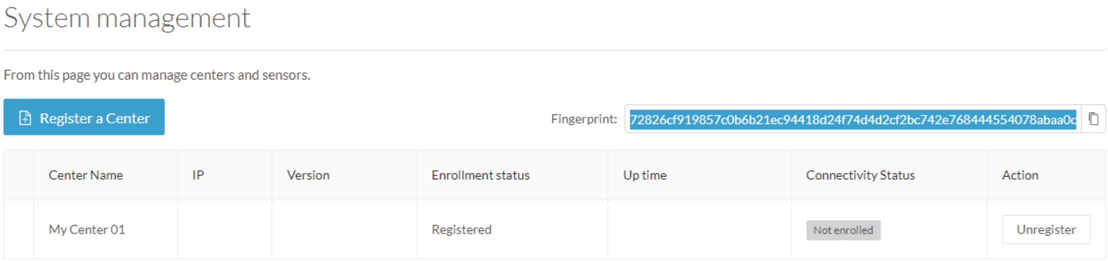
From this page you can manage cer

REGISTER A CENTER

Name * : My Center 01

Fingerprint * : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61

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



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

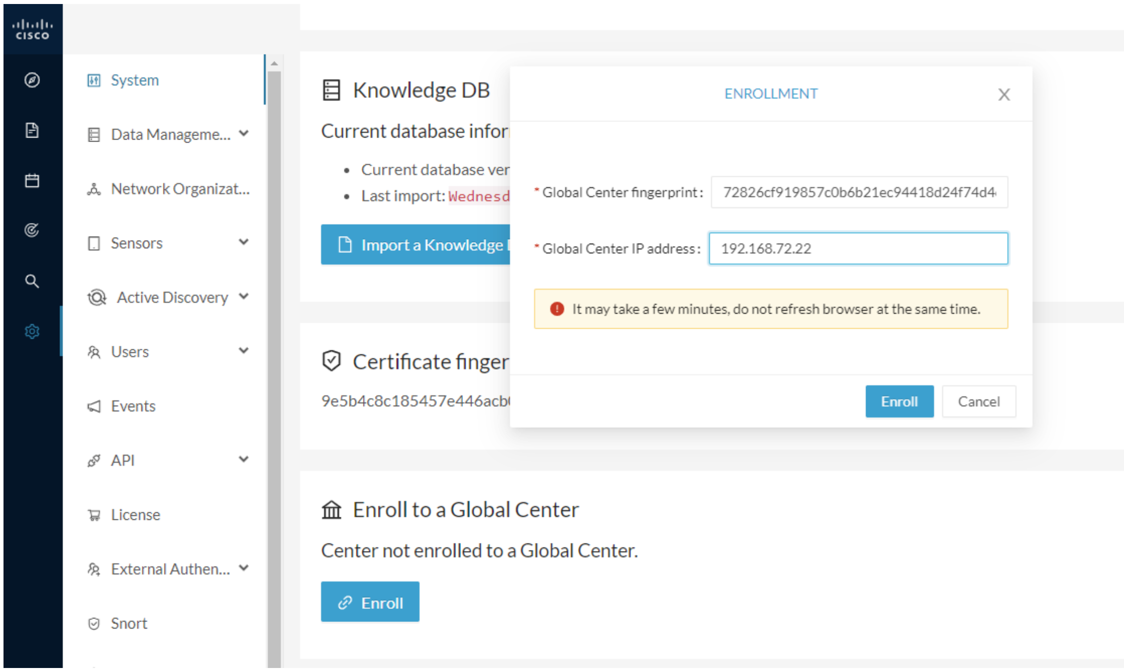
Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
My Center 01			Registered		Not enrolled	Unregister

