



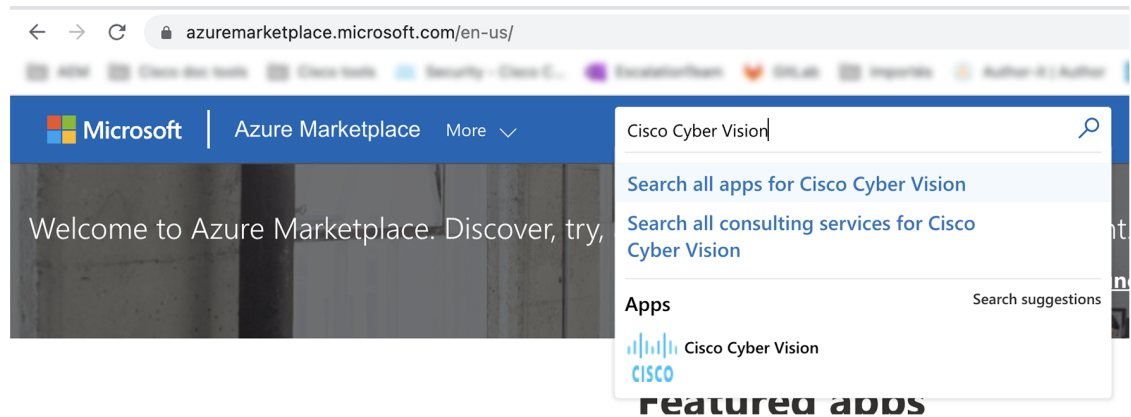
# Deploy the Cisco Cyber Vision Center

- [Access Azure portal, on page 1](#)
- [Basics, on page 3](#)
- [Virtual Machine settings, on page 4](#)
- [Cisco Cyber Vision settings, on page 7](#)
- [Review and create custom deployment, on page 10](#)
- [Basic Center configuration, on page 11](#)
- [Azure firewall settings, on page 23](#)

## Access Azure portal

### Procedure

- Step 1** Access Azure Marketplace at <https://azuremarketplace.microsoft.com/>.
- Step 2** Search for Cisco Cyber Vision.



- Step 3** Click **Get it now**.

Products > Cisco Cyber Vision

**Cisco Cyber Vision** [Save to my list](#)  
Cisco Systems, Inc.

[Overview](#) [Plans](#) [Ratings + reviews](#)

Cisco Cyber Vision provides continuous visibility into Industrial environments

[Get It Now](#)

**Pricing information**  
Cost of deployed template components

**Categories**  
Compute  
Internet of Things

**Support**  
Support  
Help

**Legal**  
License Agreement  
Privacy Policy

Cisco Cyber Vision is a cybersecurity solution specifically designed for organizations in power and water distribution, oil & gas, manufacturing and public transportation to ensure continuity, resilience and safety of their industrial operations. It provides asset owners with full visibility into their ICS networks, so they can ensure process integrity, build secure infrastructures, drive regulatory compliance and enforce security policies through seamless integration with the IT SOC and easy deployment within the industrial network. Cisco Cyber Vision leverages Cisco industrial network equipment to monitor industrial operations and feeds Cisco IT security platforms with OT context to build a unified IT/OT cybersecurity architecture.

To learn more about Cisco Cyber Vision, visit our website at [cisco.com/go/cybervision](https://cisco.com/go/cybervision)

**Microsoft Azure**  
Custom deployment  
Deploy from a custom template

Basic Virtual Machine Settings Cyber Vision Settings Review + create

Virtual machine size  8 vCPUs, 32 GB memory  
[Change size](#)

Data disk  250 GB

Data disk capacity  GB

Diagnostic storage account  [Create New](#)

Public IP Address for the VM  [Create new](#)

DNS Prefix for the public IP Address  .eastus.cloudapp.azure.com

Configure virtual networks

Virtual network

Subnet

The popup Create this app in Azure appears.

Create this app in Azure

**Cisco Cyber Vision**  
By Cisco Systems, Inc.

Software plan  
**Cisco Cyber Vision 4.1.0 BYOL**

Pricing: This solution template deploys software components and Azure infrastructure components. The price is the cost of those components.

Details: Cisco Cyber Vision provides continuous visibility into Industrial environments

This app requires some basic profile information. You have provided the information already so you're good to go! [Edit](#)

By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be handled in accordance with the provider's [terms and privacy statement](#).

[Continue](#)

**Step 4** Click **Continue**.

The Azure portal to create a Cisco Cyber Vision machine opens.

**Step 5** Click **Create**.

[Home](#) >

## Cisco Cyber Vision

Cisco Systems, Inc.



### Cisco Cyber Vision

[Add to Favorites](#)

Cisco Systems, Inc.

Plan

Cisco Cyber Vision 4.1.0 BYOL

[Create](#)[Overview](#) [Plans](#) [Usage Information + Support](#) [Reviews](#)

Cisco Cyber Vision is a cybersecurity solution specifically designed for organizations in power and water distribution, oil & gas, manufacturing and public transportation to ensure continuity, resilience and safety of their industrial operations. It provides asset owners with full visibility into their ICS networks, so they can ensure process integrity, build secure infrastructures, drive regulatory compliance and enforce security policies through seamless integration with the IT SOC and easy deployment within the industrial network. Cisco Cyber Vision leverages Cisco industrial network equipment to monitor industrial operations and feeds Cisco IT security platforms with OT context to build a unified IT/OT cybersecurity architecture.

