



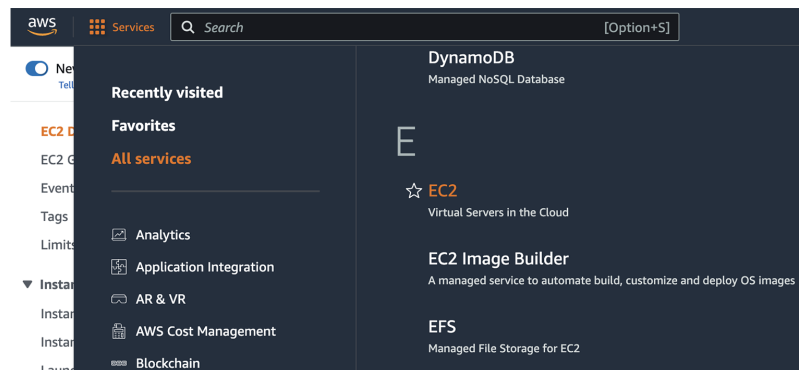
Deploy the Cisco Cyber Vision Center

- [Create and configure the instance, on page 1](#)
- [Allocate an Elastic IP to the instance, on page 9](#)
- [Cisco Cyber Vision Center setup, on page 11](#)

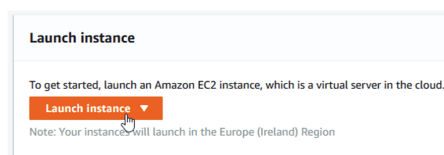
Create and configure the instance

Procedure

- Step 1** Go to <https://aws.amazon.com> Amazon Web Services and sign in.
- Step 2** Navigate to **All services > EC2**.

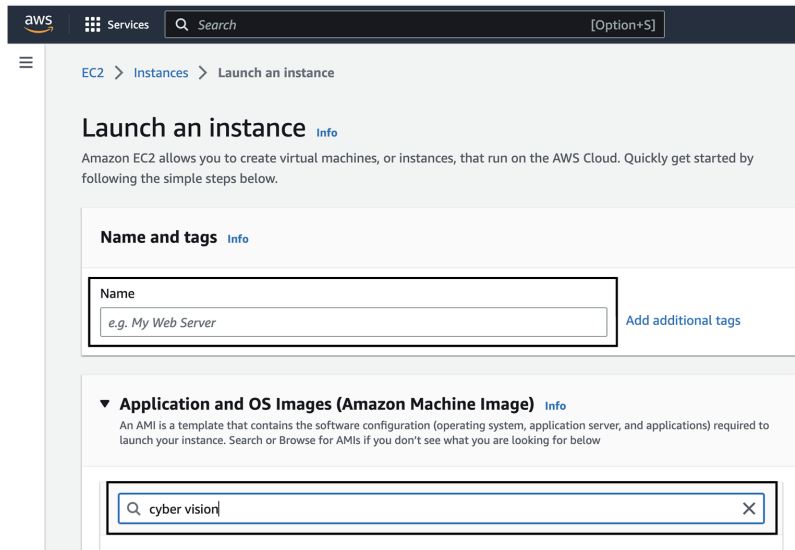


- Step 3** Click **Launch Instance**.



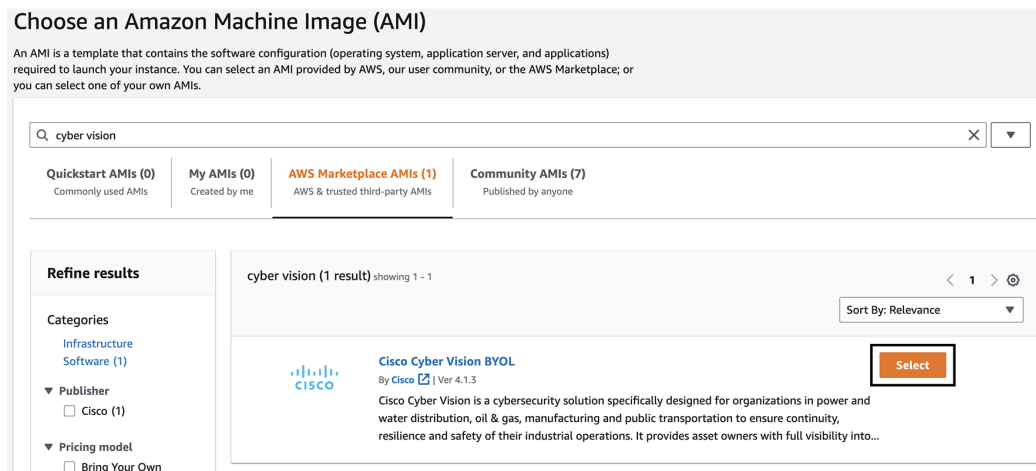
- Step 4** Give the instance a name.
- Step 5** Type "cyber vision" in the AMI search bar.

