Deploy the Cisco Cyber Vision Center

Access Azure portal

Procedure

Step 1   Access Azure Marketplace at https://azuremarketplace.microsoft.com/.

Step 2   Search for Cisco Cyber Vision.
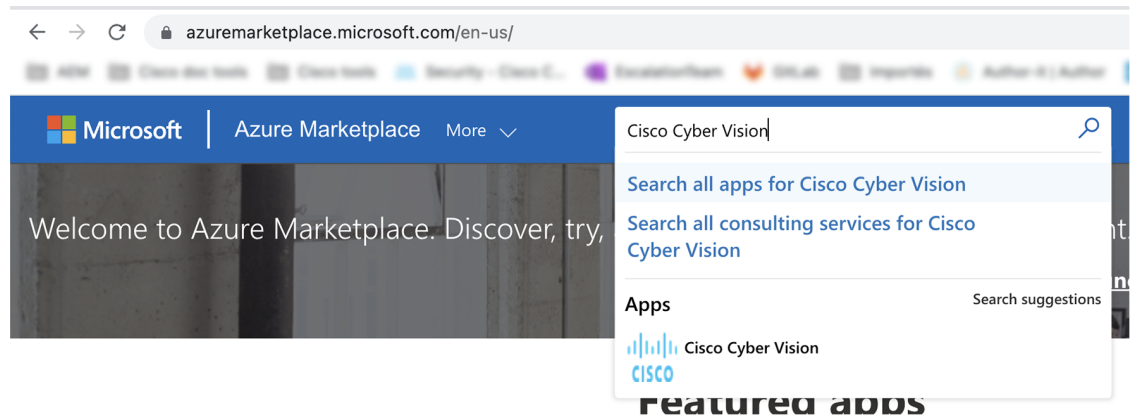
Step 3   Click **Get it now**.

The popup Create this app in Azure appears.

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

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**.

Virtual Machine settings

Procedure

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

The following screen appears.

Select a VM size

VM Size ↑↓	Type ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS
⌄ D-Series v4			The 4th generation D family sizes for your general purpose needs		
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

Showing 6 VM sizes. | Subscription: Cerberus | Region: East US | Current size: Standard_D8s_v4 | Learn more about VM sizes | Group by series

Search by VM size... | Display cost : **Monthly** | vCPUs : **All** | RAM (GiB) : **All** | Add filter

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:

a) Select **Create a new data disk** and set the /data file storage using the data disk capacity slider.
b) 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 * ⓘ

Configure right now ⌄

Cyber Vision configuration

Center type * ⓘ

Global Center ⌄

FQDN name * ⓘ

Center

Webapp TLS certificate *

◉ Generate an autosigned certificate with the FQDN

○ Use a custom certificate

DNS servers

IP address of the #1 DNS server

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

NTP servers

IP address / name of the #1 NTP server

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 *   ⓘ   Configure using a JSON config   ⌄

Cyber Vision configuration

Json config blob *   ⓘ

[Review + create]   [< Previous]   [Next : Review + create >]

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

What to do next

Proceed with .

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 user serial console wizard**.

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

Configure Cyber Vision *   ⓘ   Don't configure and use serial console wizard   ⌄

[Review + create]   [< Previous]   [Next : Review + create >]

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.

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:

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.
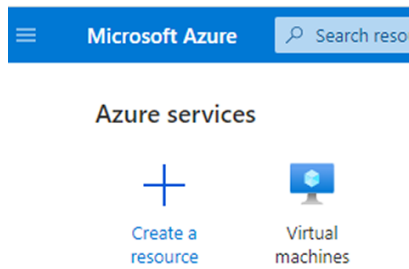
Step 2   Click the VM to configure via the serial console.
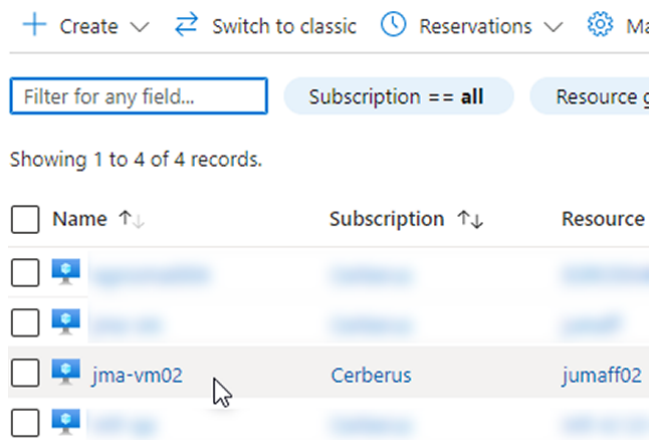
Step 3   Click **Serial console** in the left dropdown menu.
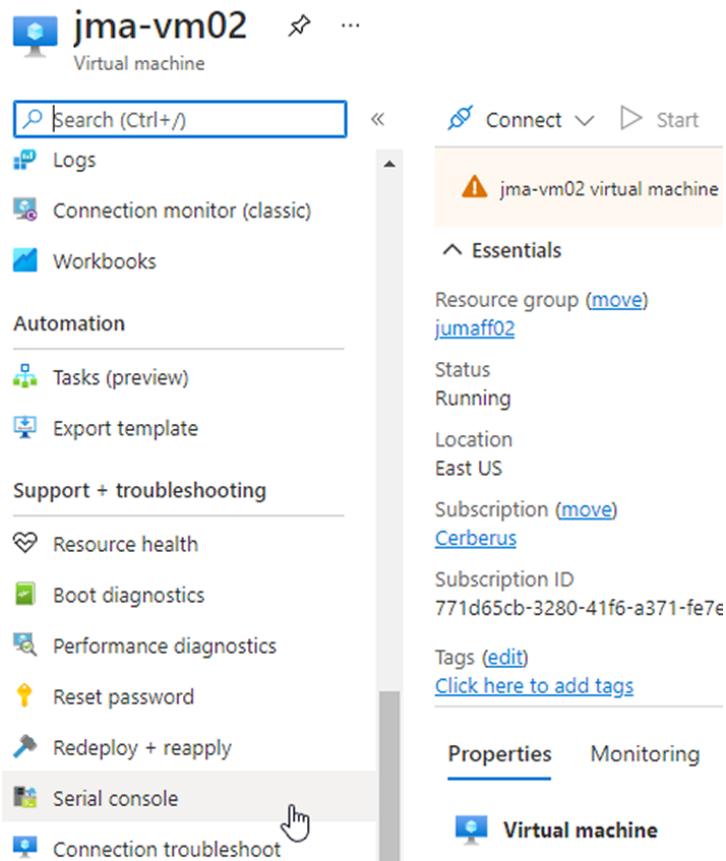
The serial console is displayed and the connection to the VM is establishing.
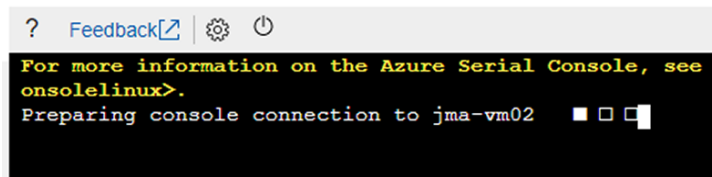
Step 4   The Center wizard is displayed on your screen as you power on the Center. Enter Start to start configuring the Center.

```
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 >                               │