To learn more about Cisco Cyber Vision, visit our website at [cisco.com/go/cybervision](https://cisco.com/go/cybervision)

# Basics

## Procedure

**Step 1** Create or select an existing resource group.

**Step 2** Select a region.

**Step 3** Type a virtual machine name.

**Note** Passwords must not include reserved words or unsupported characters.

Password must comply with three of the following conditions: 1 lower case character, 1 upper case character, 1 number, and 1 special character that is not '\ ' or '- '.

The value must be 12 to 123 characters long.

**Step 4** Type a password and confirm it.

**Step 5** You have the option of entering an SSH key.

**Step 6** Click **Next: Virtual Machine settings**.

☰
Search resources, services, and docs (G+)

Home > Cisco Cyber Vision >

## Create Cisco Cyber Vision ...

[Basics](#)  
 [Virtual Machine Settings](#)  
 [Cyber Vision Settings](#)  
 [Review + create](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Region \* ⓘ

Virtual Machine name \* ⓘ  ✓

Password of cv-admin user \* ⓘ  ✓

Confirm password \*  ✓

SSH public key (RSA) ⓘ

Review + create
< Previous
Next : Virtual Machine Settings >

# Virtual Machine settings

## Procedure

**Step 1** You can change the VM size clicking **change size**.

[Basics](#)  
 [Virtual Machine Settings](#)  
 [Cyber Vision Settings](#)  
 [Review + create](#)

Virtual machine size \* ⓘ

**1x Standard D8s v4**

8 vcpus, 32 GB memory

[Change size](#)

The following screen appears.

## Select a VM size

Display cost : **Monthly**vCPUs : **All**RAM (GiB) : **All**

Add filter

Showing 6  
VM sizes.Subscription:  
CerberusRegion:  
East USCurrent size:  
Standard\_D8s\_v4[Learn more about  
VM sizes](#)

Group by series

VM Size	Type	vCPUs	RAM (GiB)	Data disks	Max IOPS
<b>D-Series v4</b> <span style="float: right;">The 4th generation D family sizes for your general purpose needs</span>					
D4s_v4	General purpose	4	16	8	6400
D8s_v4	General purpose	8	32	16	12800
D16s_v4	General purpose	16	64	32	25600
D32s_v4	General purpose	32	128	32	51200
D48s_v4	General purpose	48	192	32	76800
D64s_v4	General purpose	64	256	32	80000

**Select**

Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. If you purchased Azure services through a reseller, contact your reseller for full pricing details.

The recommended sizes are:

- For 10,000 components:
  - D8s\_v4 - 8 CPU / 32GB RAM minimum
- For more than 10,000 components:
  - D16s\_v4 - 16 CPU / 64GB RAM minimum

Basics **Virtual Machine Settings** Cyber Vision Settings Review + create

Virtual machine size \* ⓘ **1x Standard D64s v4**  
64 vcpus, 256 GB memory  
[Change size](#)

Data disk \* ⓘ Create a new data disk

Data disk capacity ⓘ  1000 GB

Diagnostic storage account \* ⓘ (new) JMAVM9ee34d44b9  
[Create New](#)

Public IP Address for the VM ⓘ (new) JMA-VM-ip  
[Create new](#)

DNS Prefix for the public IP Address \* ⓘ jma-vm-d21b8f486e ✓  
.eastus.cloudapp.azure.com

Configure virtual networks

Virtual network \* ⓘ (new) VirtualNetwork  
[Create new](#)

Subnet \* ⓘ (new) Subnet-1 (10.0.0.0/24)

[Review + create](#) < Previous Next : Cyber Vision Settings >

A disk is required to store the data of the Center. The recommended size for a Center is 250GB and 1TB minimum for a Global Center. Choose one of the options below:

- Select **Create a new data disk** and set the /data file storage using the data disk capacity slider.
- Select **Attach an existing data disk** if it has been previously created in Azure resources and select it in **Select data disk** dropdown menu.

**Step 2** Create a diagnostic storage account for the console serie to be accessible on the Azure VM.

**Step 3** Set the resource for the public IP. If the public IP was already created you can select it here. For automatic creation, leave it has "(new)". You can set the IP address as static clicking **Create New**.

### Create public IP address ×

Name \* JMA-VM-IP ✓

SKU ⓘ  
 Basic  Standard

Assignment  
 Dynamic  Static

**Step 4** An FQDN is automatically created. You can change it.

**Step 5** A VNet is automatically created.

- Step 6** A subnet is created by default. You can select another resource.
- Step 7** Click **Next: Cisco Cyber Vision settings**.
- 

## Cisco Cyber Vision settings

### Configure right now

Configure right now is to configure everything that is available from the setup Center directly from Azure portal like the keyboard layout on the console serie, the Center type (Center and Global Center) and the FQDN.

After creating your VM wait a few moments (usually 10 minutes is enough) for autoprovision and access Cisco Cyber Vision through the domain name.

#### Procedure

---

- Step 1** Select **Configure right now**.
- Step 2** Select **Center** or **Global Center**.
- Step 3** Set a FQDN.
- Step 4** Select a Webapp TLS certificate option.

This will allow you to use a trusted certificate accessing the IP address from a browser to reach Cisco Cyber Vision session directly. You can generate an autosigned certificate with the FQDN or use a custom certificate adding a P12 and its password.

- Step 5** If needed, set DNS servers.
- Step 6** Click **Next: Review + Create**.

