Cisco Cyber Vision for Azure Cloud Installation Guide, Release 4.4.0

First Published: 2022-09-16

Last Modified: 2022-09-16

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

CONTENTS

CHAPTER 1

About this documentation

Document purpose

This documentation describes how to install Cisco Cyber Vision in Azure Cloud.

This documentation is applicable to Cisco Cyber Vision **version 4.1.2**.

Warnings and notices

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

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.

Warning Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

Important Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

Note Indicates important information on the product described in the documentation to which attention should be paid.

CHAPTER 2

Getting started

Overview

Deploy Cisco Cyber Vision in Microsoft Azure using a solution template available in the Azure Marketplace. When you deploy Cisco Cyber Vision using the Azure portal you can use an existing empty resource group and storage account (or create new ones). The solution template walks you through a set of configuration parameters that provide the initial setup of your Cisco Cyber Vision instance, allowing you to login to Cisco Cyber Vision web interface after first boot.

Prerequisites

- An Azure account.
- An SSH client (required to access the Cisco Cyber Vision Center console).
- Communication path: Microsoft.Network/publicIPAddresses IPs for access to the Cisco Cyber Vision resources.
- A Static IP (the default public IP may change after a reboot. This can cause an issue for sensors).
- Minimum configuration to run and test the product are 4 vCPU and 16GB RAM.
- SSD disks are mandatory.

Supported features

- Center
- Global Center

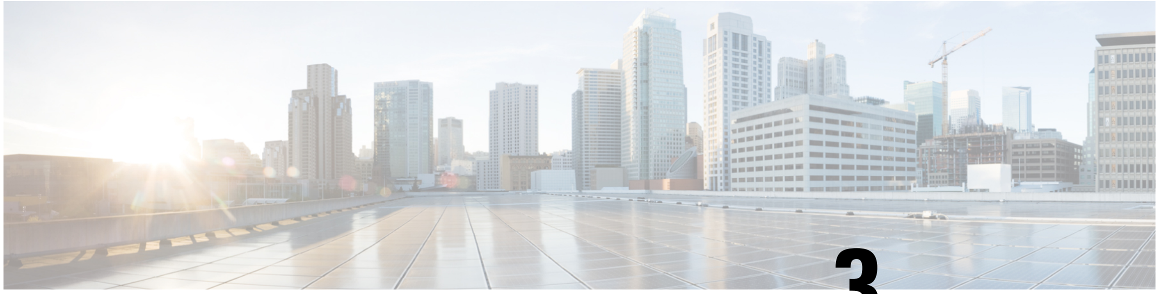
Limitations

The following features or hardware are not supported:

- Dual interface Centers.
- Sensors using the sensor management extension.

IPs

The IP attributed during the VM creation is dynamic by default. The IP may change at the VM reboot. If you want this IP address to be static, you can set it during the VM deployment in Virtual Machine settings, on page 8 or change it later in the VM settings of the Azure portal by clicking the VM IP address and modifying the IP address assignment.



CHAPTER 3

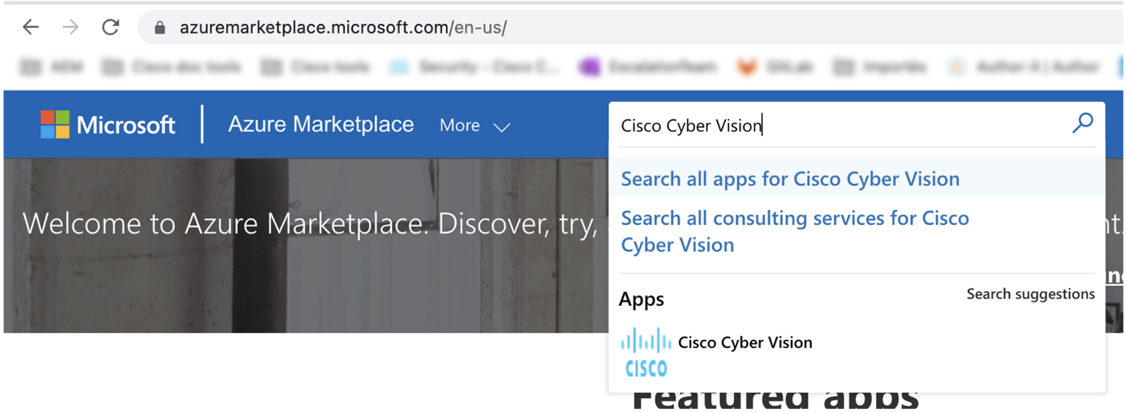
Deploy the Cisco Cyber Vision Center

Access Azure portal

Procedure

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

Step 2 Search for Cisco Cyber Vision.