  └─────────────────────────────────────────────────────────────┘
```
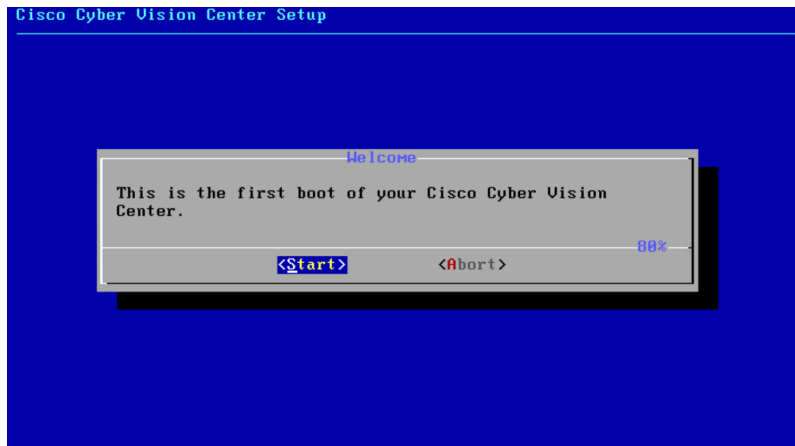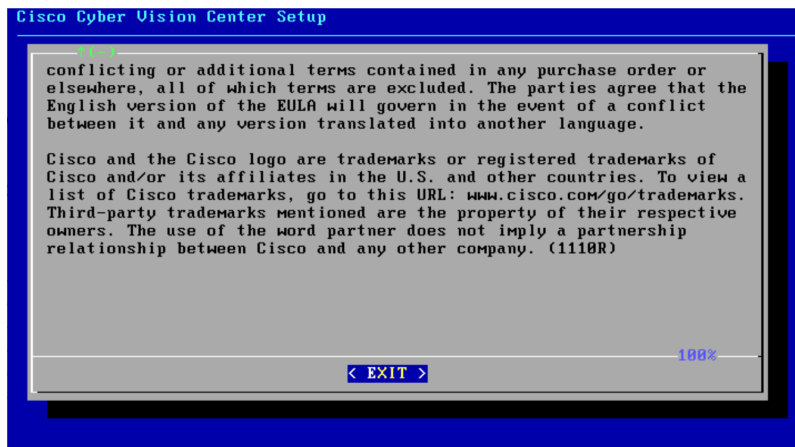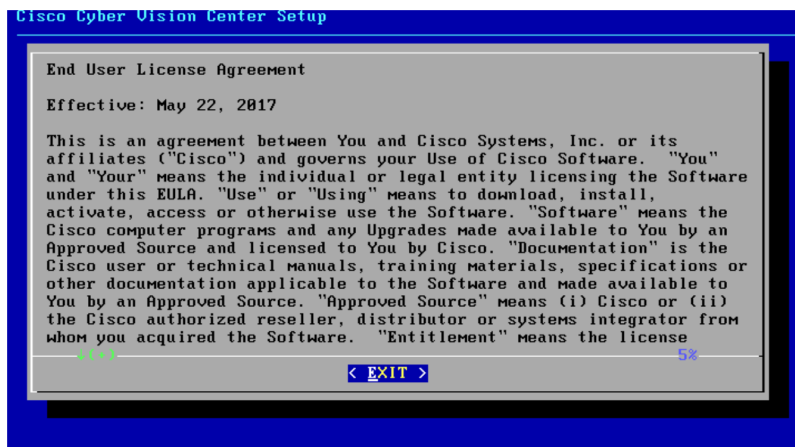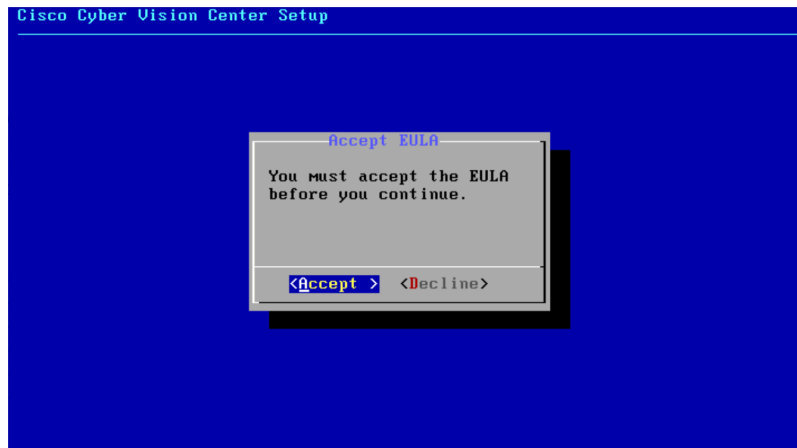
```
Cisco Cyber Vision Center Setup

  ┌─────────────────────────────────────────────────────────────┐
  │ 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 >                               │
  └─────────────────────────────────────────────────────────────┘
```
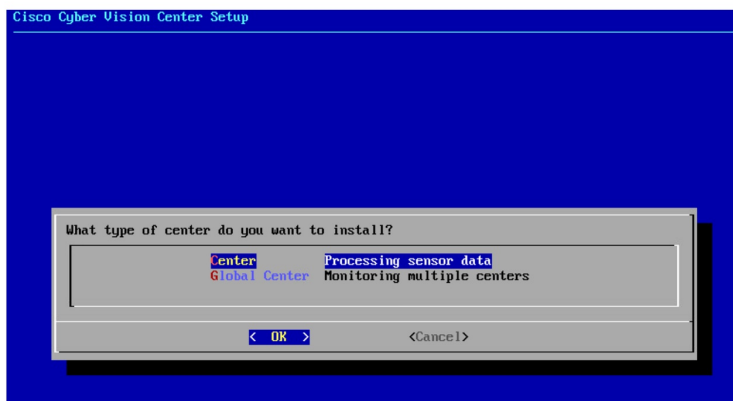
Select the Center type