Create and configure the instance



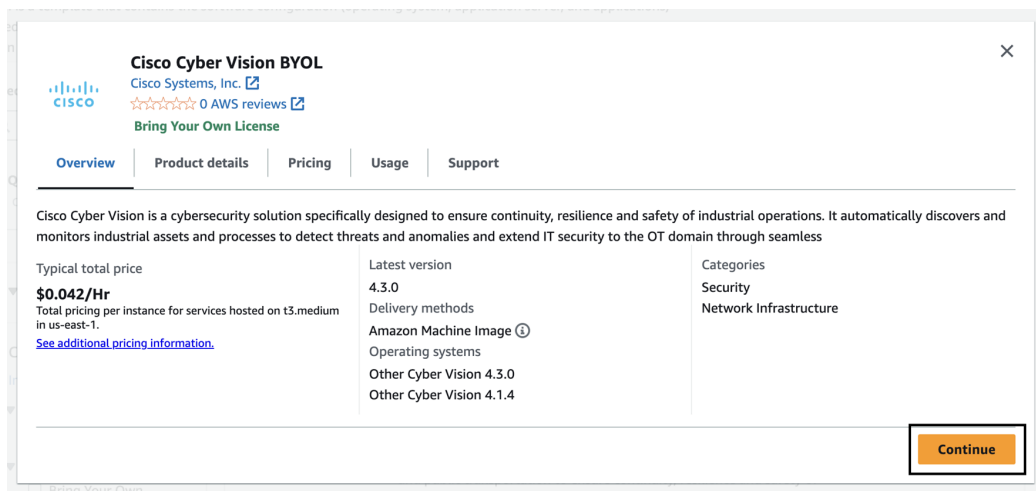
Step 6

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



Step 7

Click Continue.



Step 8 Slide down to instance type.

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

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

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t3.medium
Family: t3 2 vCPU 4 GiB Memory Current generation: true

Q t3.x

t3.xlarge
Family: t3 4 vCPU 16 GiB Memory Current generation: true

All generations

[Compare instance types](#)
this product.

▼ **Key pair (login)** [Info](#)

Step 10 Select or create a new key pair.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

JMA

[Create new key pair](#)

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

Edit

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

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 [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 [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)

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

[Add new volume](#)

[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.

[Choose file](#)

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
64%

Subscribing to Marketplace AMI

▶ Details

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

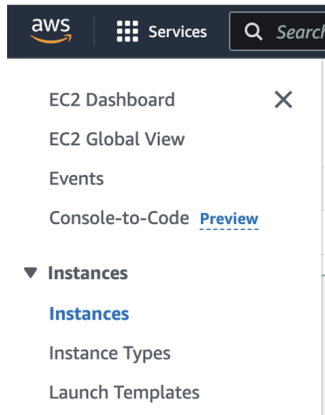
EC2 > Instances > Launch an instance

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, click on the link in the top right corner.

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 >

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**

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

Warning: 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

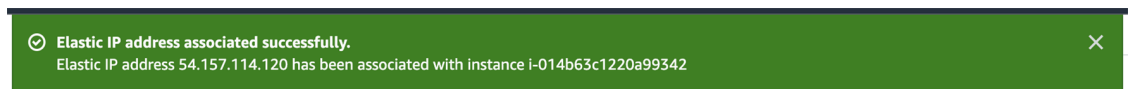
Private IP address
The private IP address with which to associate the Elastic IP address.
172.31.7.229

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

Cancel Associate

The following status should appear.



Cisco Cyber Vision Center setup

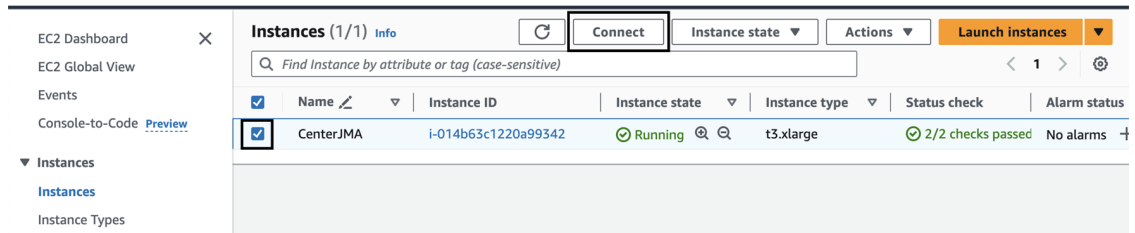
Establish a serial connection or open an SSH connection from AWS and then proceed to the basic Center configuration.

