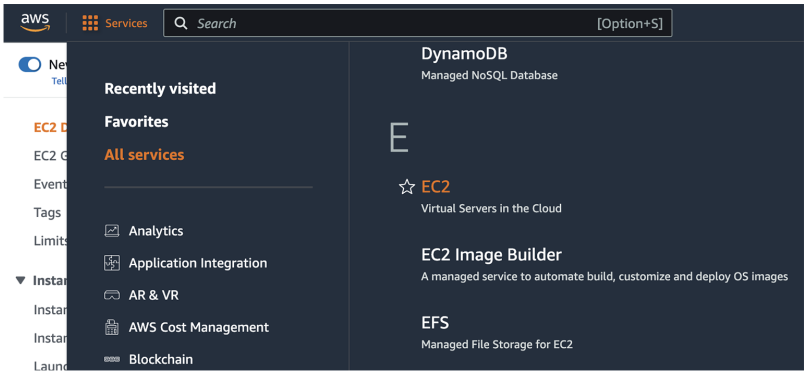
Deploy the Cisco Cyber Vision Center

Create and configure the instance

Procedure

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

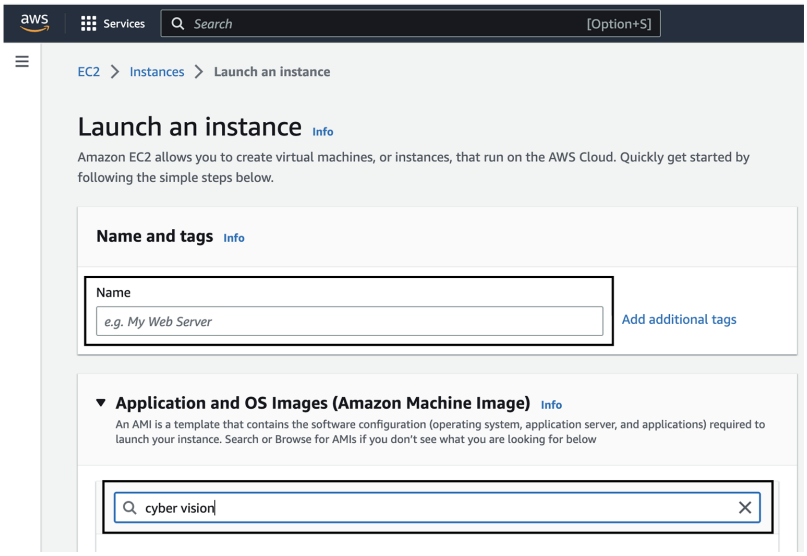
Step 2 Navigate to **All services** > **EC2**.



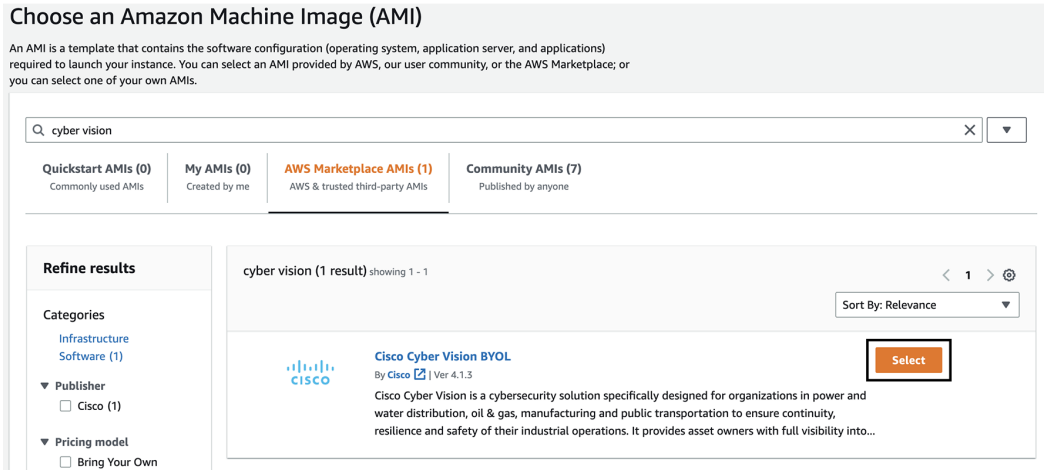
Step 3 Click **Launch Instance**.

Step 4 Give the instance a name.

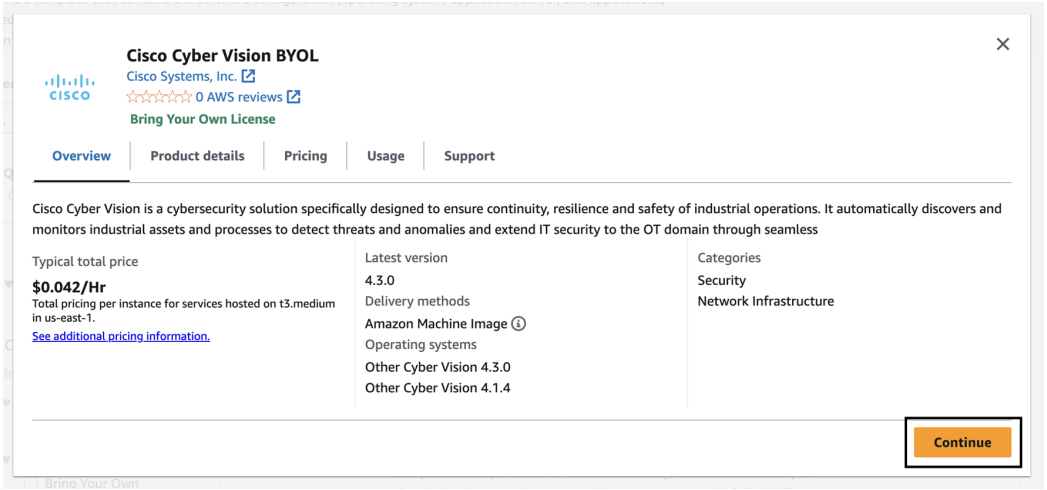
Step 5 Type "cyber vision" in the AMI search bar.



Step 6 In the AWS Marketplace AMIs menu, **select** Cisco Cyber Vision BYOL.



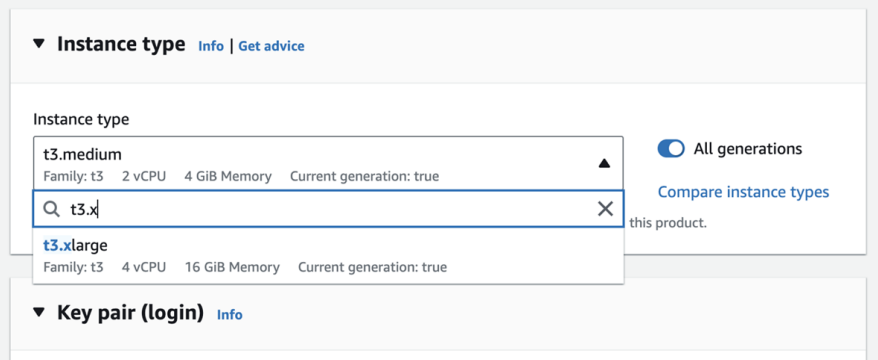
Step 7 Click **Continue**.



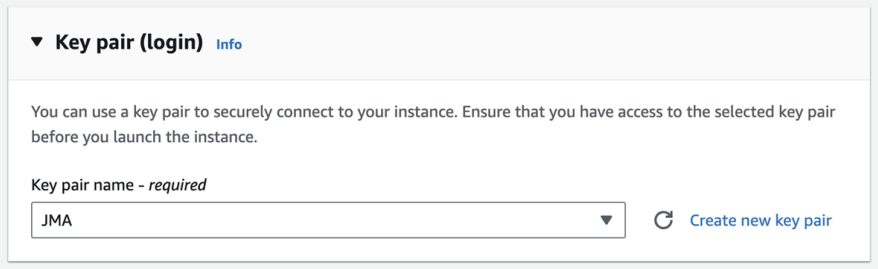
Step 8 Slide down to instance type.