azuremarketplace.microsoft.com/en-us/

Cisco Cyber Vision

Search all apps for Cisco Cyber Vision

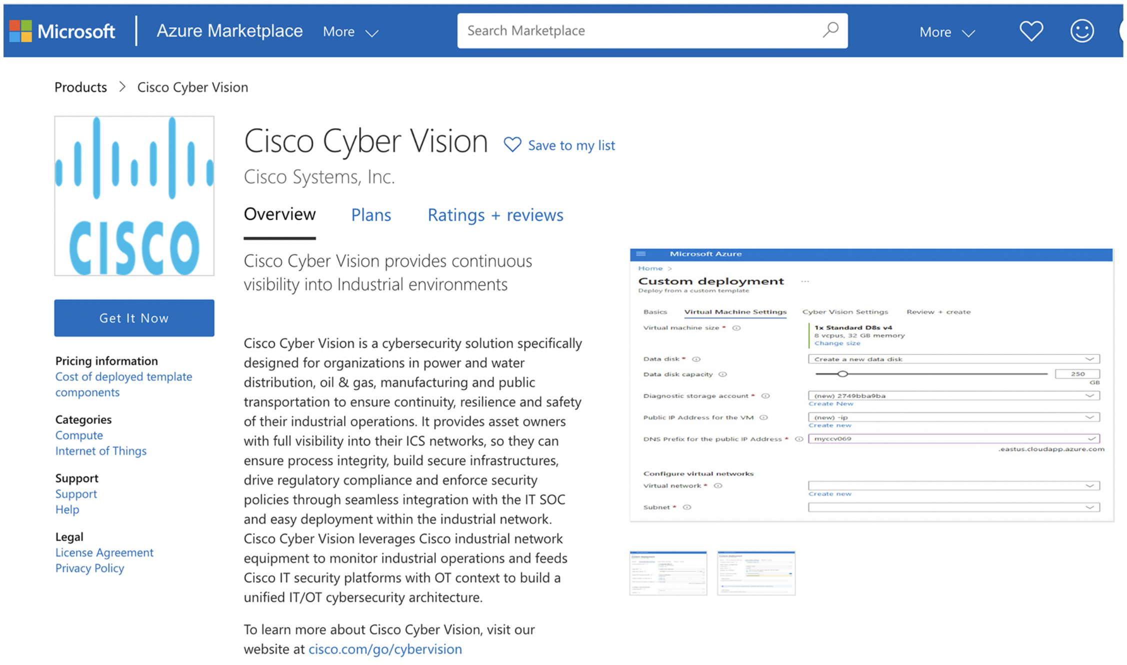
Search all consulting services for Cisco Cyber Vision

Apps

Search suggestions

Cisco Cyber Vision

Step 3 Click **Get it now**.



Products > Cisco Cyber Vision

Cisco Cyber Vision Save to my list

Cisco Systems, Inc.