Establish a serial connection

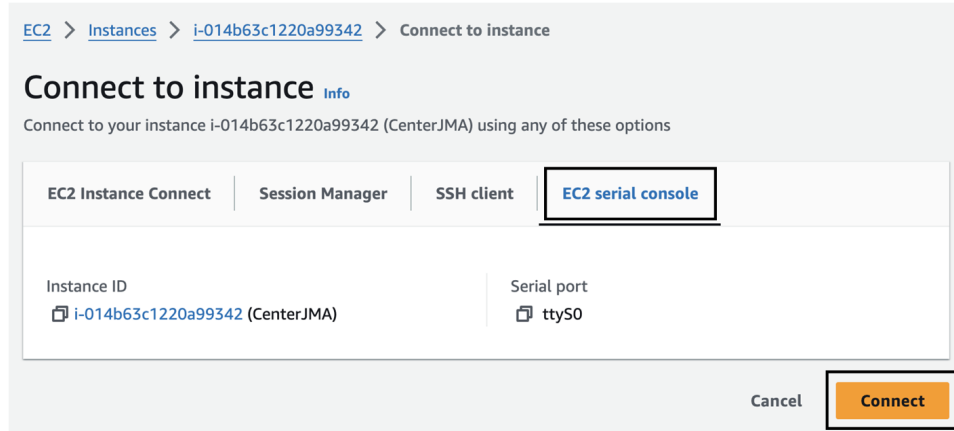
Procedure

- 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**.

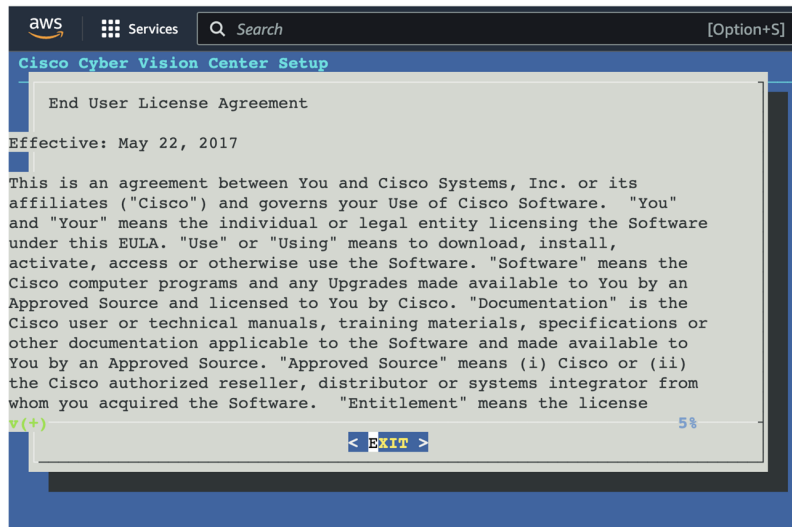


Step 3 Click **Connect**.

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. The summary includes the following details:

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

Below the summary, the 'Instance details' section is expanded, showing:

Platform	AMI ID	Monitoring
Linux/UNIX (Inferred)	ami-0ddb5a307abb22bd2	disabled
Platform details	AMI name	Termination protection
Linux/UNIX	Cyber Vision Center - 4.0.0-RC4	Disabled