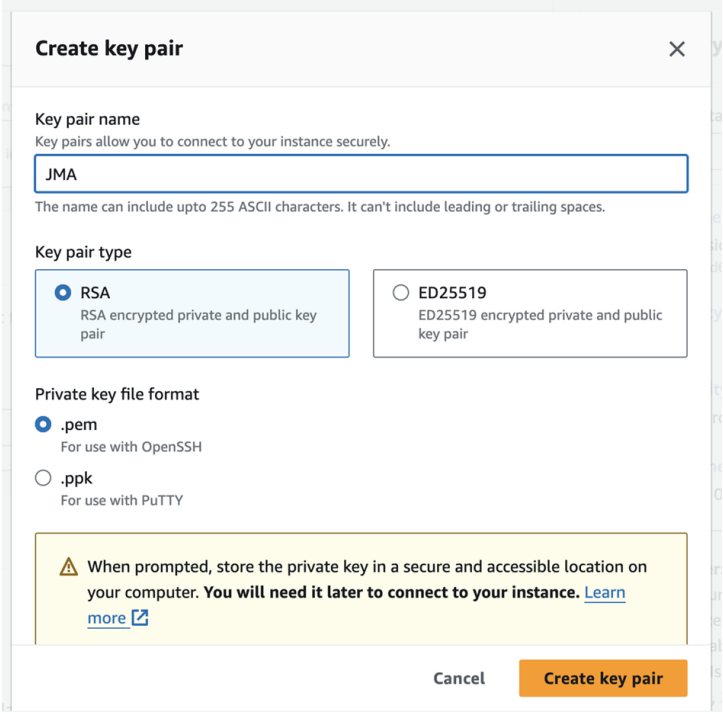
Supported instance families
• C5, C5a, C5ad, C5d, C5n, C6g, C6gd • M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd • R5, R5a, R5ad, R5d, R5dn, R5n, R6, R6gd • T3, T3a, T4g • Z1d

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



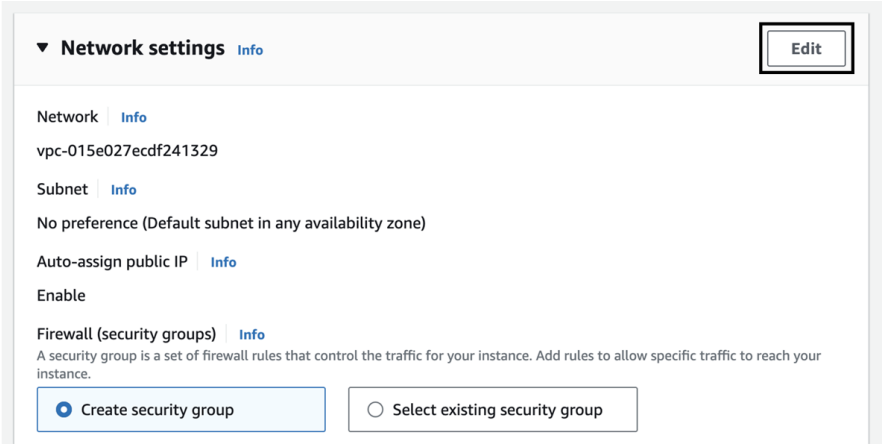
Step 10 Select or create a new key pair.



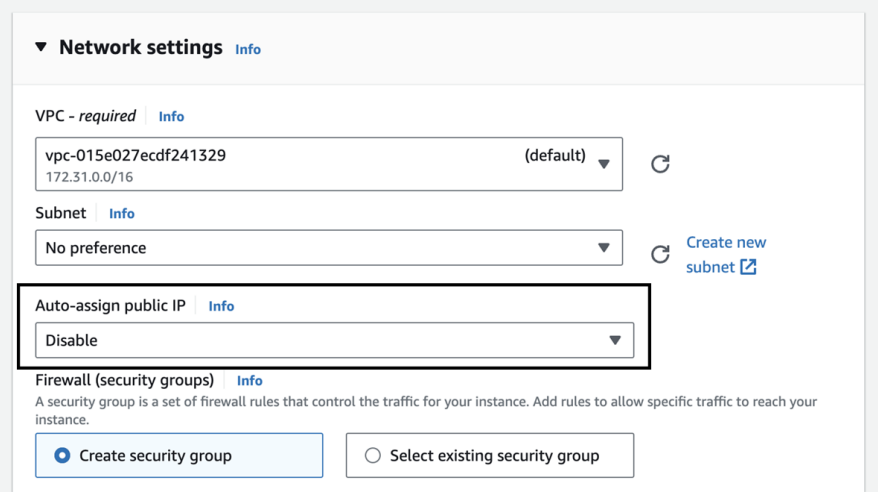


A file called YOURKEYPAIRNAME.pem will be downloaded.

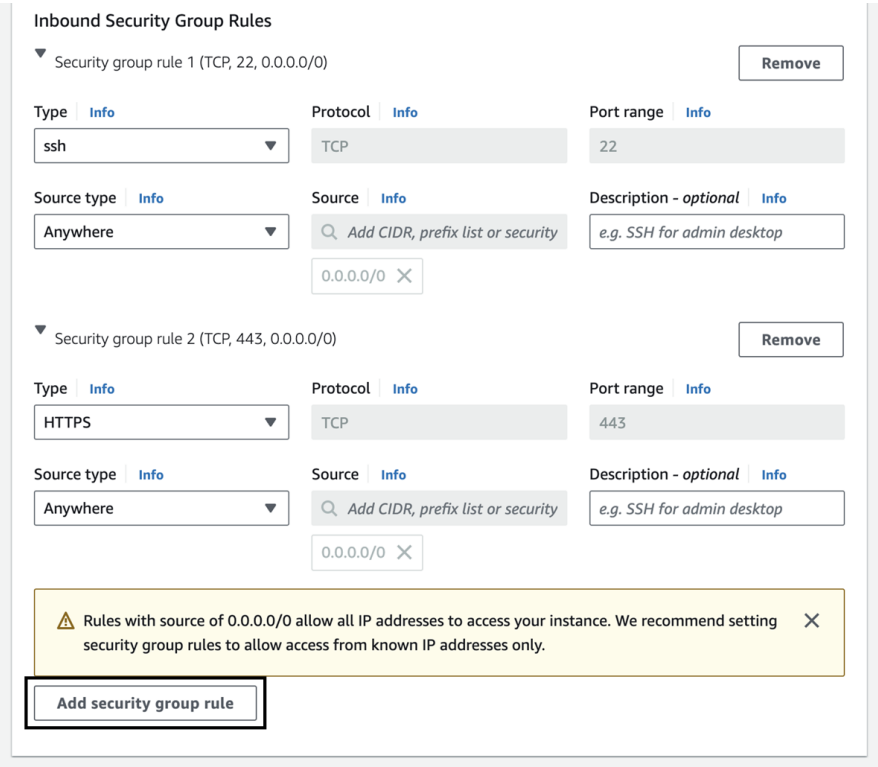
Step 11 Slide down to Network settings and click **Edit**.



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



Inbound Security Group Rules appears.



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)

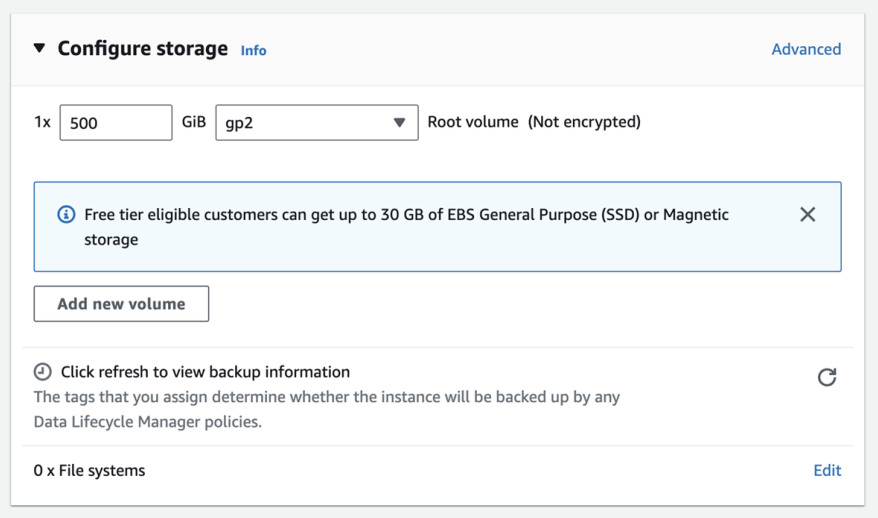
Step 14 Configure storage by changing the value or ,if needed, adding a new volume.