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 push events to it.

- A **Global Center** introduces a centralized architecture which collects all industrial insights and events from Centers with Global Center 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.
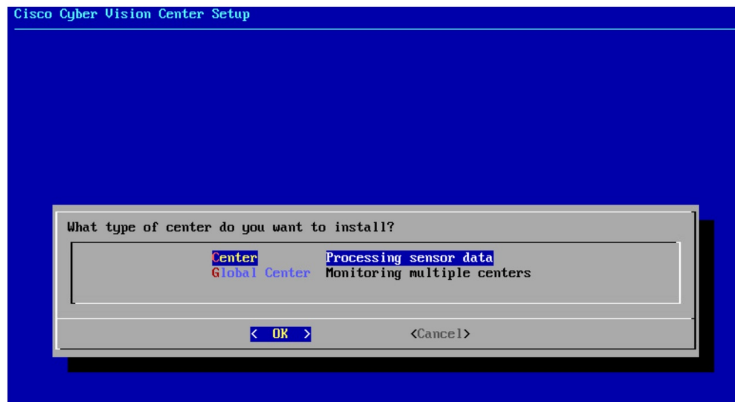
Then you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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.
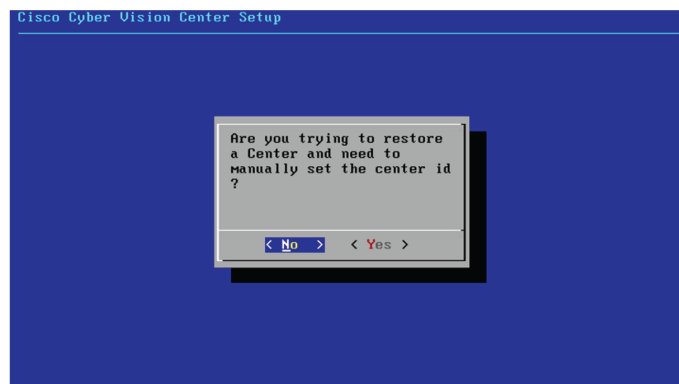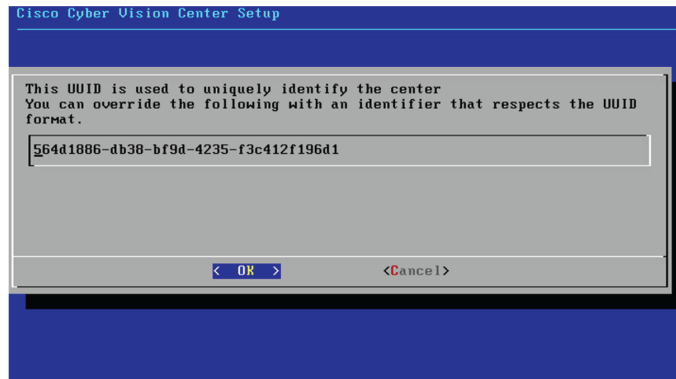