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

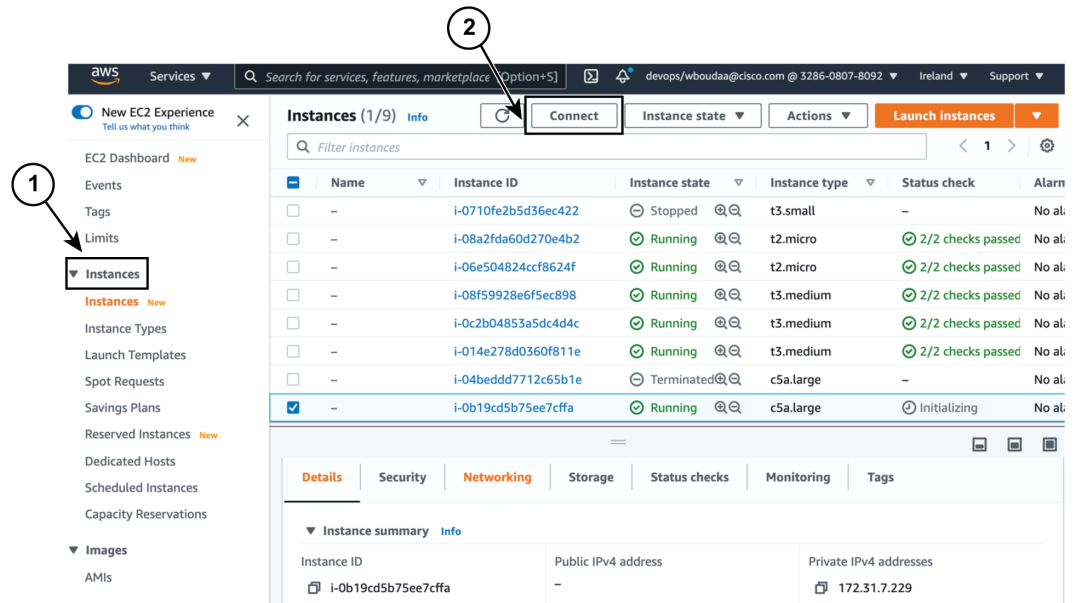


Note It is possible to add multiple keys on that file if an access is needed from another device that is not using the same certificates than the installed one.

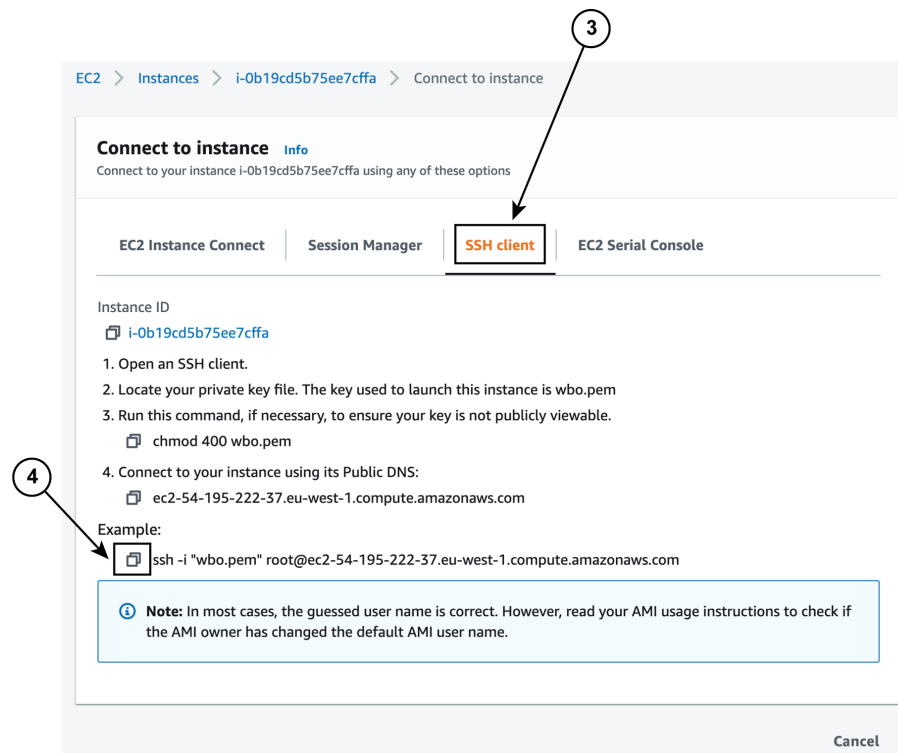
This key is downloaded locally or already exists.

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).



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
```

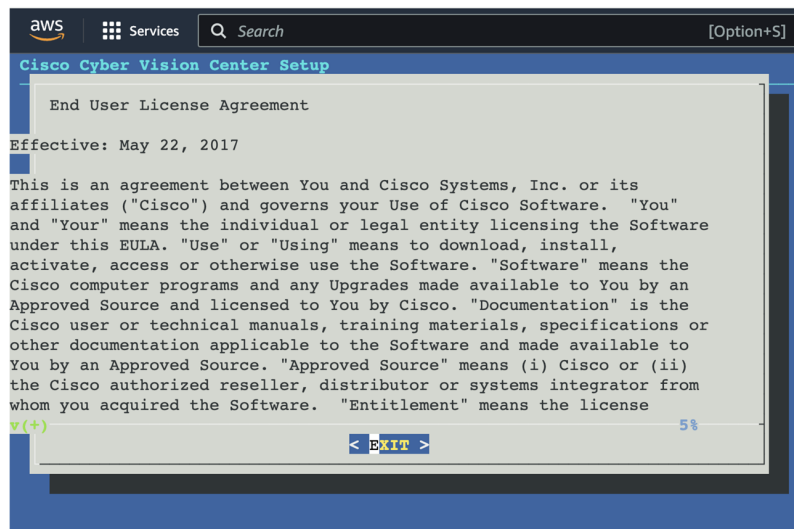
7. Type the following command:

```
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**.