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.



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

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:

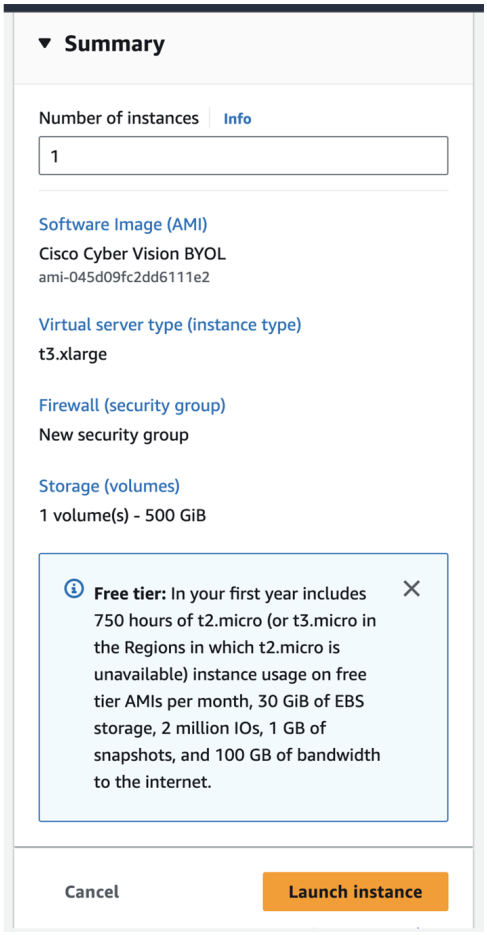
```
{
"center-type": "Local Center",
}
```

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

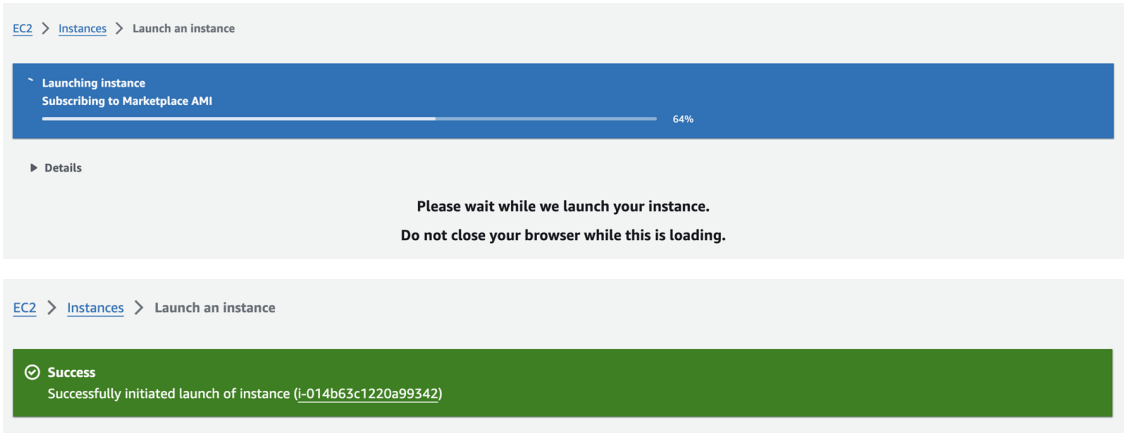
```
{
"center-type": "Global Center",
}
```

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

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

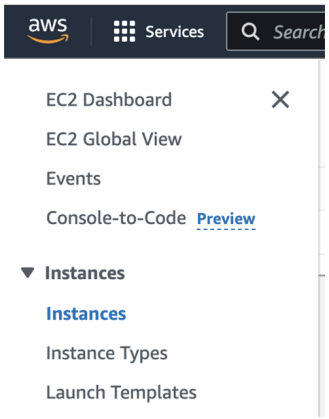


The following status should appear.

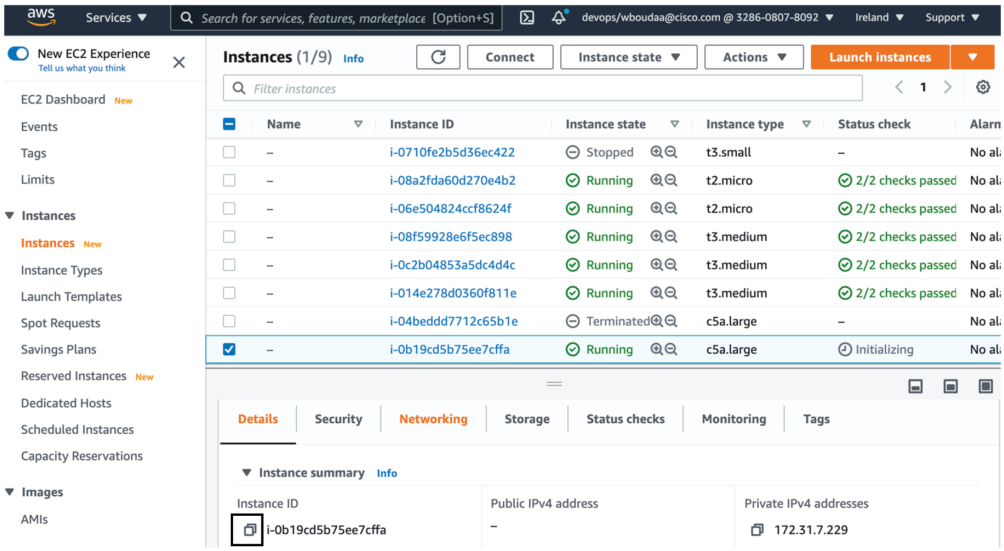


Allocate an Elastic IP to the instance

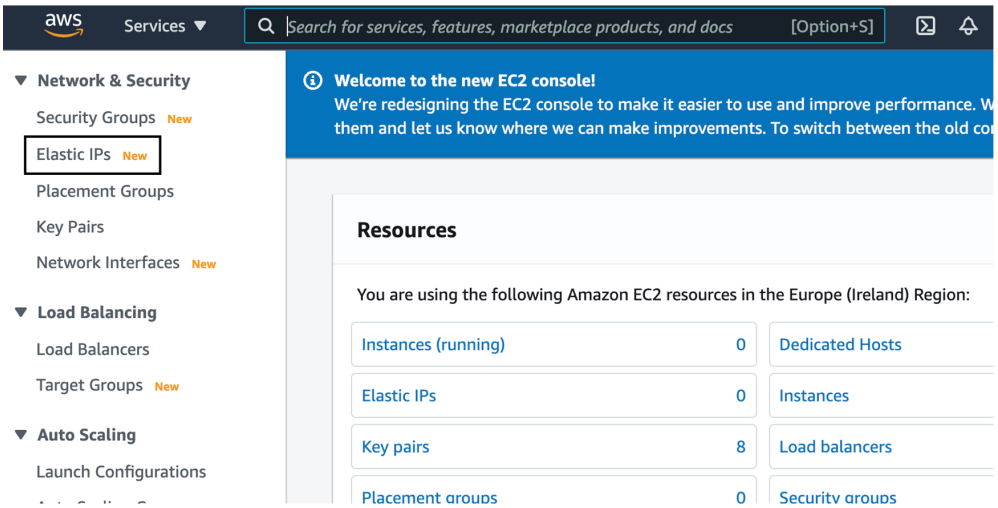
1. Click **Instances** in AWS left menu.