If you're reinstalling the Center and want to restore it, select Yes.
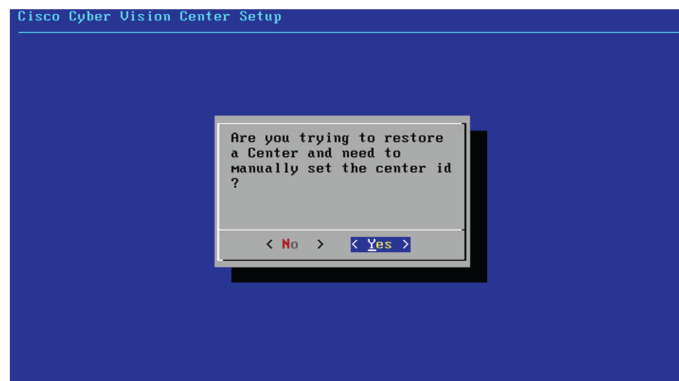
Use the following command from the Global Center's CLI to get a list of all Center's id:
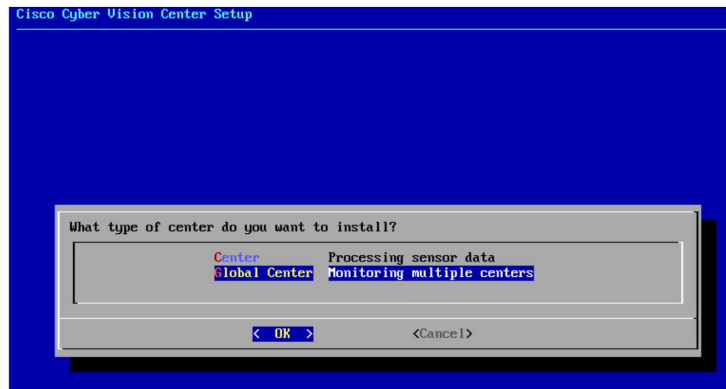
```
sbs-db exec "select name, id from center"
```

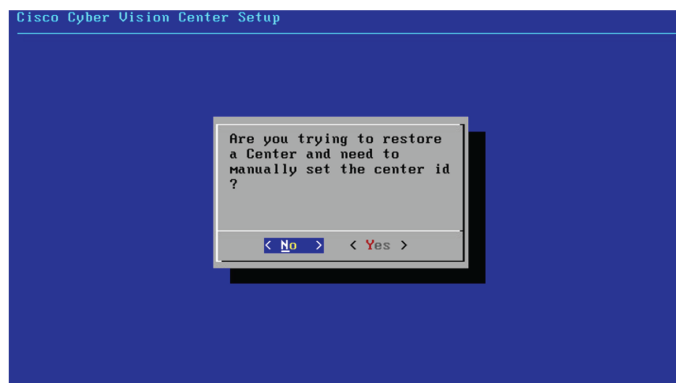Type the id into the basic Center configuration UUID field.

Click OK. You will be direct 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.

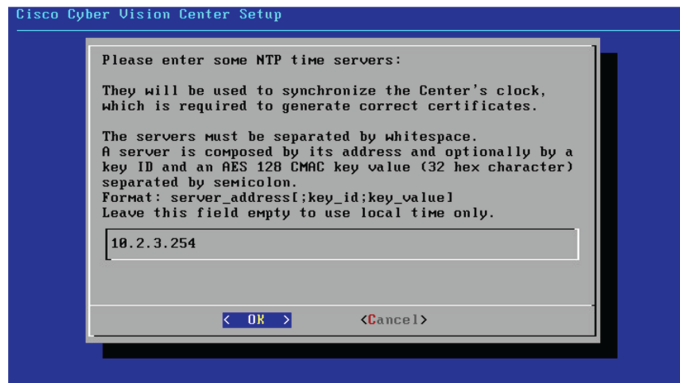You will be directed to the next step.