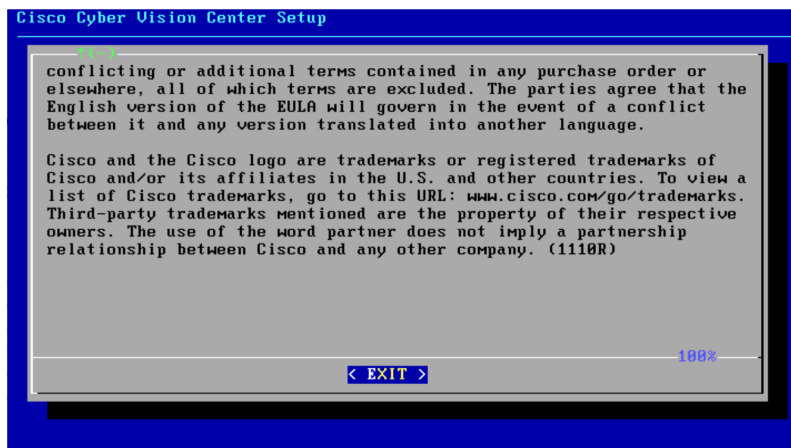
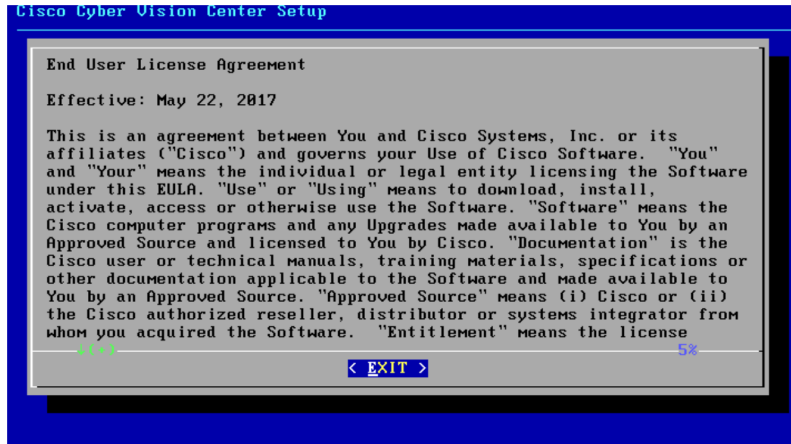
The Cisco Cyber Vision Center Setup appears.