Cisco Cyber Vision provides continuous visibility into Industrial environments

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

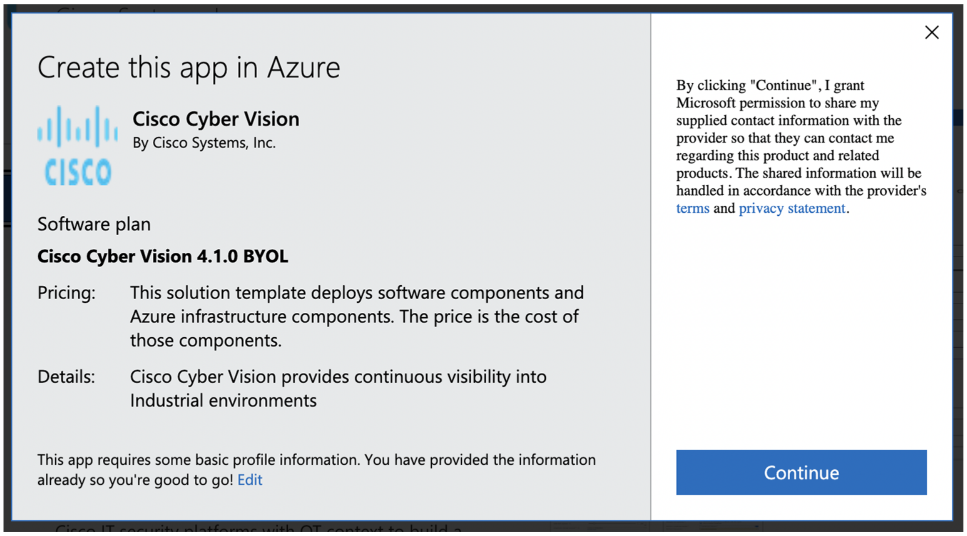
Microsoft Azure
Home >
Custom deployment
Deploy from a custom template

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

Virtual machine size *: 1x Standard D8s v4, 8 vcpus, 32 GB memory, Change size
Data disk *: Create a new data disk
Data disk capacity: 250 GB
Diagnostic storage account *: (new) 2749bba9ba — Create New
Public IP Address for the VM: (new) -ip — Create new
DNS Prefix for the public IP Address *: myccv069 .eastus.cloudapp.azure.com

Configure virtual networks
Virtual network *: — Create new
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

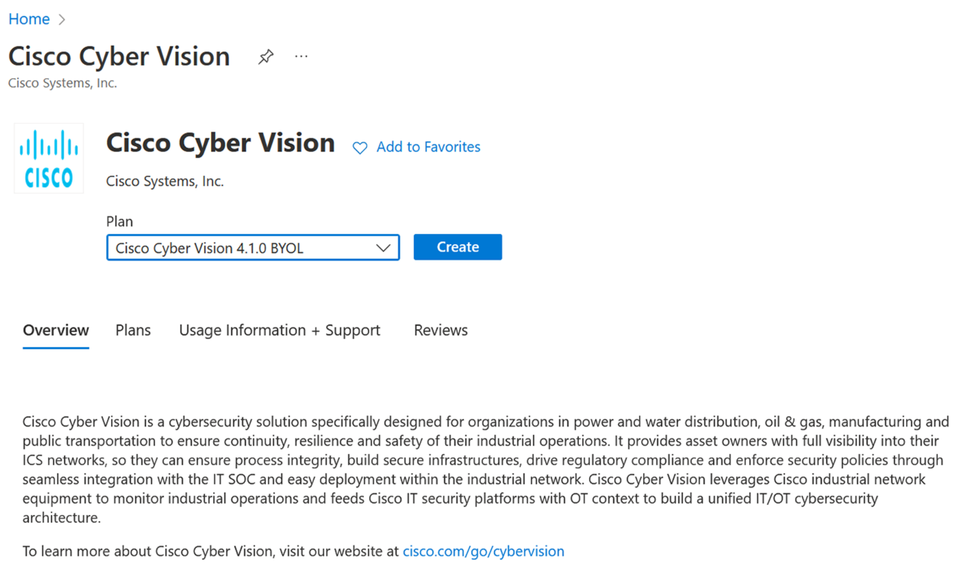
This app requires some basic profile information. You have provided the information already so you're good to go! Edit

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.

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.