Configure the Center's DNS

Type a DNS server address and optional fallbacks.

```
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.
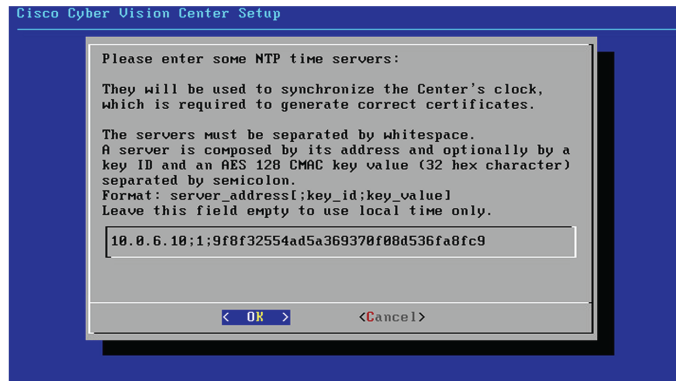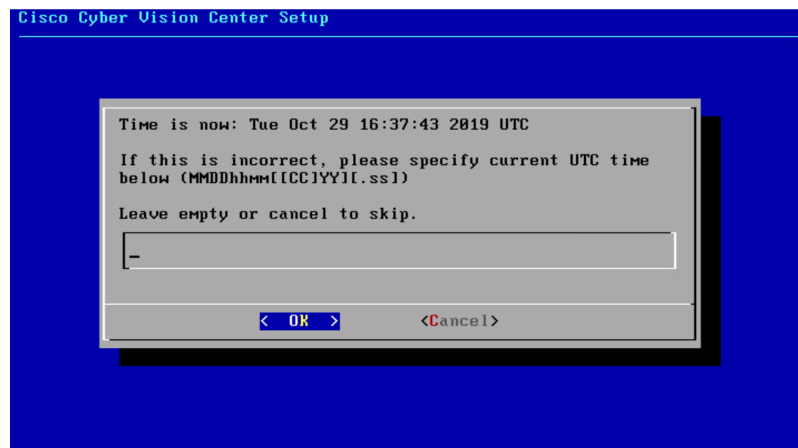
The synchronization takes a few seconds.

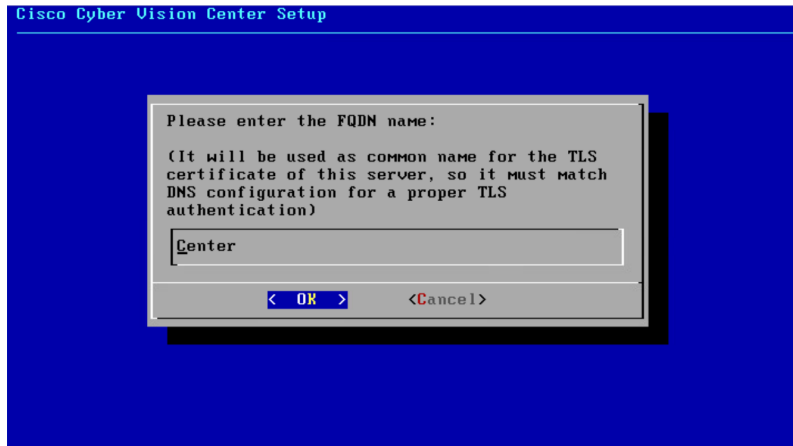Check that the time is correct, or set the time manually.

Note   The time is set in the UTC standard.

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

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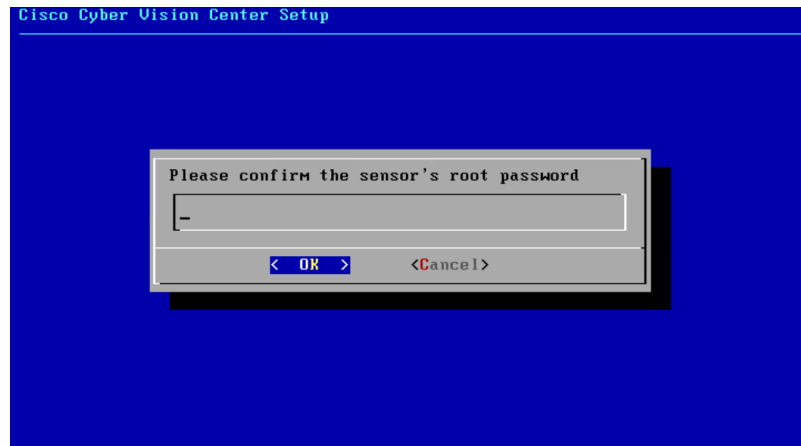
Although, if you're installing a Center, proceed as below.

The sensors' root password must be set for security reasons.