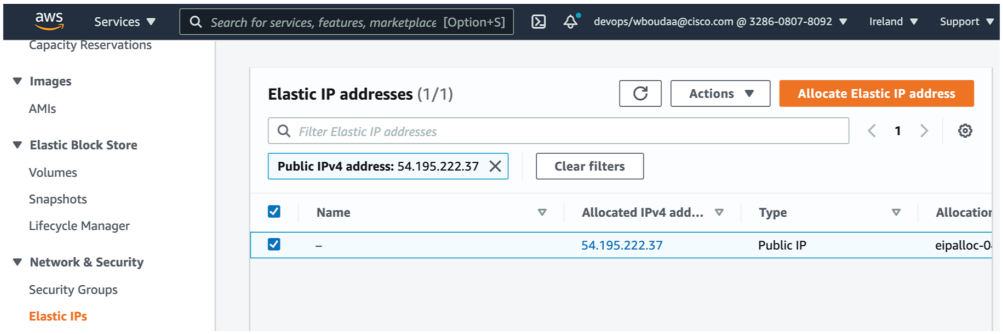
2. Choose your instance on the instances list and copy your instance ID.



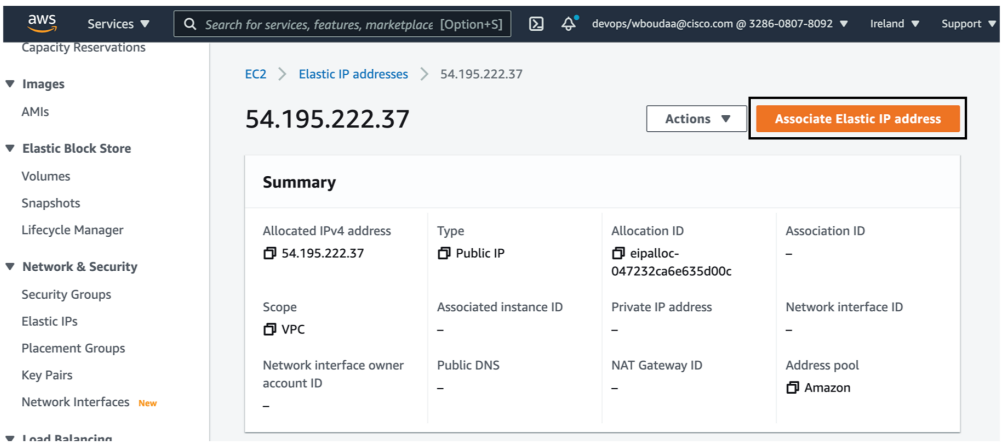
3. Click **Elastic IPs** in AWS left menu.



4. Click the created Elastic IP.

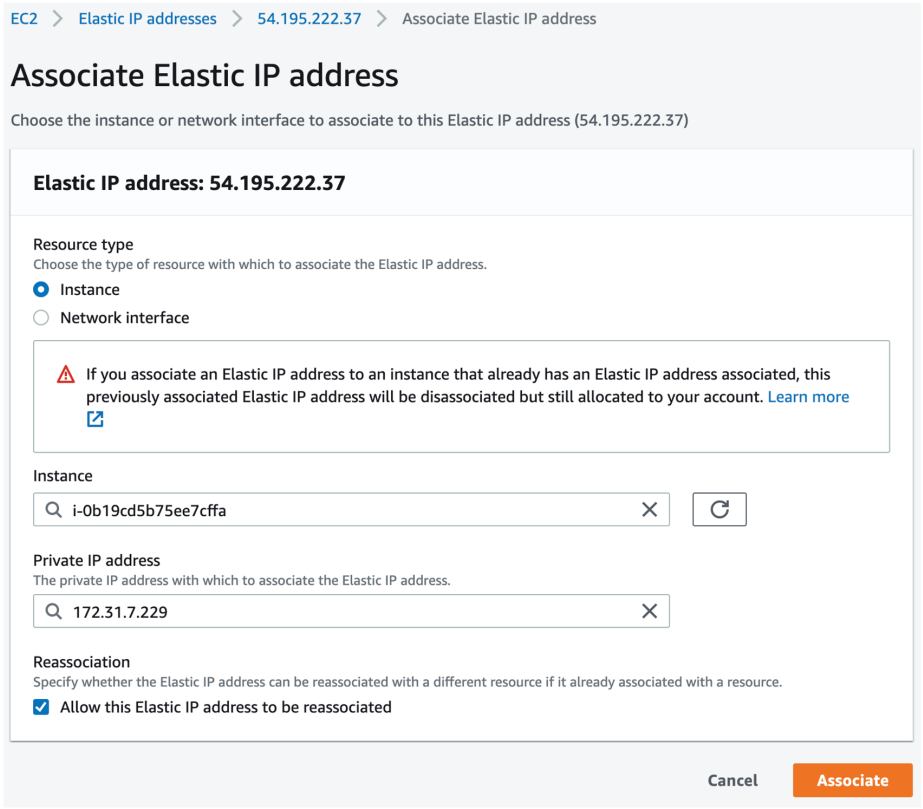


5. Click **Associate Elastic IP address**.

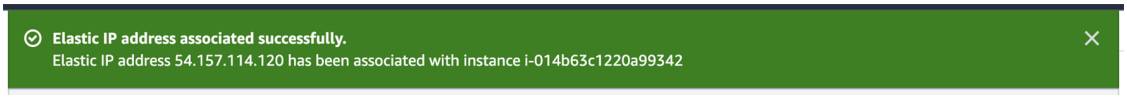


6. Select **Instance**.
7. Paste the instance ID previously copied.

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



The following status should appear.



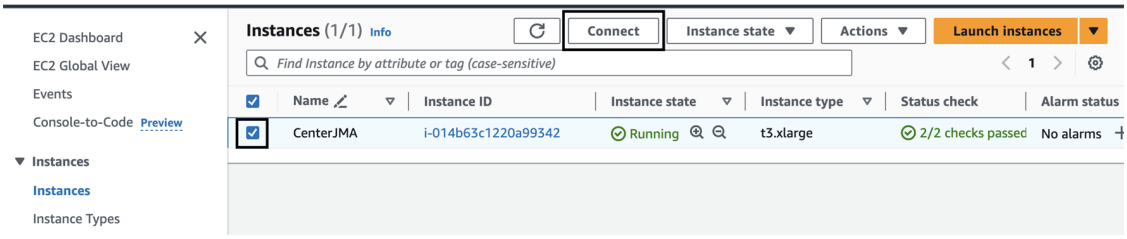
Cisco Cyber Vision Center setup

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

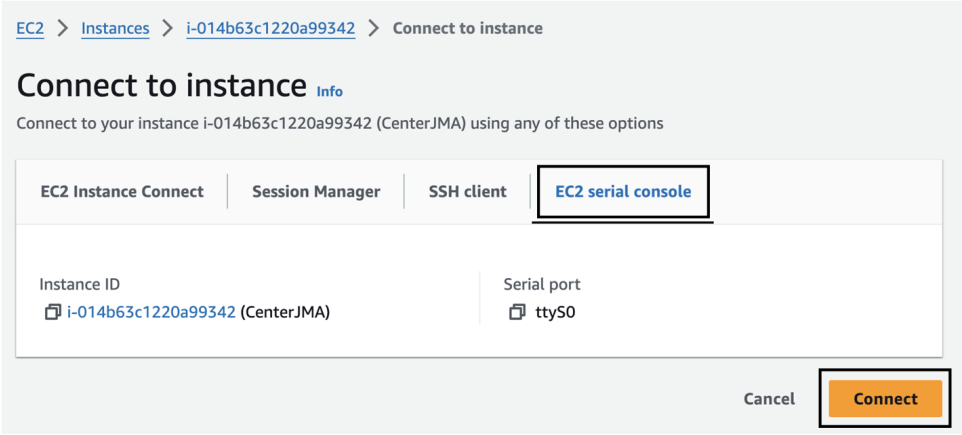
Establish a serial connection

Procedure

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



Step 2 Click **EC2 serial console**.