Basics Virtual Machine Settings **Cyber Vision Settings** Review + create

Configure Cyber Vision \* ⓘ

Cyber Vision configuration

Center type \* ⓘ

FQDN name \* ⓘ

Webapp TLS certificate \*  Generate an autosigned certificate with the FQDN  
 Use a custom certificate

DNS servers

**i** If no servers are provided, the default provider is OpenDNS: 208.67.222.222, 208.67.220.220

NTP servers

**Review + create** < Previous Next : Review + create >

### What to do next

Proceed with [Review and create custom deployment, on page 10](#).

## Configure using a JSON config

You can configure the Cisco Cyber Vision Center automatically through a json file. The configuration will be run at the machine boot. The format is the same as the syntax shown in the annex: [Annex – Setup Center json file](#)

### Procedure

- Step 1** Select **Configure using a JSON config**.
- Step 2** Fill in the Json config blog using the annex syntax.



Basics Virtual Machine Settings **Cyber Vision Settings** Review + create

Configure Cyber Vision \* ⓘ

Cyber Vision configuration

Json config blob \* ⓘ

---

**Step 3** Click **Next: Review + Create**.

### What to do next

Proceed with [Review and create custom deployment, on page 10](#).

## Serial console connection to Azure virtual machine

You can choose not to configure Cisco Cyber Vision for now and use the serial console wizard available in Azure portal instead.

### Procedure

**Step 1** Select **Don't configure and use serial console wizard**.

Basics Virtual Machine Settings **Cyber Vision Settings** Review + create

Configure Cyber Vision \* ⓘ

---

**Step 2** Click **Next: Review + create**.

# Review and create custom deployment

Data entered and configuration is being checked. The mention "Validation Passed" should be displayed.

During this step, you will find the terms and configurations summary of the custom deployment.

Validation Passed

Basics Virtual Machine Settings Cyber Vision Settings **Review + create**

Summary

Customized template  
11 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

Create < Previous Next

1. Click **Create** to create the custom deployment.

The deployment follow up is displayed showing the resources creation: virtual network, security group, public ip, storage account for the serial console, VM, etc. This step can take a few moments.

Deployment completed:

Home >

Microsoft.Template-20220201152928 | Overview ✕ ...

Deployment

Search (Ctrl+/) << Delete Cancel Redeploy Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

**✓ Your deployment is complete**

Deployment name: Microsoft.Template-20220201152928      Start time: 2/1/2022, 3:29:32 PM  
 Subscription: Cerberus      Correlation ID: c73f8b6d-935e-4576-b881-5dcff6  
 Resource group: jumaff

Deployment details (Download)

Resource	Type	Status
✓ jma-vm	Microsoft.Compute/virtualMachines	OK
✓ jmavm7babbe46cb	Microsoft.Storage/storageAccounts	OK
✓ jma-vm-nic	Microsoft.Network/networkInterfaces	Created
✓ jma-vm-ip	Microsoft.Network/publicIPAddresses	OK
✓ jmavm7babbe46cb	Microsoft.Storage/storageAccounts	OK
✓ jma-vm-ip	Microsoft.Network/publicIPAddresses	OK
✓ VirtualNetwork	Microsoft.Network/virtualNetworks	OK
✓ nsg-cyber-vision	Microsoft.Network/networkSecurityGroups	OK
✓ useridentity/khnz3neba4aeg	Microsoft.ManagedIdentity/userAssignedIdentities	Created
✓ pid-00000000-0000-0000-0000-000000000000	Microsoft.Resources/deployments	OK

Next steps

[Go to resource group](#)

If you have used the serial console to configure the Azure virtual machine, proceed with the [Basic Center configuration, on page 11](#).

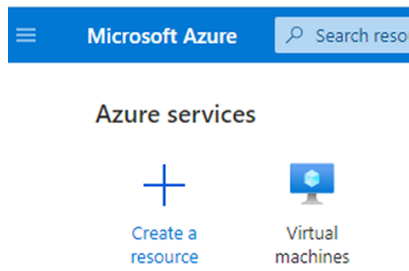
## Basic Center configuration

### Access the Basic Center Configuration

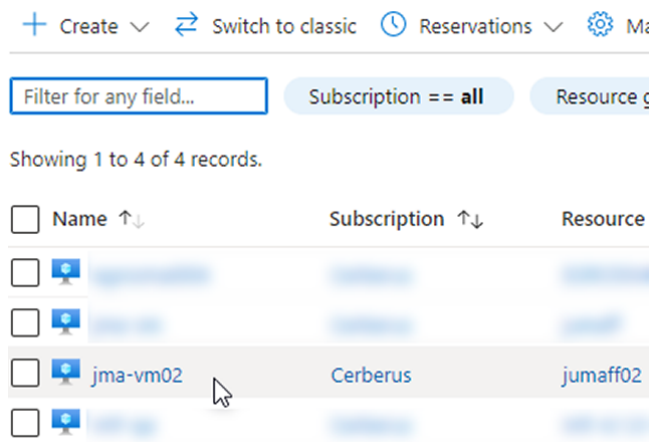
To access the Basic Center Configuration and setup the Cisco Cyber Vision Center or Global Center:

#### Procedure

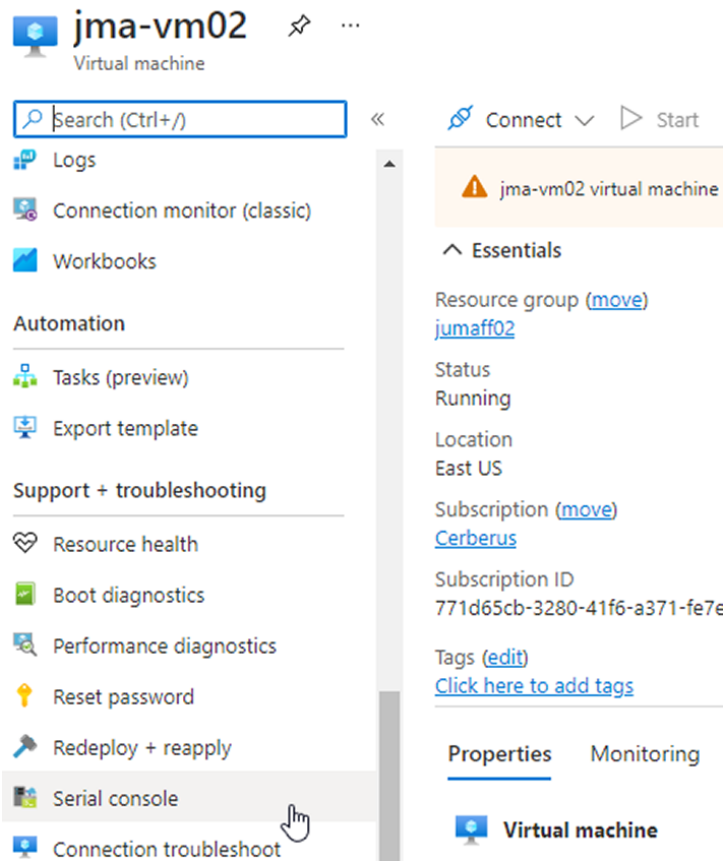
- Step 1** In the Azure portal, navigate to Home > Virtual Machines.



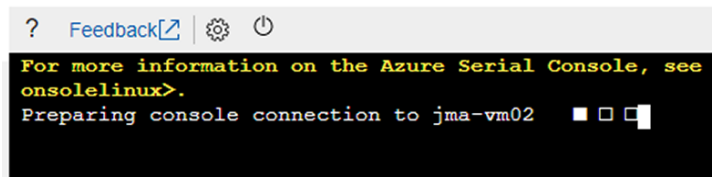
**Step 2** Click the VM to configure via the serial console.



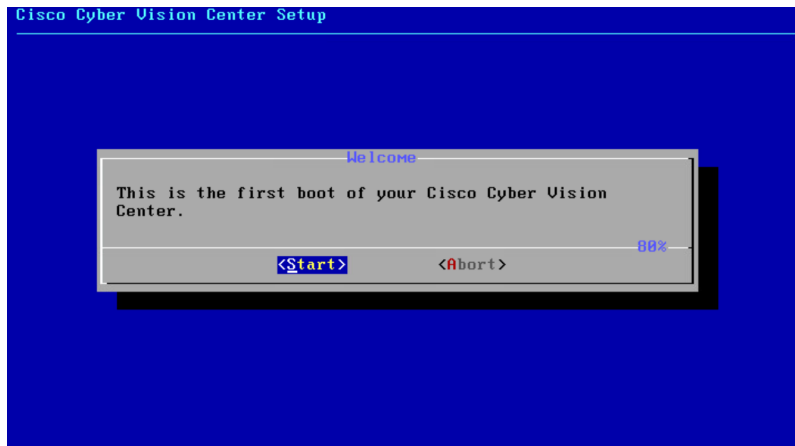
**Step 3** Click **Serial console** in the left dropdown menu.



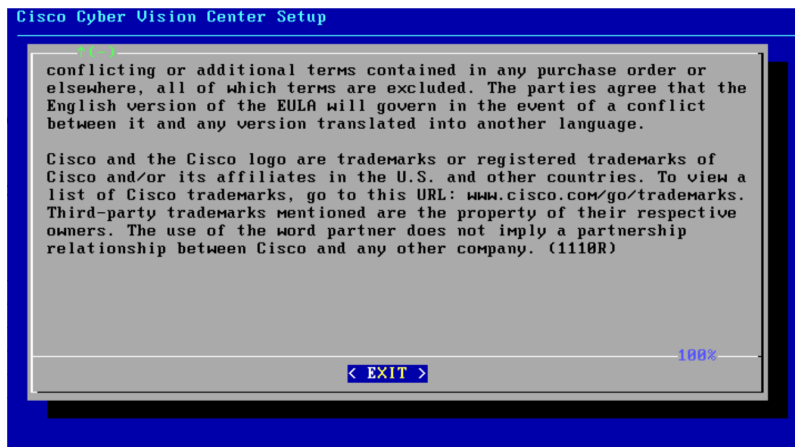
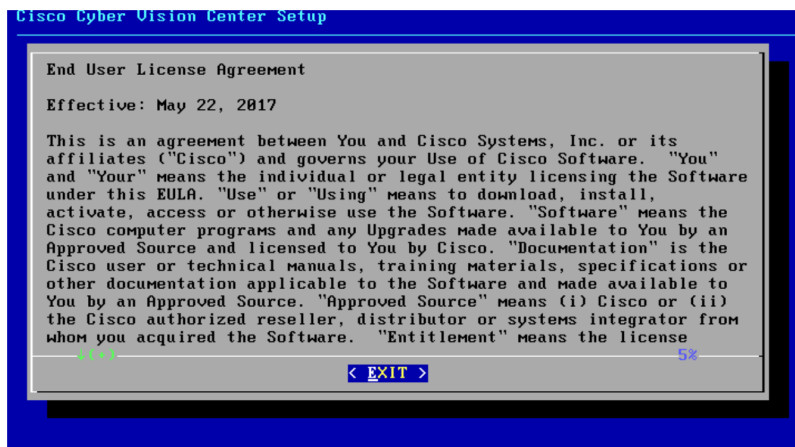
The serial console is displayed and the connection to the VM is establishing.