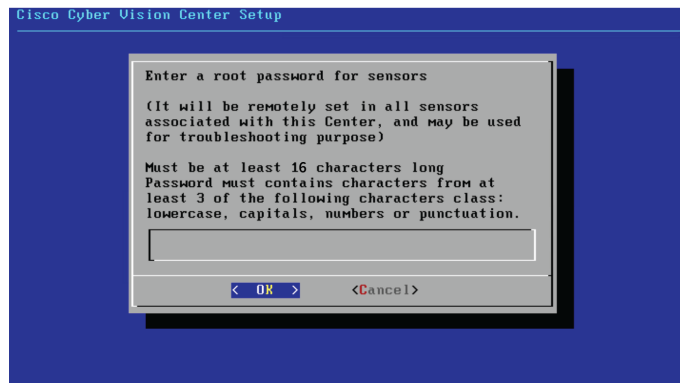
This password will be assigned once you will have enrolled the sensors on the Center. You will need this password for troubleshooting, diagnostics, and updates.

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.
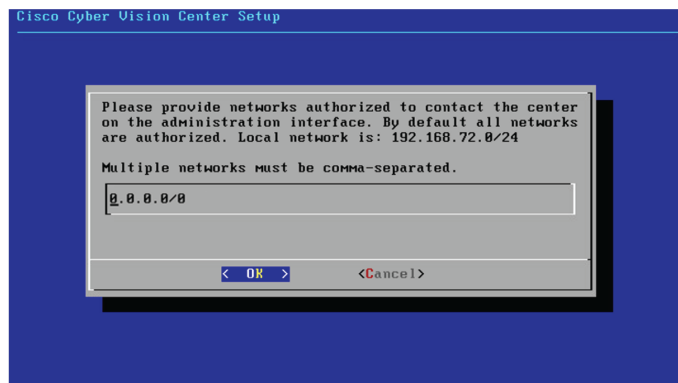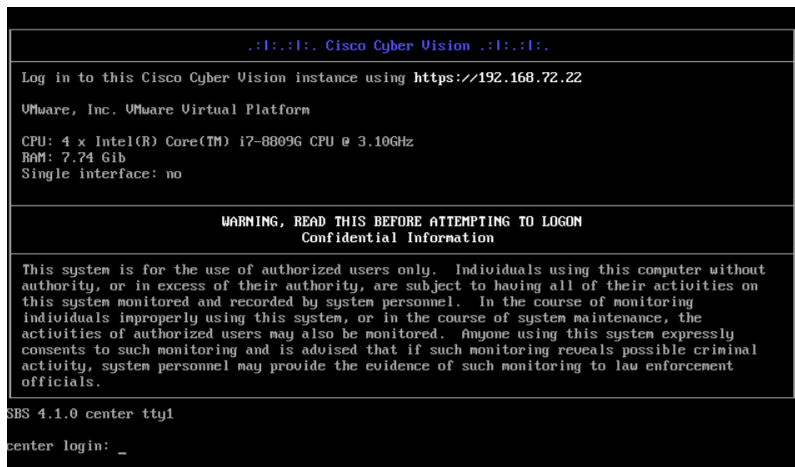

Complete the basic Center configuration

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.
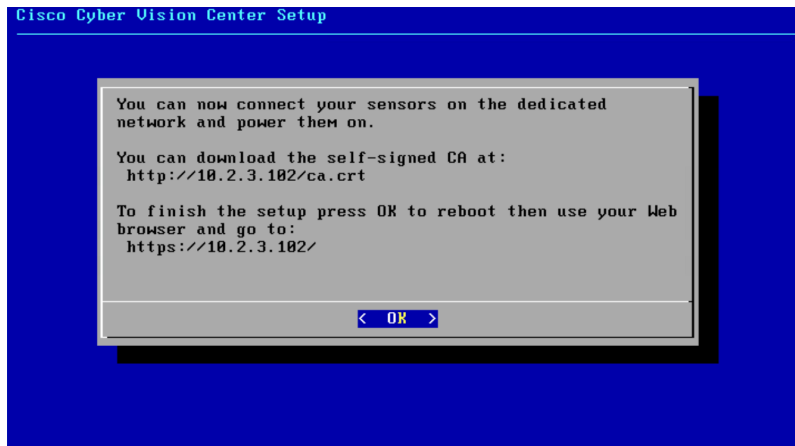
Enter OK to finish the basic Center configuration.

Note A major change regarding the Center command line (CLI) access through serial console or SSH was made in Cisco