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

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

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

c) press on **Enroll**



Current database infor

- Current database ver
- Last import: Wednesd

9e5b4c8c185457e446acb

ENROLLMENT

* Global Center fingerprint: 72826cf919857c0b6b21ec94418d24f74d4

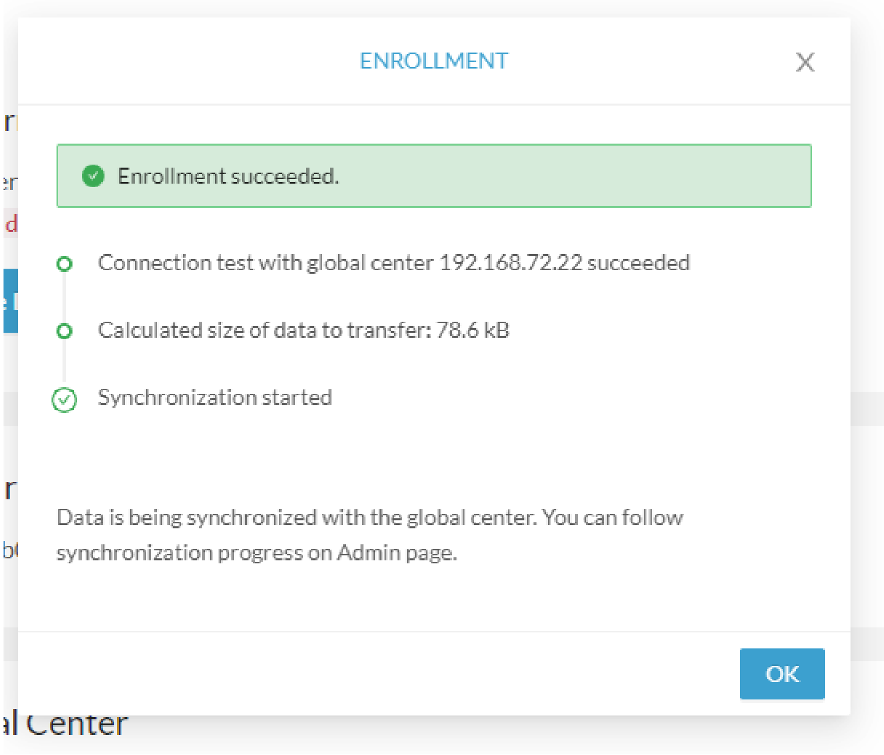
* Global Center IP address: 192.168.72.22

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

Enroll to a Global Center

Center not enrolled to a Global Center.

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



ENROLLMENT

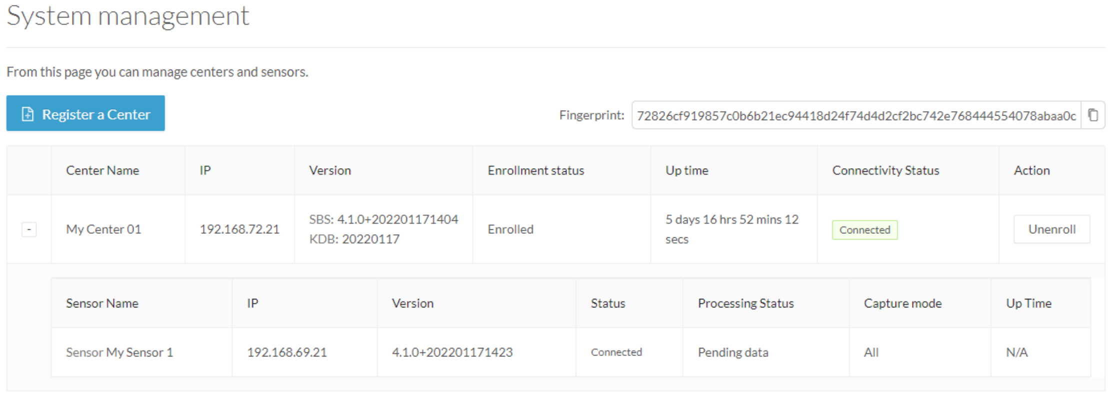
Enrollment succeeded.