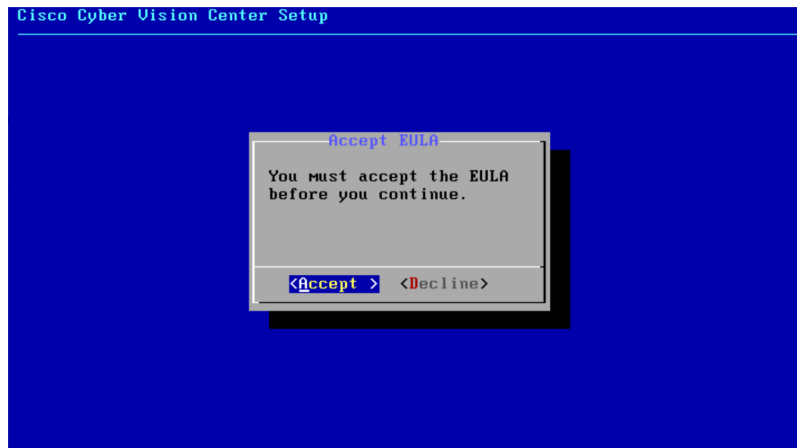


**Step 4** The Center wizard is displayed on your screen as you power on the Center. Enter Start to start configuring the Center.



## Accept the End User License Agreement



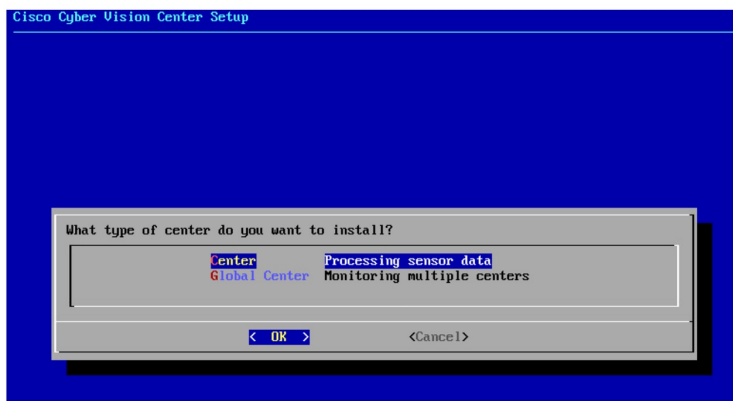


## Select the Center type

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

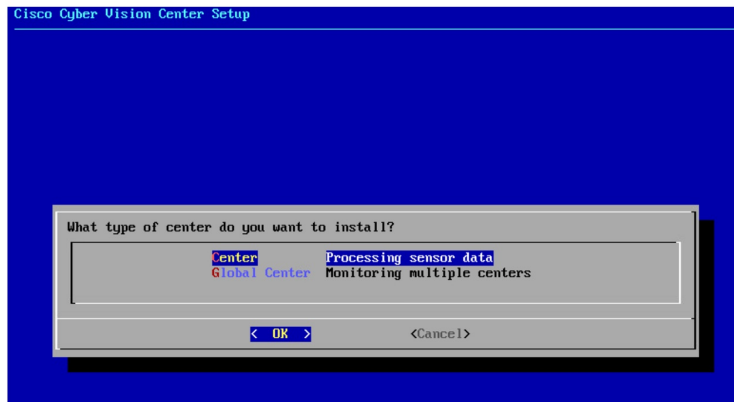
- A **Center** receives metadata from sensors and store them into an internal database (Postgresql). It can be standalone or synchronized with a Global Center. A Center with sync is similar to a standalone Center from a functionality point of view, except for the link to a Global Center. You must install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



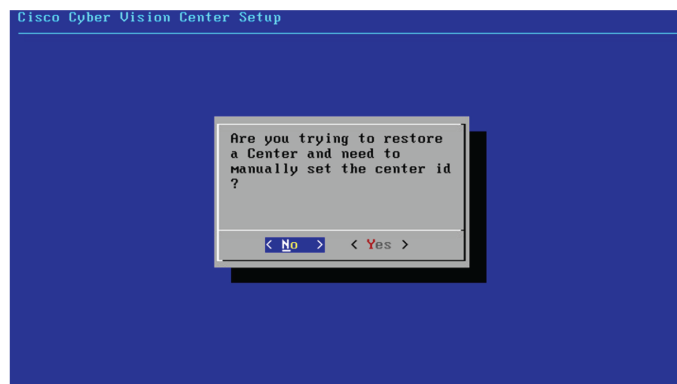
## Center

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.

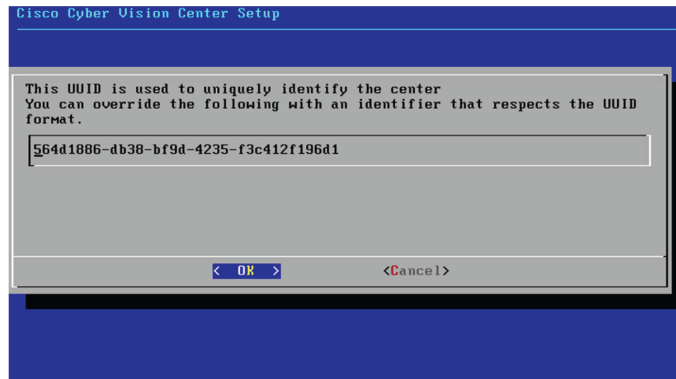


Use the following command from the Global Center's CLI to get a list of all Center's id:

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



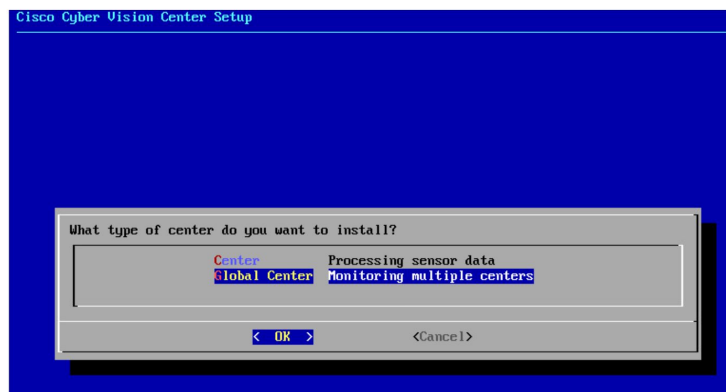
Type the id into the basic Center configuration UUID field.



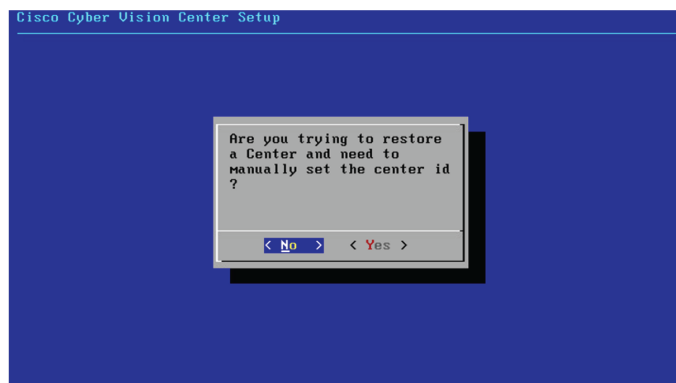
Click OK. You will be directed to the next step.

## Global Center

If installing a Global Center, select the second option.



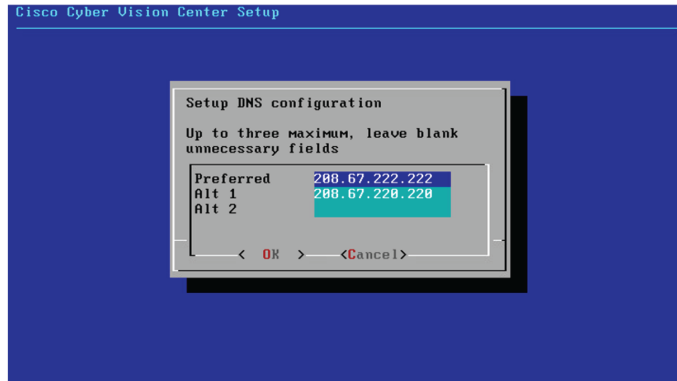
As this step does not apply to a Global Center, select No.



You will be directed to the next step.

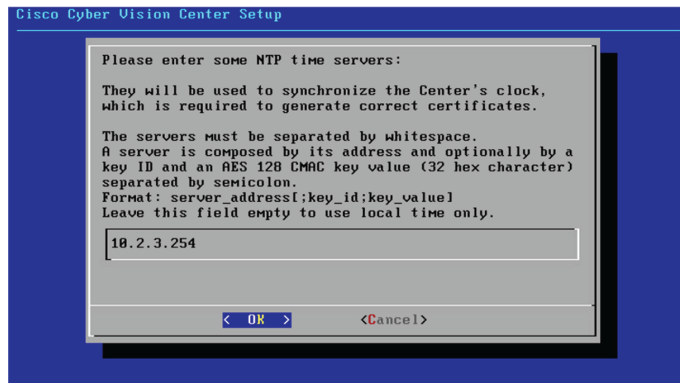
## Configure the Center's DNS

Type a DNS server address and optional fallbacks.

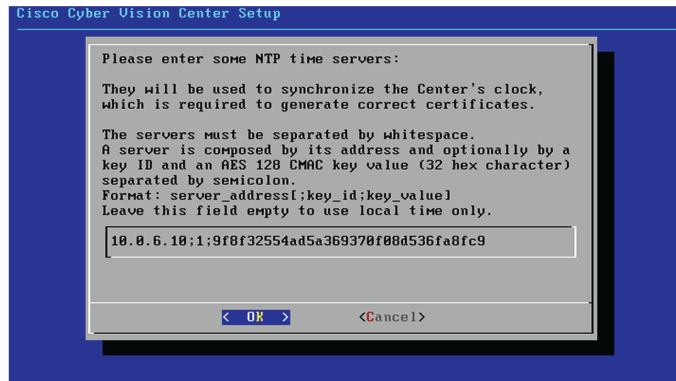


## Synchronize the Center and the sensors to NTP servers

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.

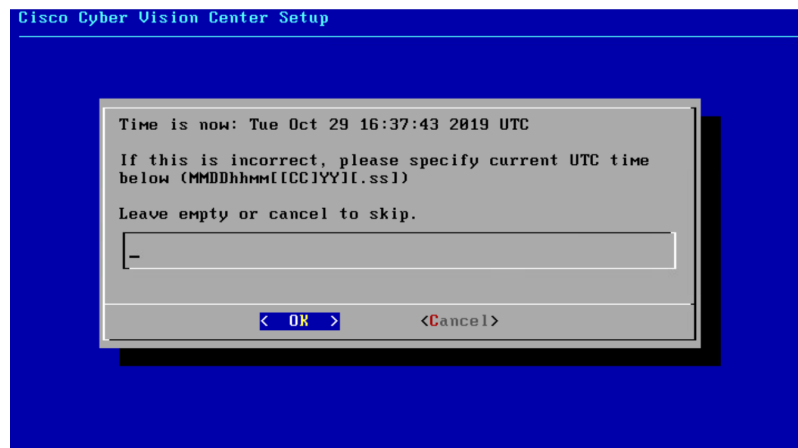
Check that the time is correct, or set the time manually.