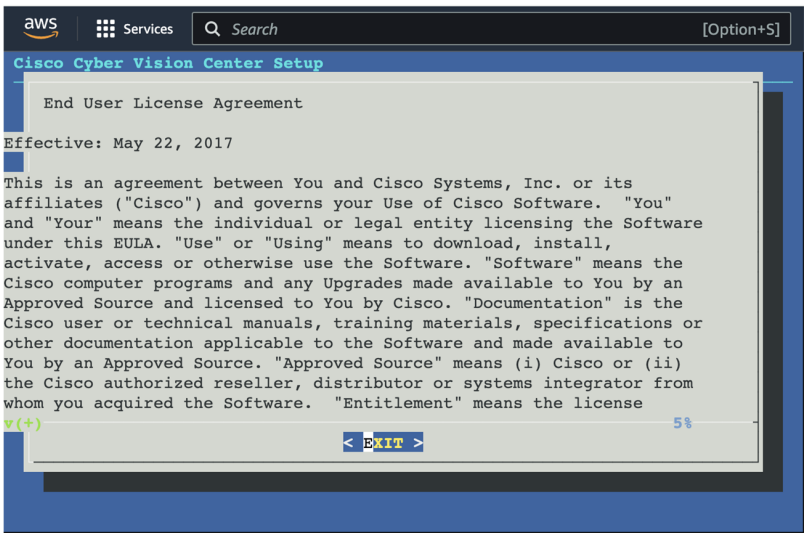


Step 3 Click **Connect**.

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

Step 5 Press **Enter**.

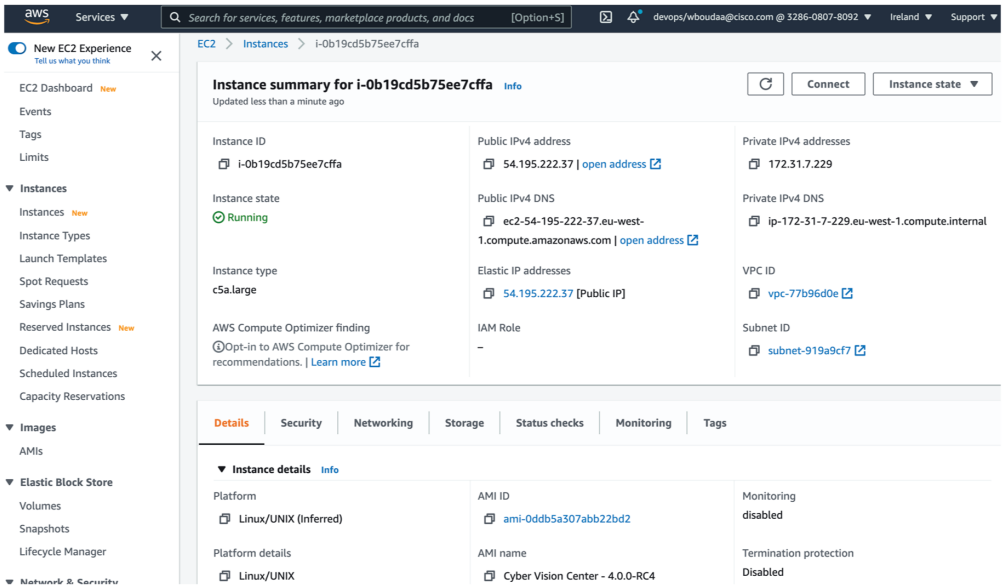
The Cisco Cyber Vision Center Setup appears.



Step 6 Press **Enter**.

Open an SSH connection from AWS

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



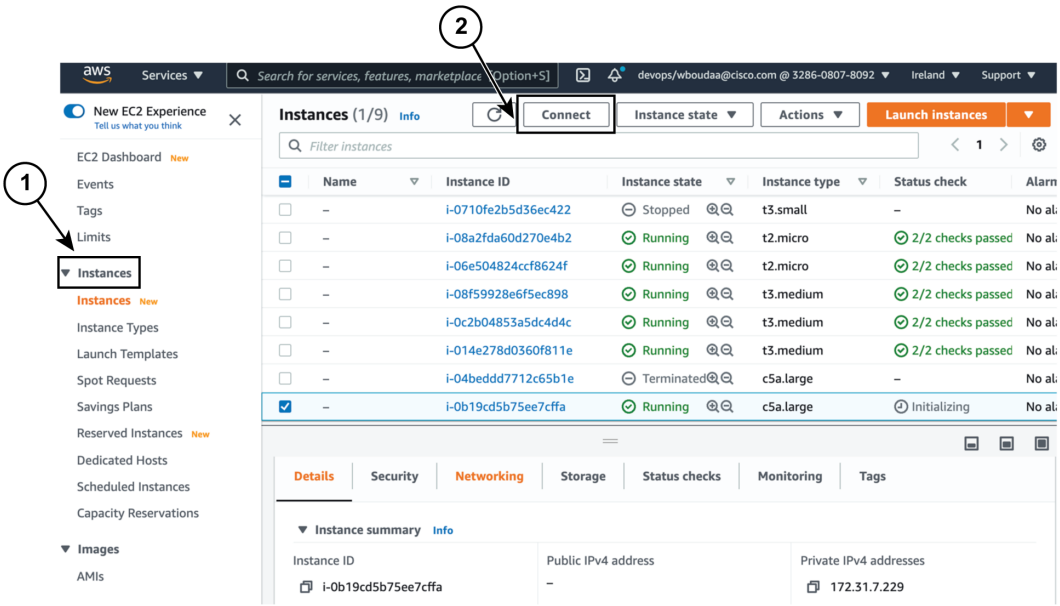
The key previously created or chosen will be automatically added to /data/etc/ssh/userkey/root.

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.

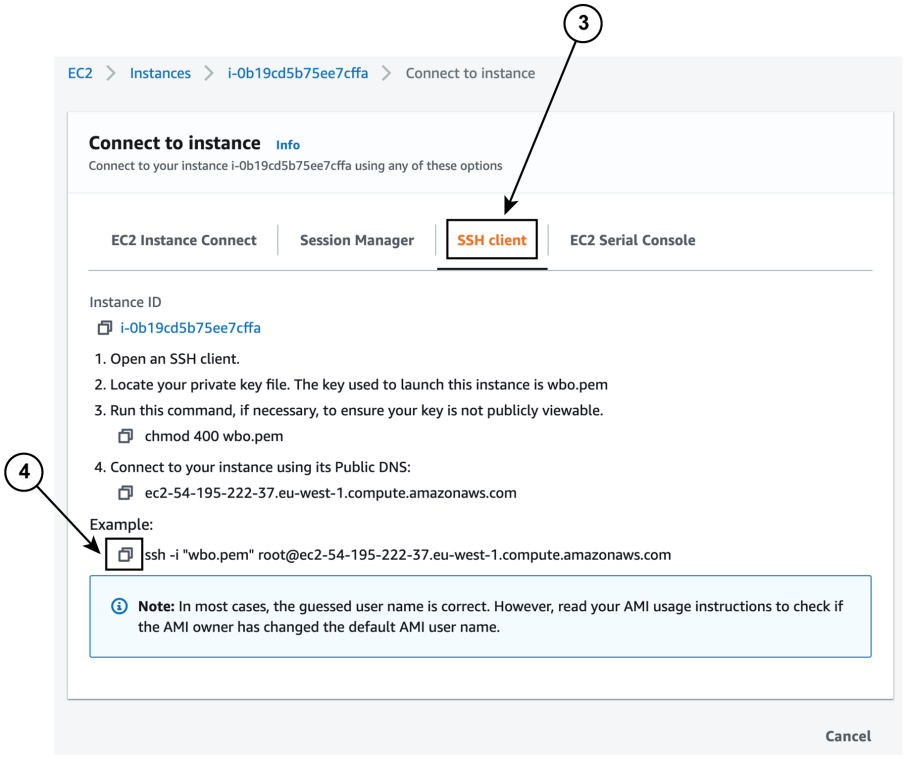
This key is downloaded locally or already exists.

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.