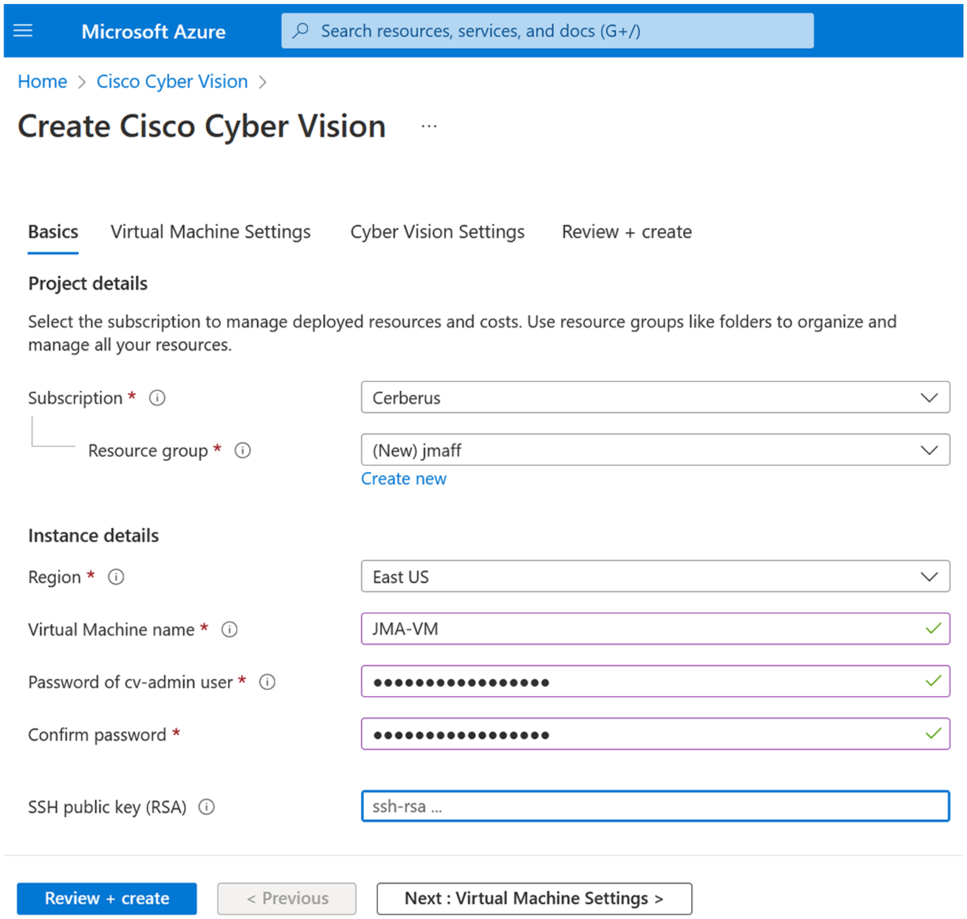
Password must comply with three of the following conditions: 1 lower case character, 1 upper case character, 1 number, and 1 special character that is not '\' or '-'.

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**.



Microsoft Azure
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 * : Cerberus

Resource group * : (New) jmaff

Create new

Instance details

Region * : East US

Virtual Machine name * : JMA-VM

Password of cv-admin user * : ●●●●●●●●●●●●●●●●

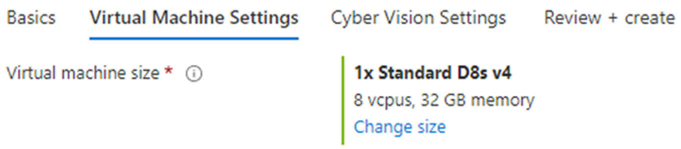
Confirm password * : ●●●●●●●●●●●●●●●●

SSH public key (RSA) : ssh-rsa ...