---

**Note** The time is set in UTC standard.

---



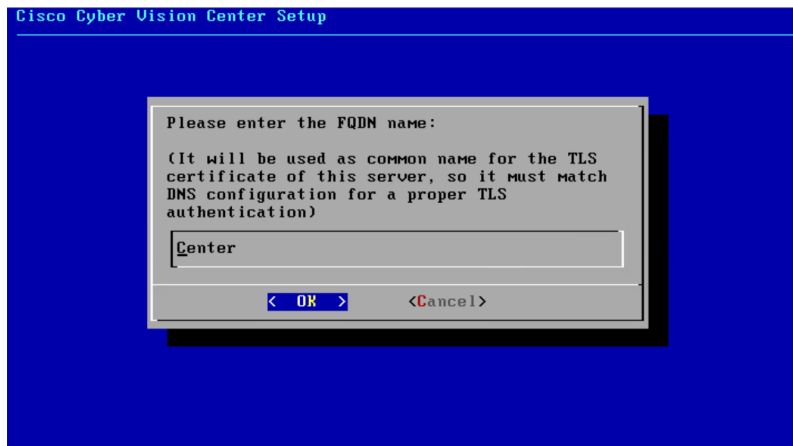
## Give the Center a name



---

**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.

## Configure the sensors' password

Not applicable to a Global Center. Instead, you'll be directed to [Authorize networks](#).

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

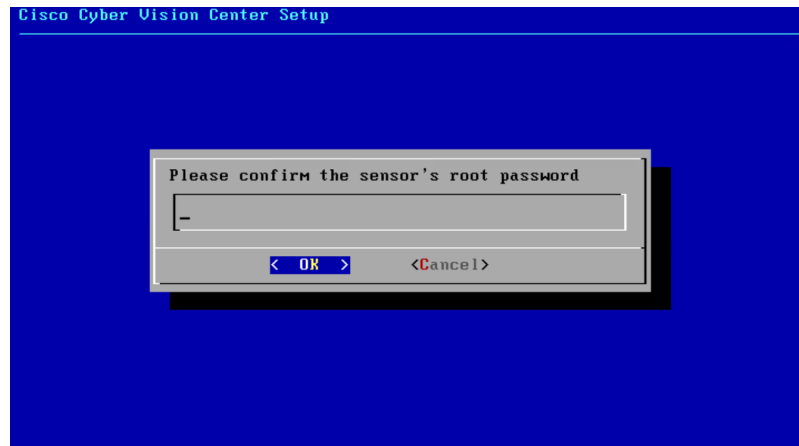
The sensors' root password must be set for security reasons.

This password must be different than the one used for the Center, otherwise you will get an error message.



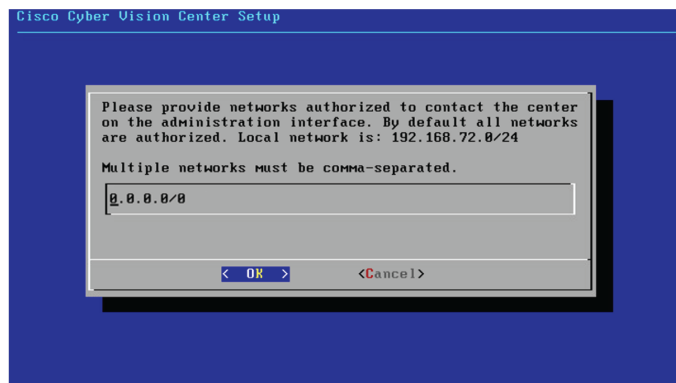
This password will be assigned once you will have enrolled the sensors on the Center. You will need this password for troubleshooting, diagnostics, and updates.

Confirm the password.



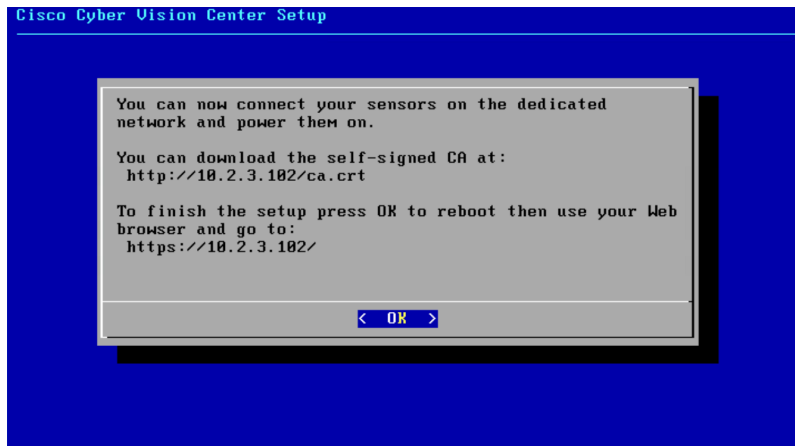
## Authorize networks

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.