9. Press **Enter**.

Basic Center configuration

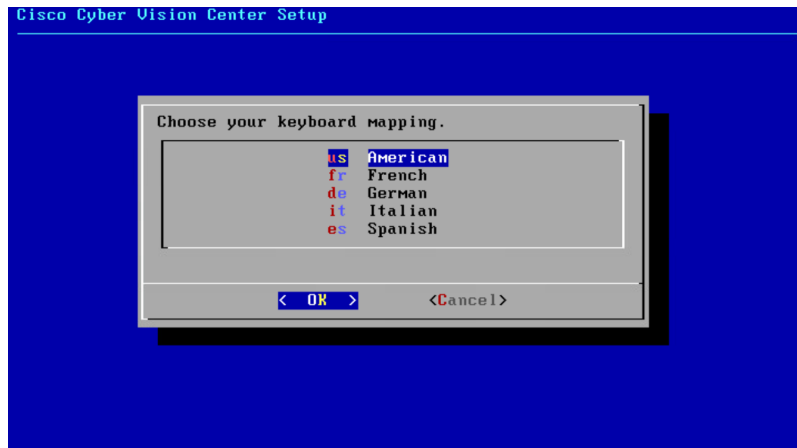
Accept the End User License Agreement



Select the language to match your keyboard



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

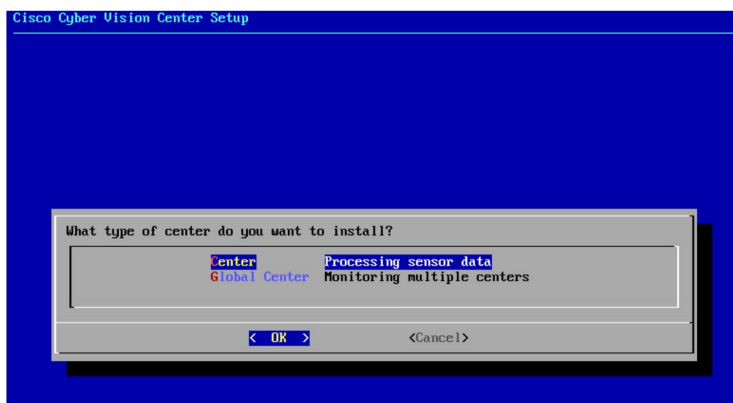


Select the Center type

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

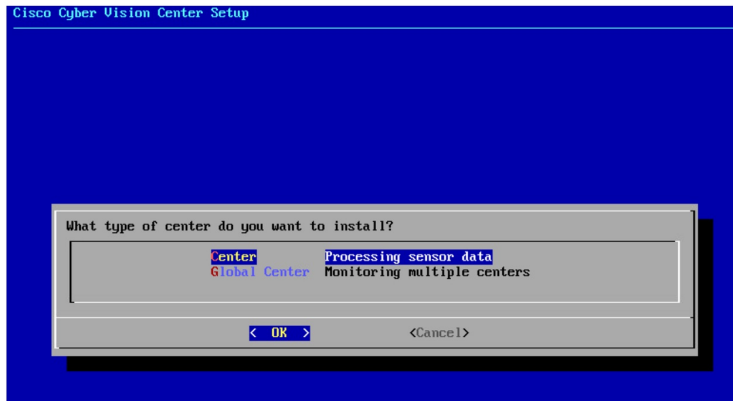
- A **Center** receives metadata from sensors and store them into an internal database (Postgresql). It can be standalone or synchronized with a Global Center. A Center with sync is similar to a standalone Center from a functionality point of view, except for the link to a Global Center. You must install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



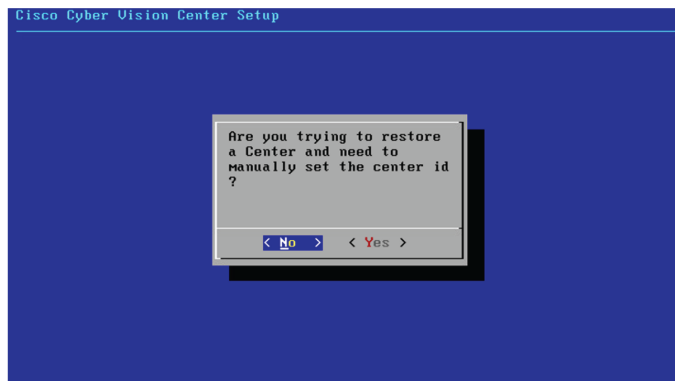
Center

If installing a Center, select the first option.

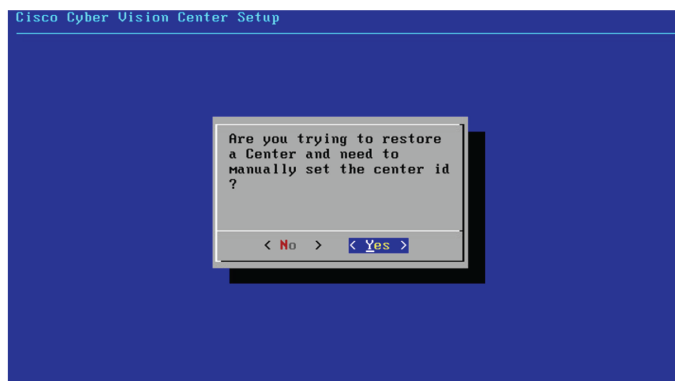


Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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.



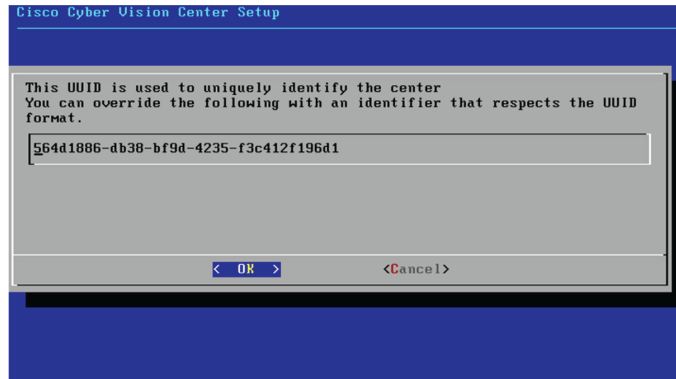
If you're reinstalling the Center and want to restore it, select Yes.