Virtual Machine settings

Procedure

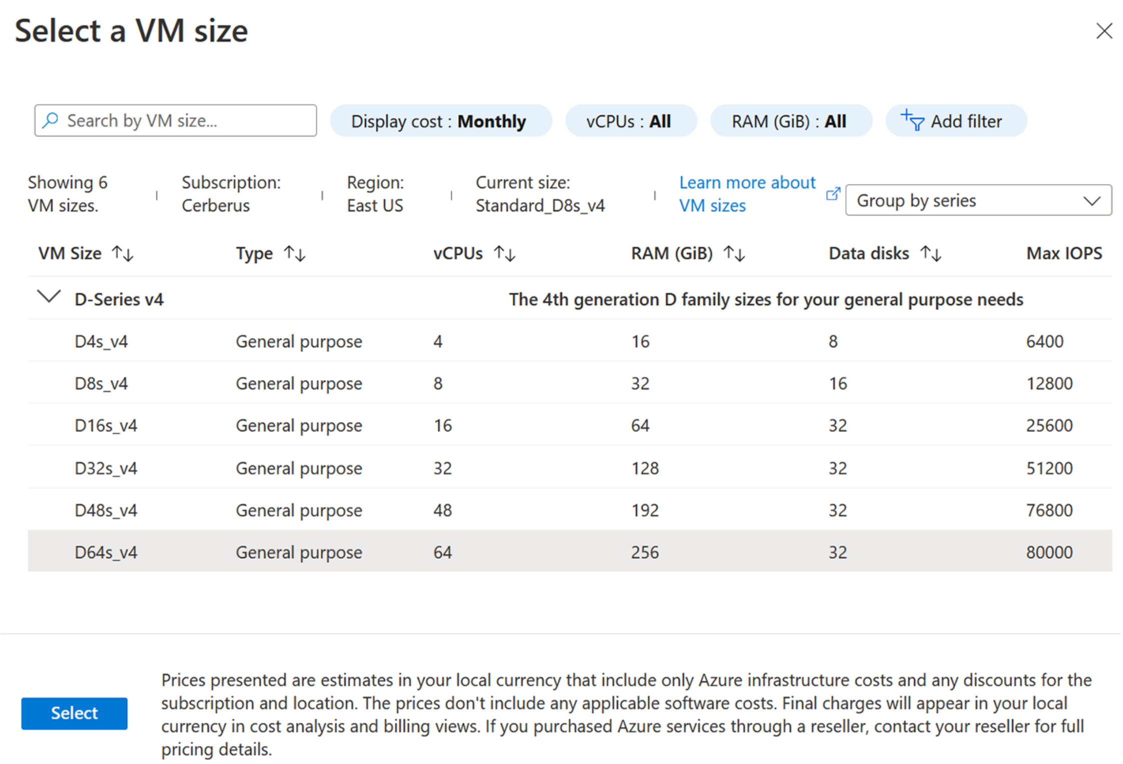
Step 1 You can change the VM size clicking **change size**.



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

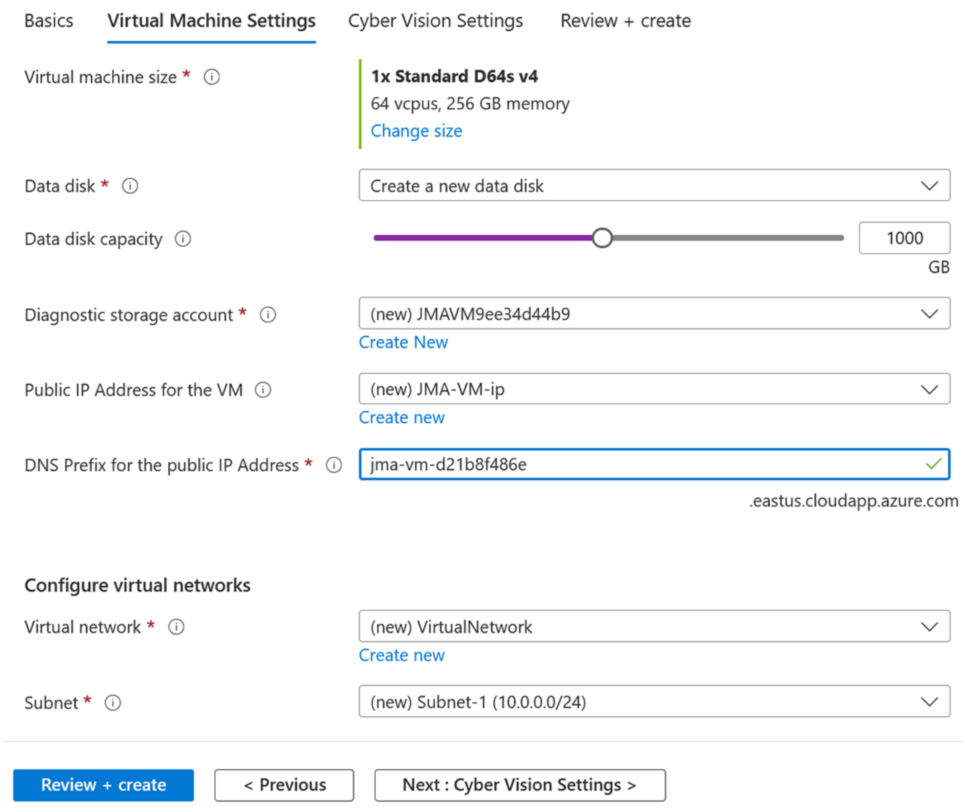
Showing 6 VM sizes. | Subscription: Cerberus | Region: East US | Current size: Standard_D8s_v4 | Learn more about VM sizes