- Connection test with global center 192.168.72.22 succeeded
- Calculated size of data to transfer: 78.6 kB
- Synchronization started

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

What to do next

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



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

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

Center unenrollment

Before you begin

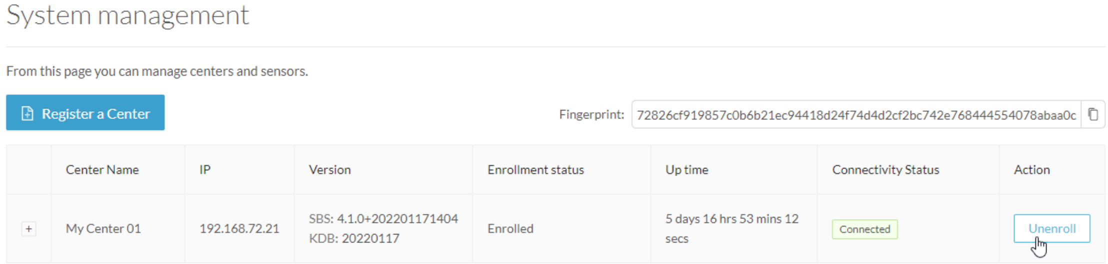
A Center can be unenrolled whenever it is needed, for example as a maintenance operation to replace the Center or the Global Center. This will delete all the Center's data in the Global Center.

Procedure

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

All Centers of the Global Center are listed.

Step 2 Click Unenroll on the Center required.



System management

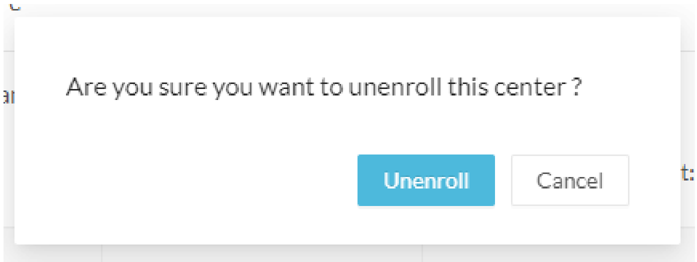
From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

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

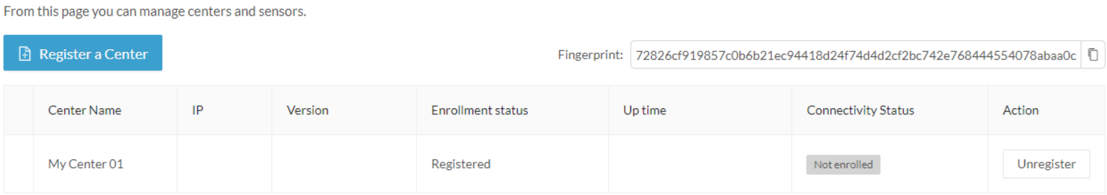
Step 3 A popup asking for confirmation appears. Click **Unenroll** to start the process.



Are you sure you want to unenroll this center ?

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

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



From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

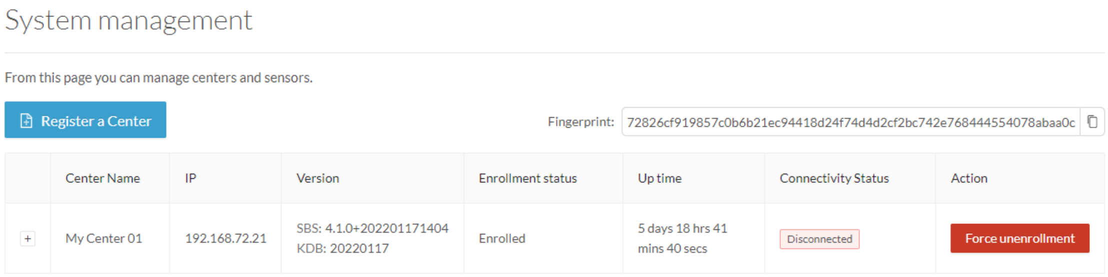
Force the unenrollement of a Center

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

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

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

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



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

CHAPTER 8

Annex – Setup Center json file

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",
}
```