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"
```

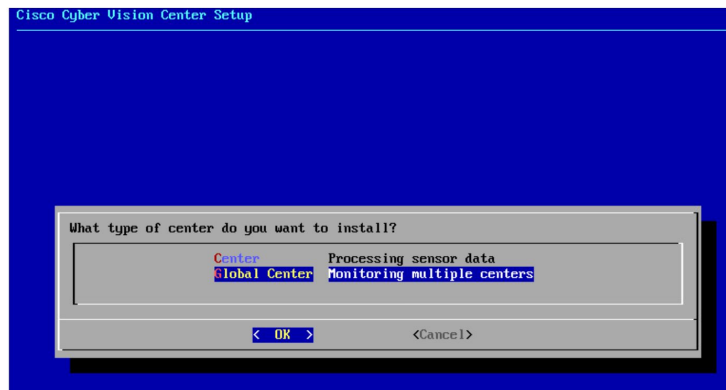
Type the id into the basic Center configuration UUID field.



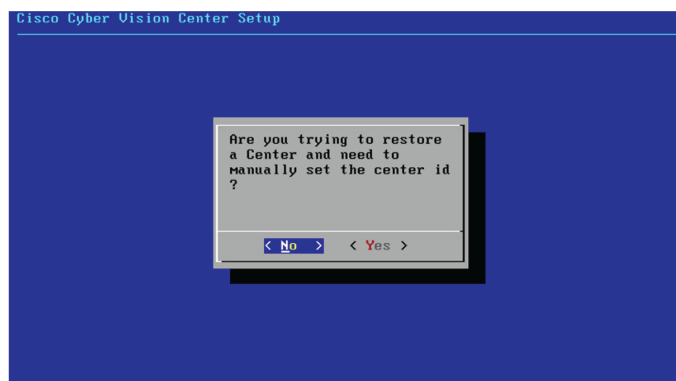
Click OK. You will be directed to the next step.

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.

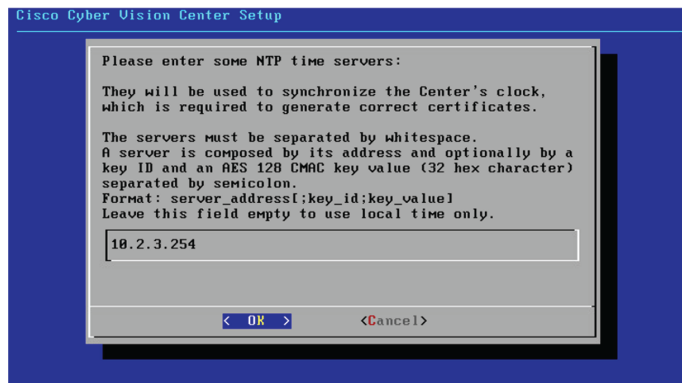
Configure the Center's DNS

Type a DNS server address and optional fallbacks.

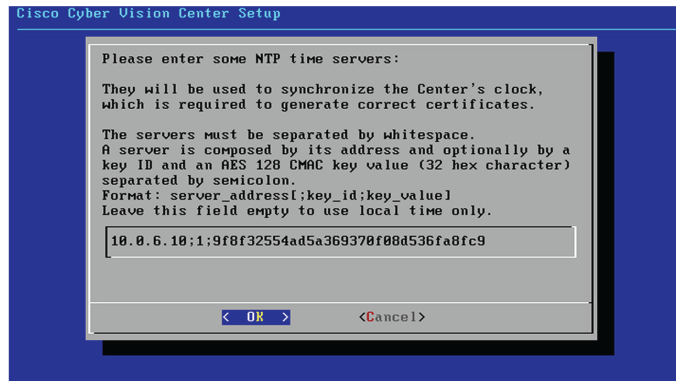


Synchronize the Center and the sensors to NTP servers

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.

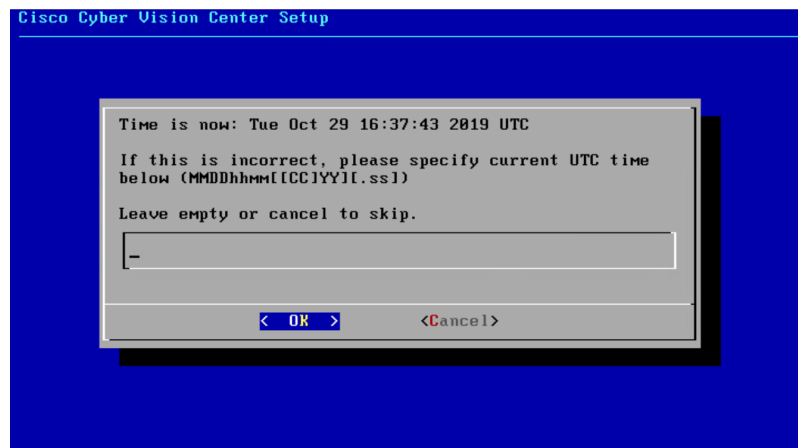


The synchronization takes a few seconds.

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



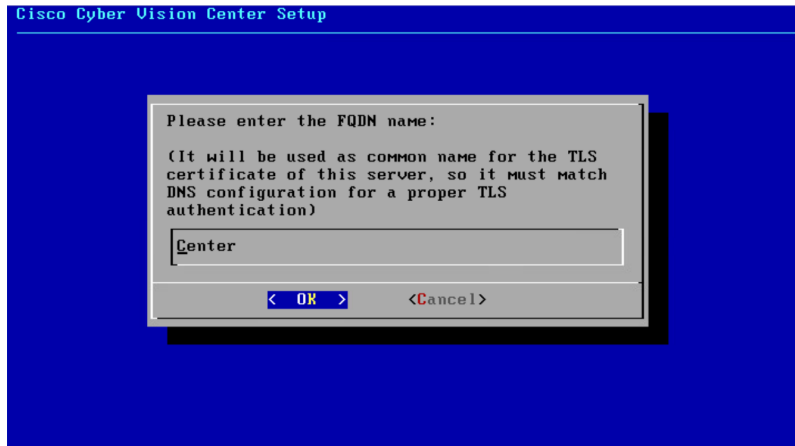