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

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)

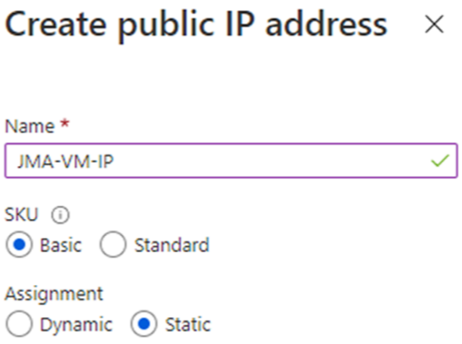
A disk is required to store the data of the Center. The recommended size for a Center is 250GB and 1TB minimum for a Global Center. Choose one of the options below:

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**.

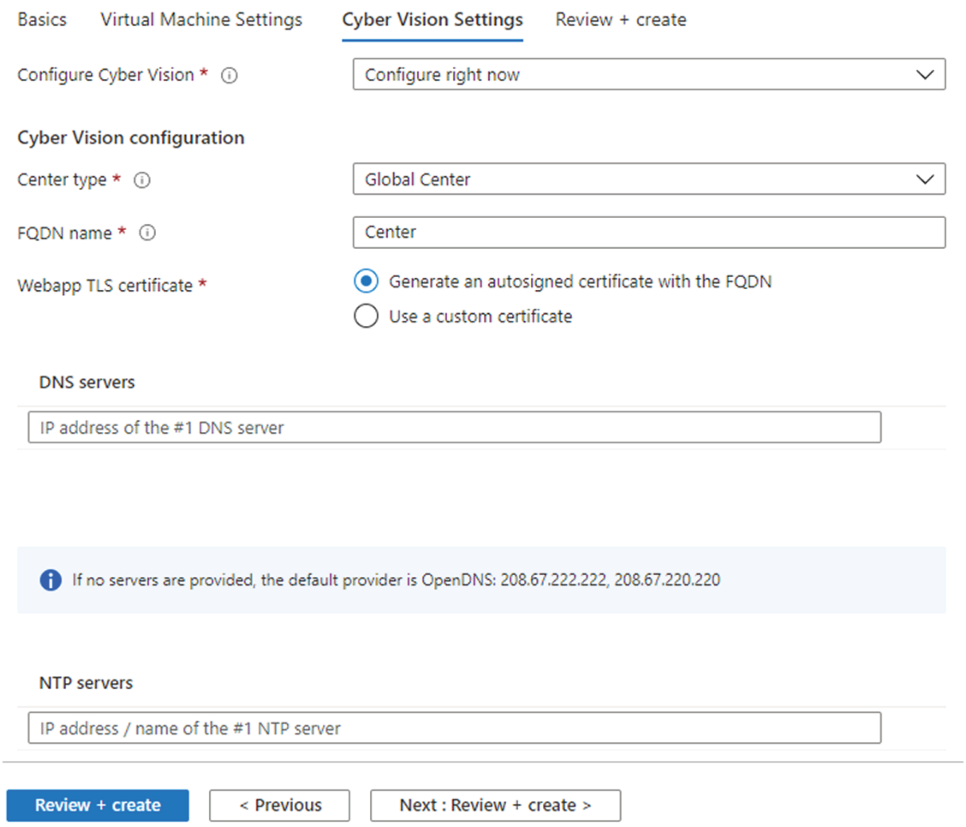
Step 3 Set a FQDN.

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**.



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

What to do next

Proceed with Review and create custom deployment, on page 14.