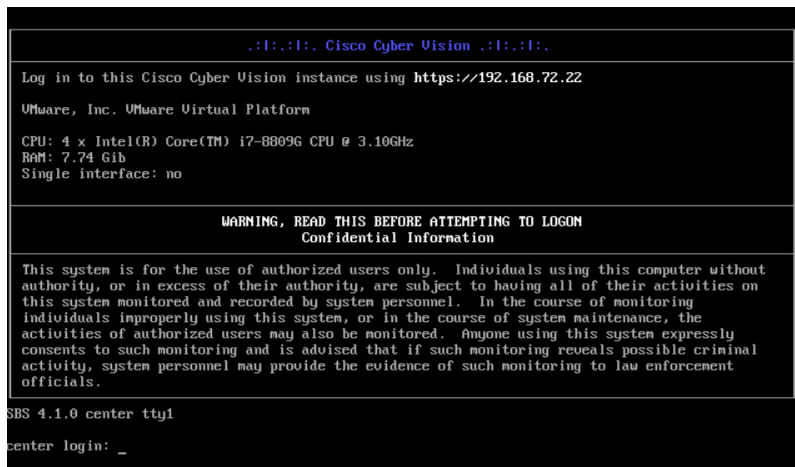


## Complete the basic Center configuration

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 console 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).

# Azure firewall settings

## Communication ports list

Herebelow are the rules that provide access from users or other resources to the Global Center or the Center and the 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 to Center communication:

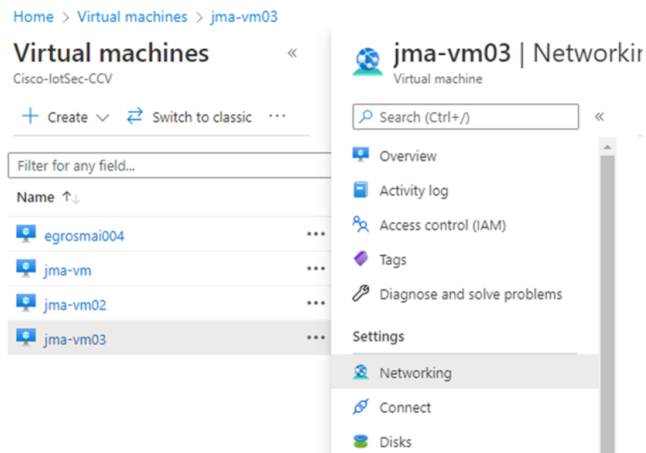
Protocol	Port
AMPQ	TCP/5671
Syslog	UDP/10514

## Configure communication ports

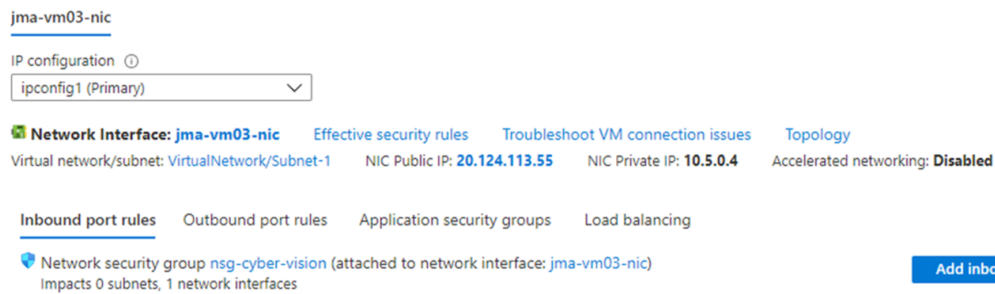
To configure a communication port:

### Procedure

- 
- Step 1** In the Home page of the Azure portal, access the VM.
  - Step 2** Click Networking in the Settings section.



**Step 3** Click the **Add inbound port rule** button.



**Step 4** Fill in the settings according to the ports listed in [Communication ports list, on page 23](#).

In our example, we're adding the AMPQ communication port for Global Center <--> Center communication.

Set Service as **Custom** if the service is not available in the list.

If the protocol to add is UDP/TCP, set protocol as **Any**.



**Add inbound security rule**
✕

nsg-cyber-vision

Source  ⓘ

Source port ranges \*  ⓘ

Destination  ⓘ

Service  ⓘ

Destination port ranges \*  ⓘ

Protocol  
 Any  
 TCP  
 UDP  
 ICMP

Action  
 Allow  
 Deny

Priority \*  ⓘ

Name \*  ⓘ

Description

**Step 5** Click **Add**.

The added port appears in the Inbound port rules list.

Priority	Name	Port	Protocol	Source	Destination	Action
1000	AllowSSH	22	TCP	Any	Any	Allow ...
1010	AllowHTTP	80	TCP	Any	Any	Allow ...
1020	AllowHTTPS	443	TCP	Any	Any	Allow ...
1030	AMPQ	5671	TCP	Any	Any	Allow ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow ...
65001	AllowAzureLoadBala...	Any	Any	AzureLoadBalancer	Any	Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	Deny ...

**Step 6** Repeat the previous steps to add all the communication ports required.

The final configuration for a Global Center:

## Configure communication ports

Priority	Name	Port	Protocol	Source	Destination	Action
1000	⚠ AllowSSH	22	TCP	Any	Any	✔ Allow
1010	AllowHTTP	80	TCP	Any	Any	✔ Allow
1020	AllowHTTPS	443	TCP	Any	Any	✔ Allow
1030	AMPQ	5671	TCP	Any	Any	✔ Allow
1040	NTP	123	UDP	Any	Any	✔ Allow
1060	Syslog	514	Any	Any	Any	✔ Allow
1070	SSH	22	TCP	Any	Any	✔ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowAzureLoadBalance...	Any	Any	AzureLoadBalancer	Any	✔ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✘ Deny