Cyber Vision version 4.1.0. The user root is no more usable to establish the connection. A new user called 'cv-admin' must be used. 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:**
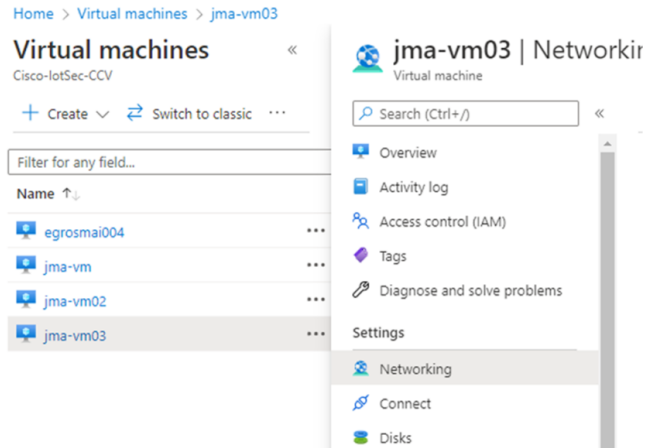
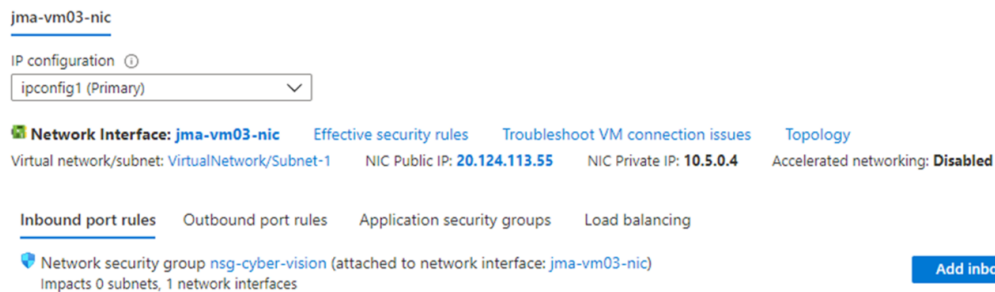| Protocol	Port
AMPQ	TCP/5671
Syslog	UDP/10514

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 ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

5671

Protocol

◯ Any
◉ TCP
◯ UDP
◯ ICMP

Action

◉ Allow
◯ Deny

Priority * ⓘ

1030

Name *

AMPQ

Description

Add   Cancel

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:

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