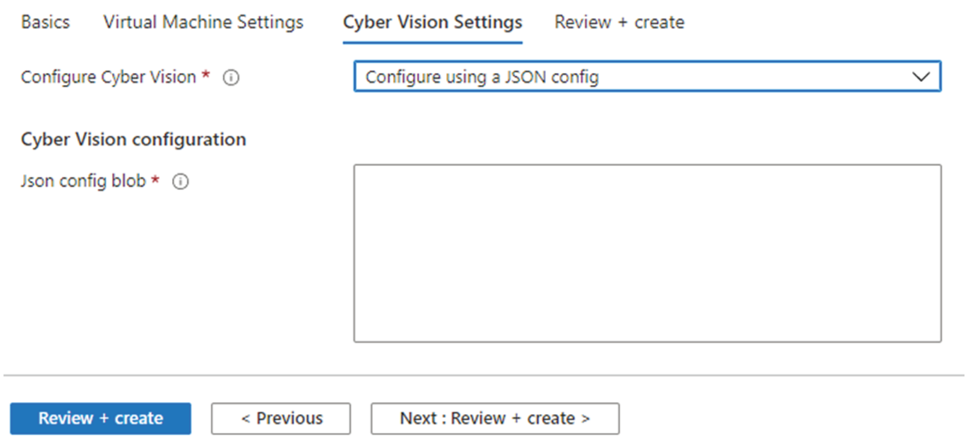
Configure using a JSON config

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, on page 37

Procedure

Step 1 Select **Configure using a JSON config**.

Step 2 Fill in the Json config blog using the annex syntax.



Configure Cyber Vision * : Configure using a JSON config

Cyber Vision configuration

Json config blob *

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

What to do next

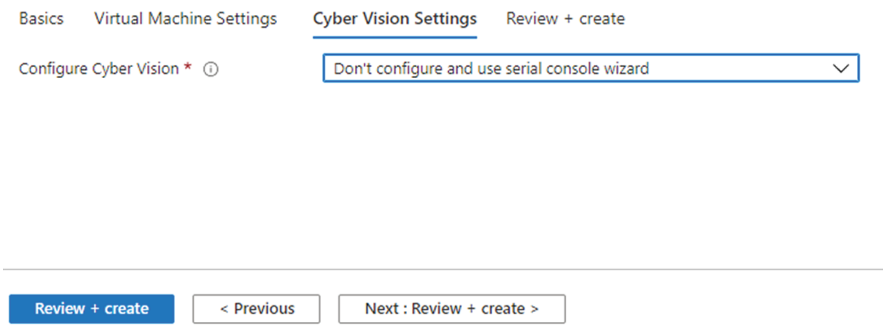
Proceed with Review and create custom deployment, on page 14.

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**.



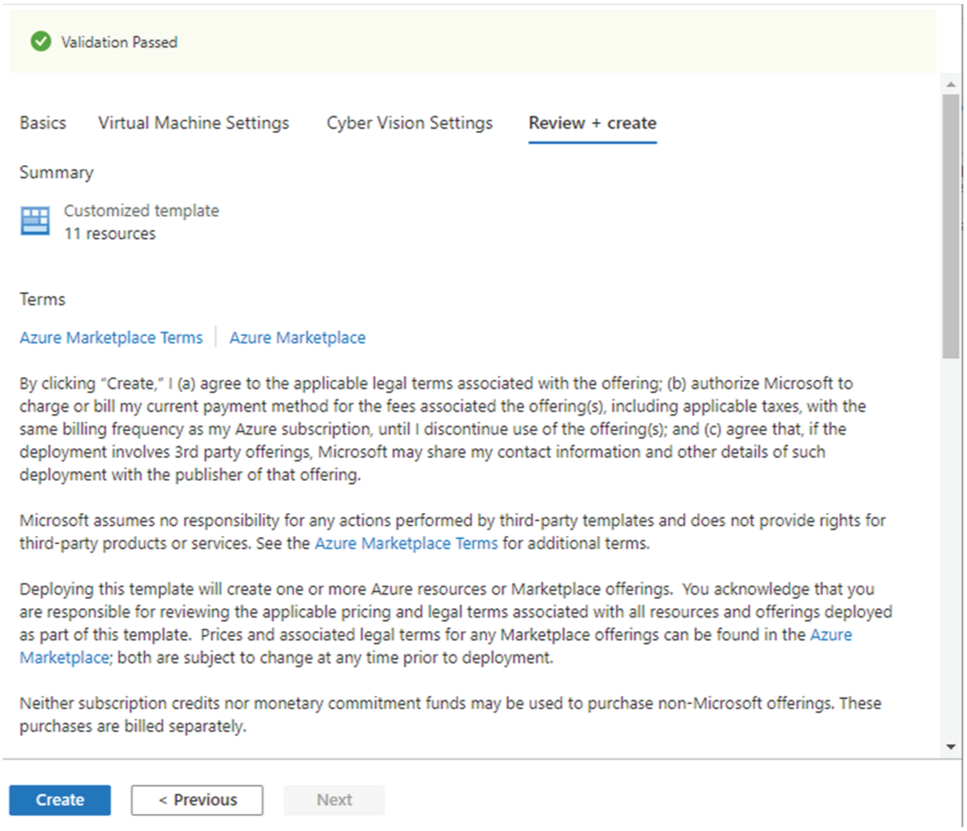
Configure Cyber Vision * : Don't configure and use serial console wizard