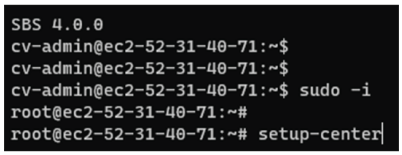


5. Copy and paste the example **(4)** into the ssh client and replace ‘root’ with ‘cv-admin’, like below: ssh -i wbo.pem cv-admin@ec2-54-195-222-376.eu-west-1.compute.amazonaws.com
6. Once connected to the Center, type the following command:

```
sudo -i
```

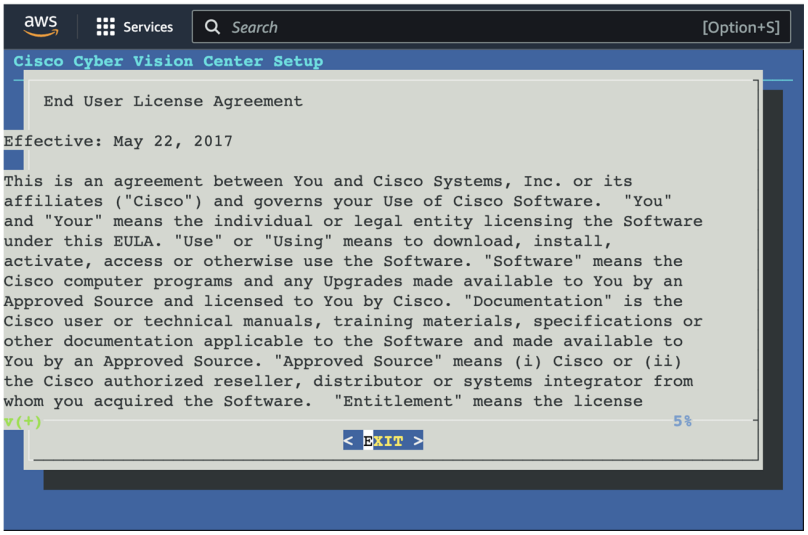
7. Type the following command:

```
setup-center
```



8. Press **Enter**.

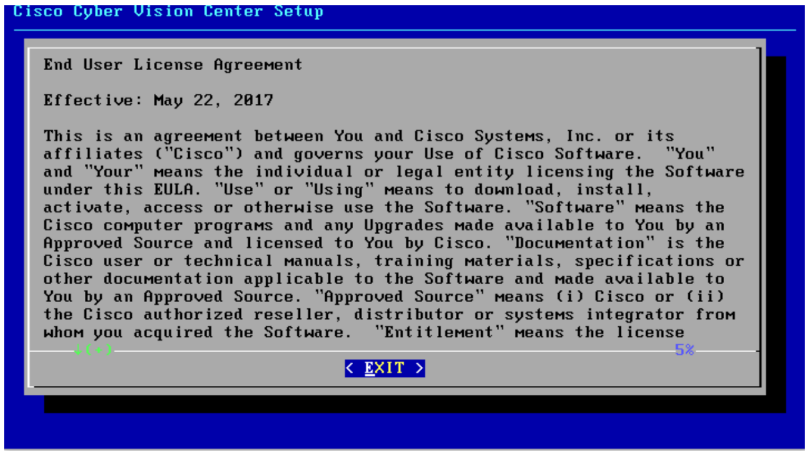
   The Cisco Cyber Vision Center Setup appears.

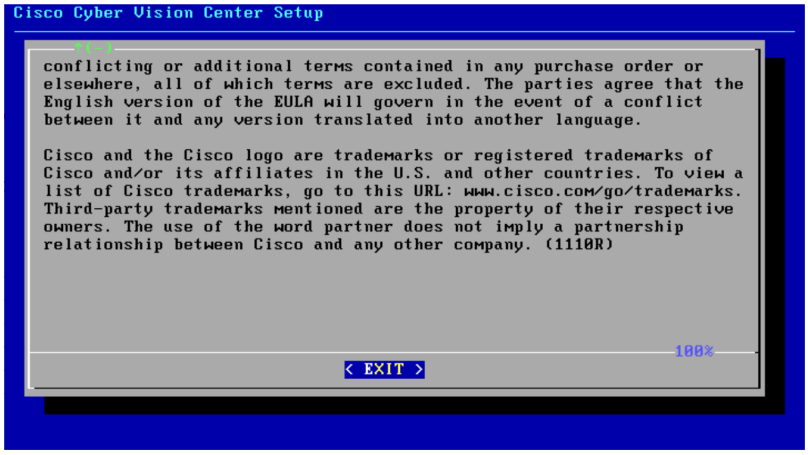


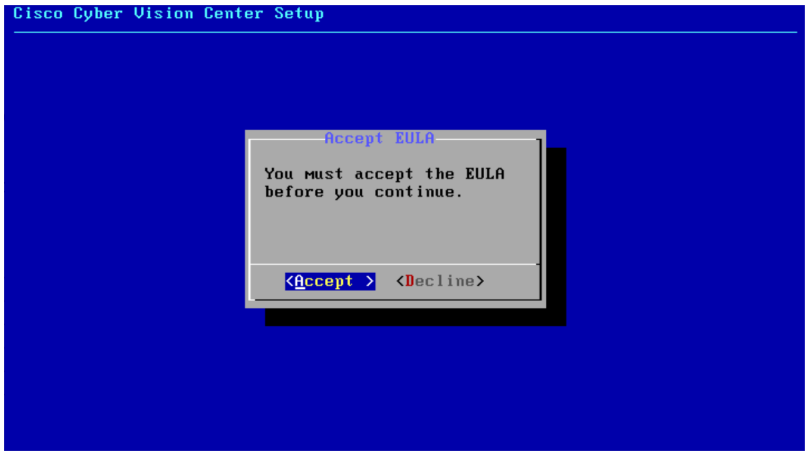
9. Press **Enter**.

Basic Center configuration

Accept the End User License Agreement

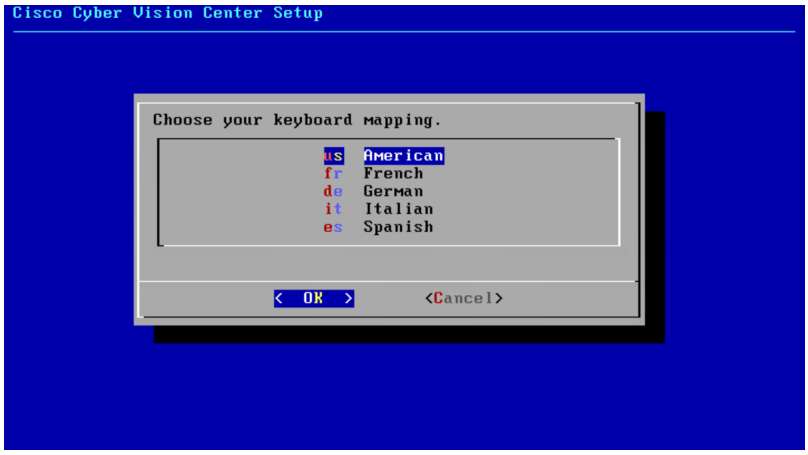






Select the language to match your keyboard

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

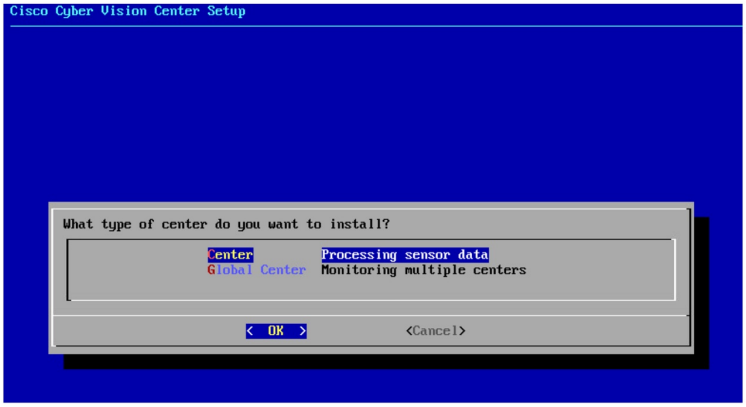


Select the Center type

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

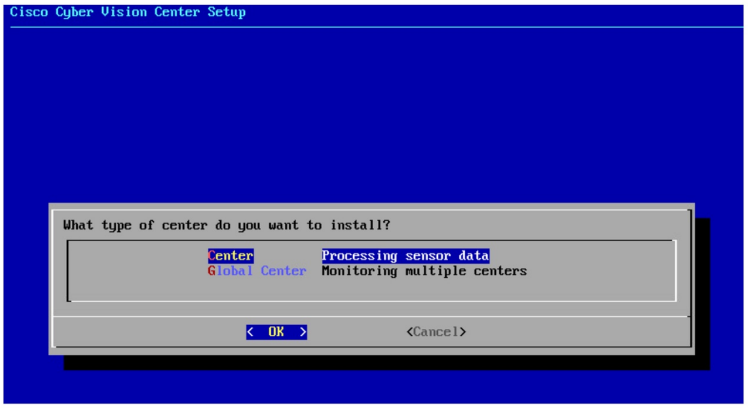
- A **Center** receives metadata from sensors and store them into an internal database (Postrgresql). It can be standalone or synchronized with a Global Center. A Center with sync is similar to a standalone Center from a functionality point of view, except for the link to a Global Center. You must install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

Select the type of Center you want to install.