Note The time is set in UTC standard.



Give the Center a name



Note This name will be used in the Center certificate.



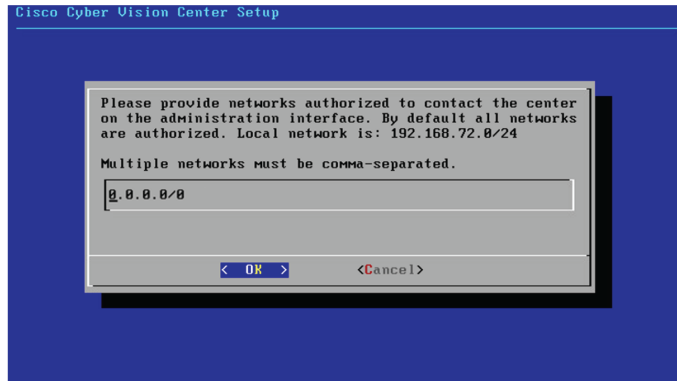
Enter the Center name provided by your administrator or type 'Default' which is a secure value.



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

Authorize networks

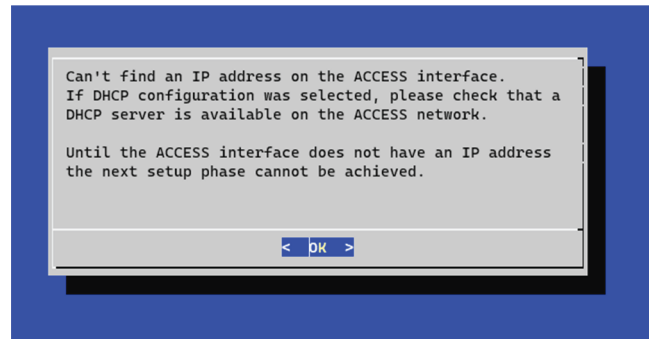
This step allows you to restrict IP addresses that can connect to the Administration interface. If no IP is entered, all networks are authorized by default.



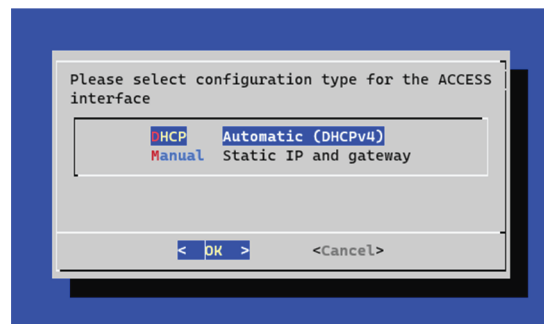
Set DHCP

Procedure

Step 1 If the following message appears, select OK.

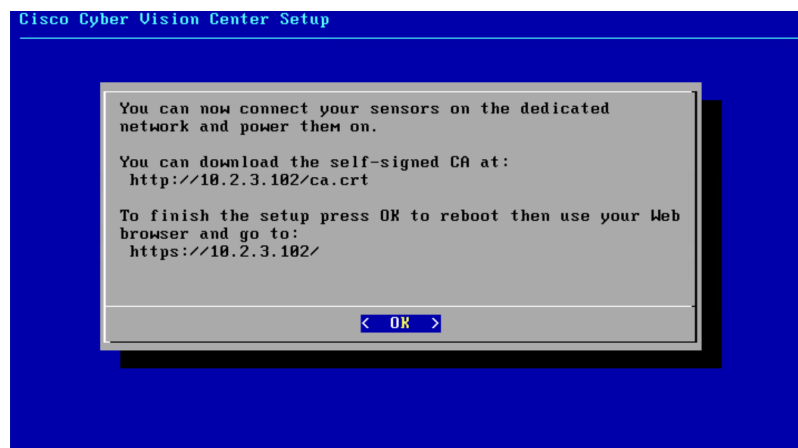


Step 2 Select DHCP.



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).