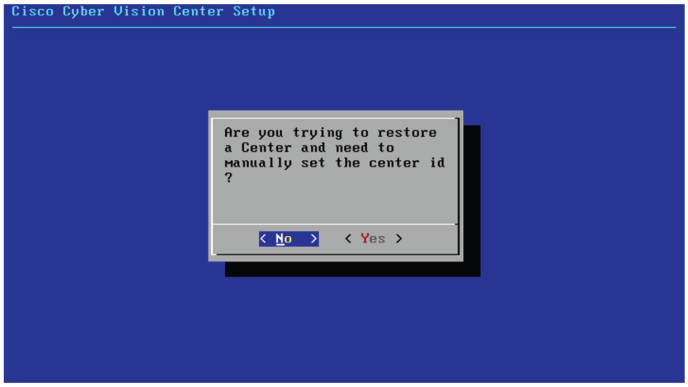
Center

If installing a Center, select the first option.

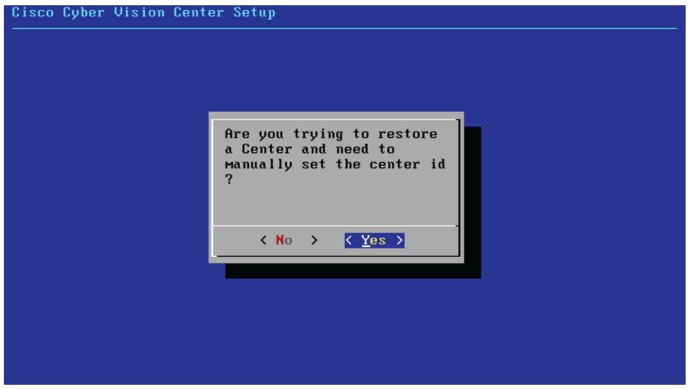


Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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.



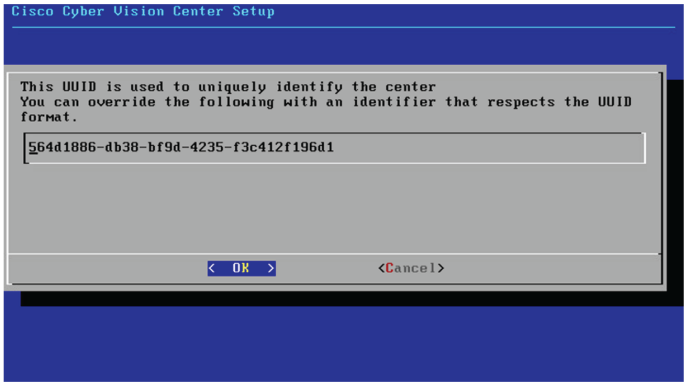
If you're reinstalling the Center and want to restore it, select Yes.



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"
```

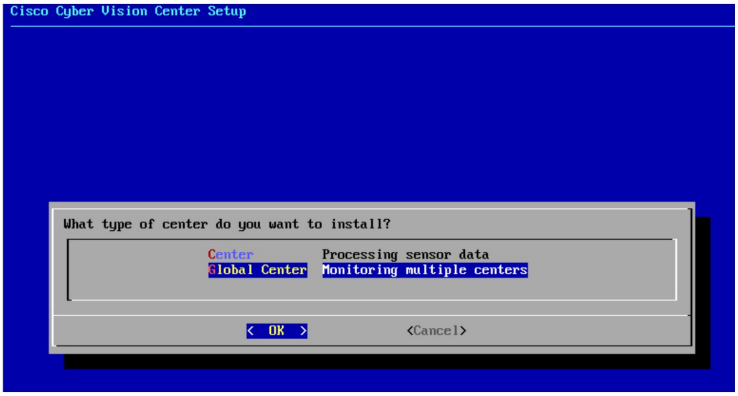
Type the id into the basic Center configuration UUID field.



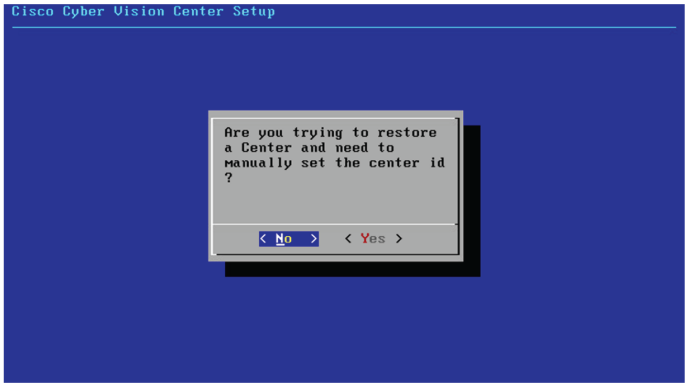
Click OK. You will be directed to the next step.

Global Center

If installing a Global Center, select the second option.



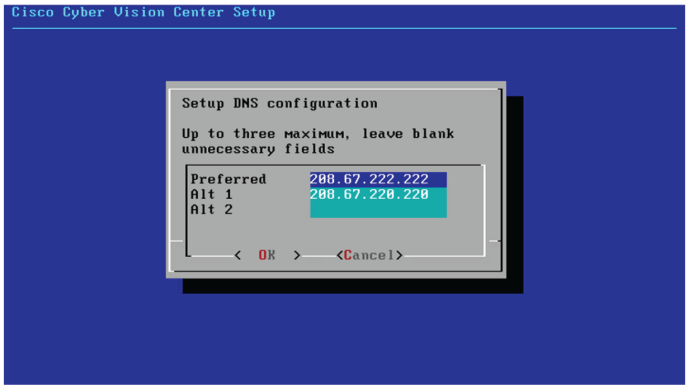
As this step does not apply to a Global Center, select No.



You will be directed to the next step.

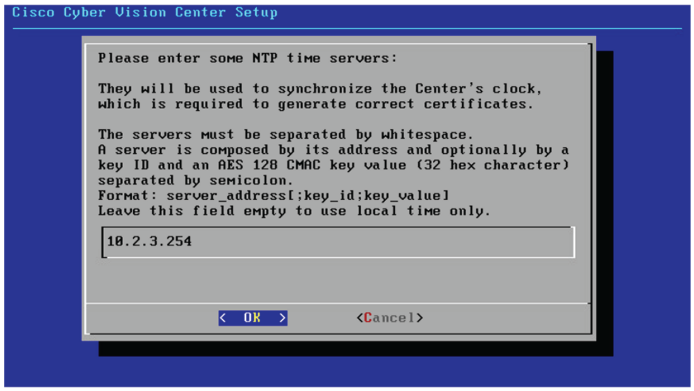
Configure the Center's DNS

Type a DNS server address and optional fallbacks.

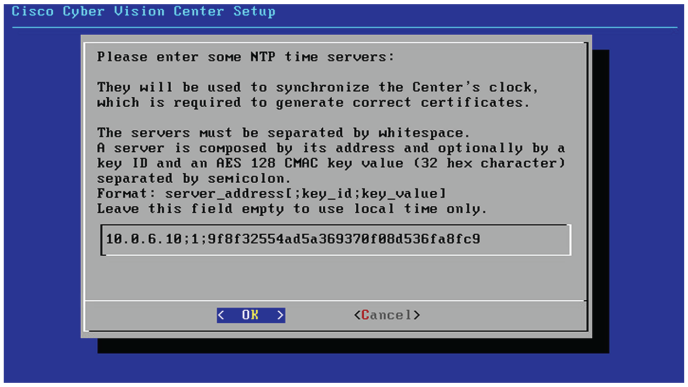


Synchronize the Center and the sensors to NTP servers

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.



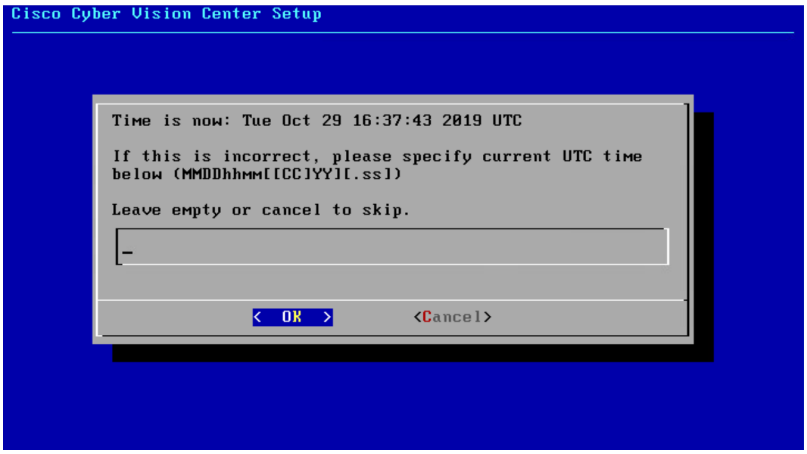
Optionally, add a key ID and an AES A28 CMAC key value separated by a semicolon with the corresponding NTP server.



The synchronization takes a few seconds.

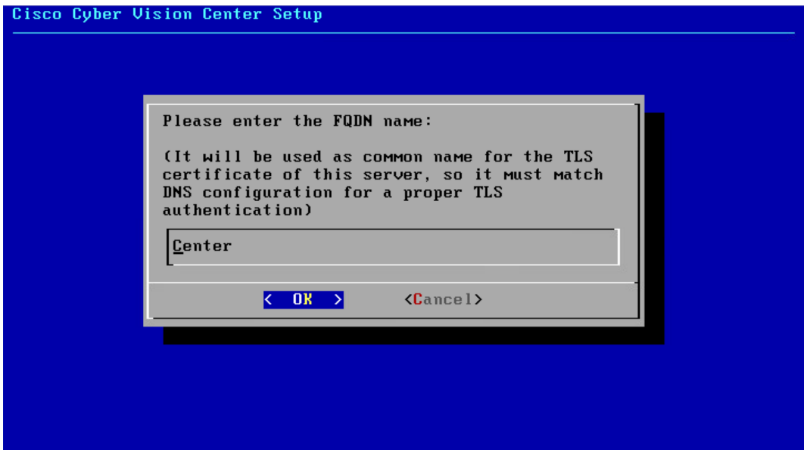
Check that the time is correct, or set the time manually.

Note The time is set in UTC standard.



Give the Center a name

Note This name will be used in the Center certificate.

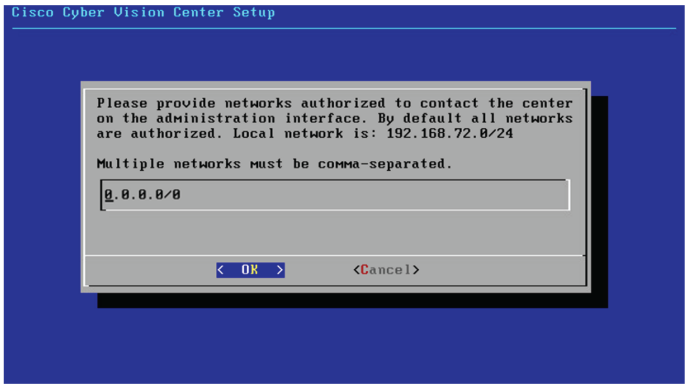


Enter the Center name provided by your administrator or type 'Default' which is a secure value.

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

Authorize networks

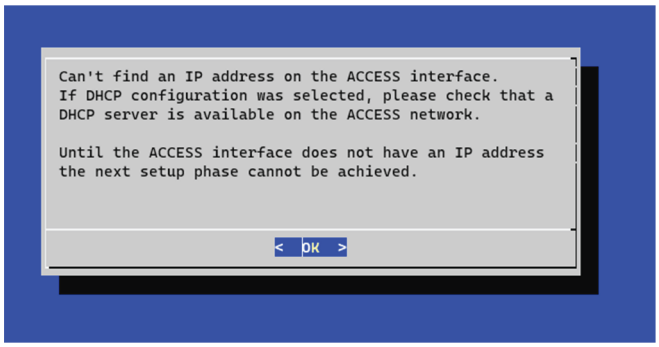
This step allows you to restrict IP addresses that can connect to the Administration interface. If no IP is entered, all networks are authorized by default.



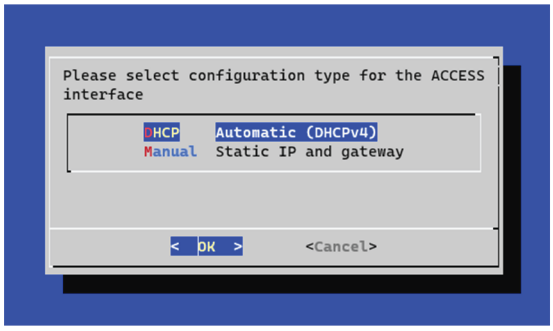
Set DHCP

Procedure

Step 1 If the following message appears, select OK.

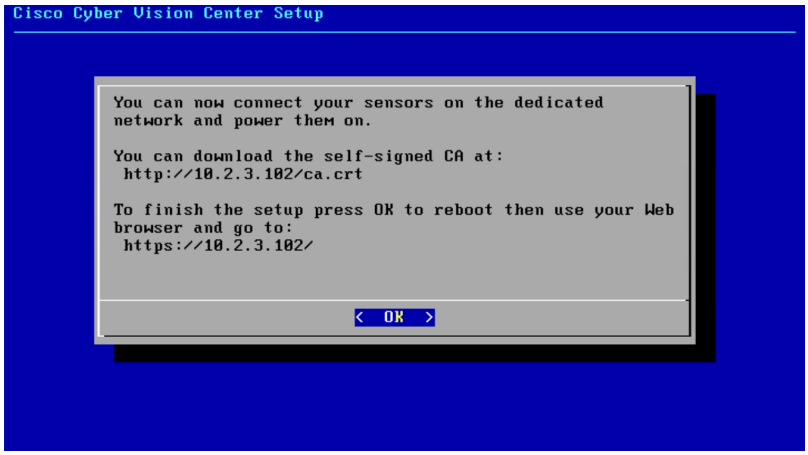


Step 2 Select DHCP.

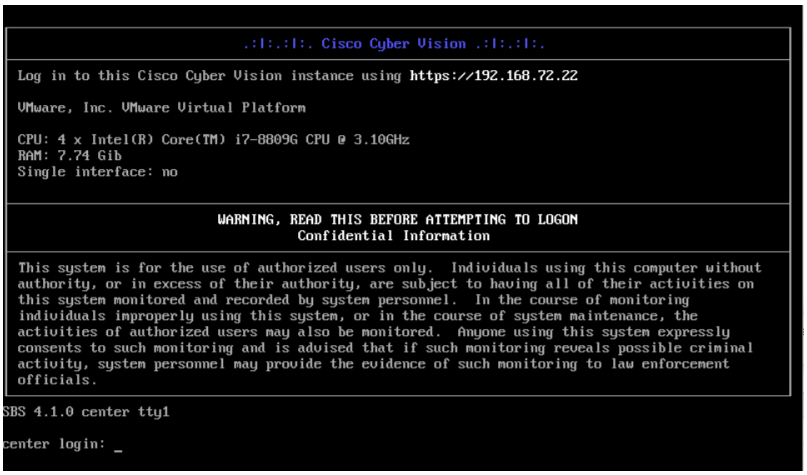


Complete the basic Center configuration

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.



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).