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

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.

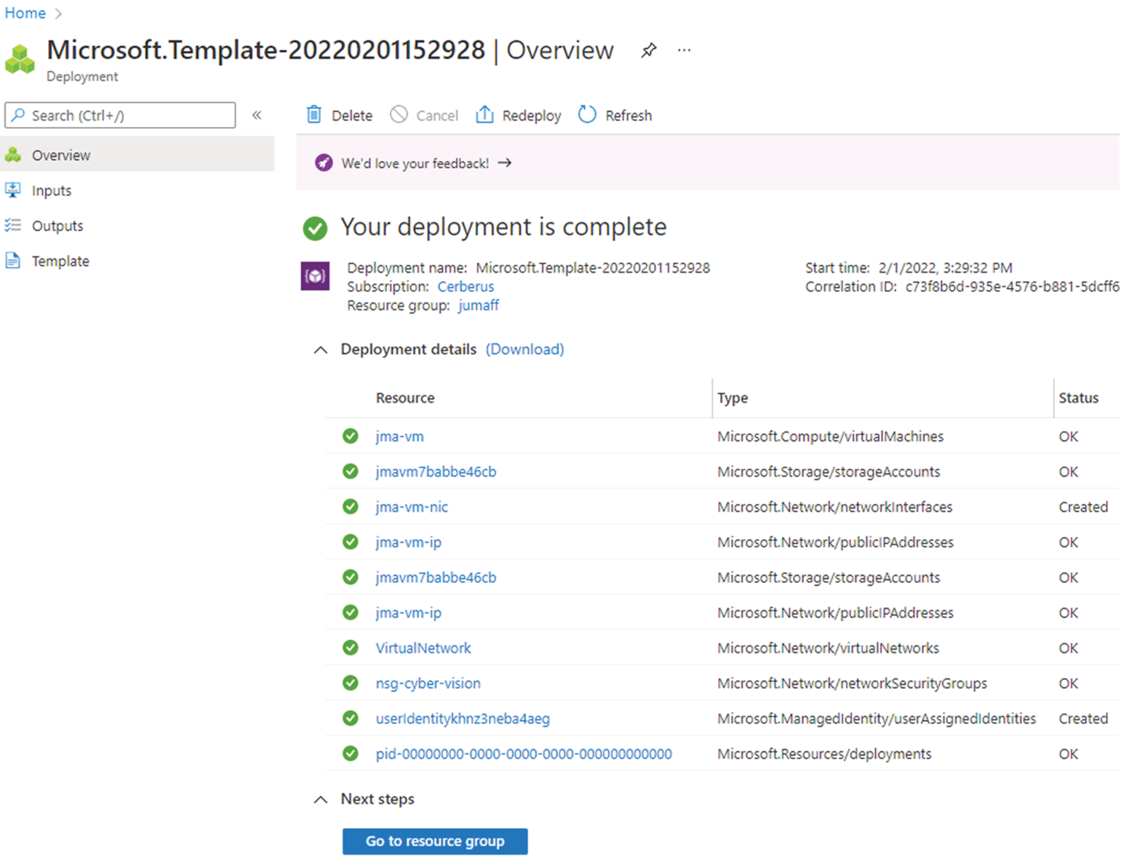
Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for 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.

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:



Microsoft.Template-20220201152928 | Overview

Deployment

Your deployment is complete

Deployment name: Microsoft.Template-20220201152928
Subscription: Cerberus
Resource group: jumaff

Start time: 2/1/2022, 3:29:32 PM
Correlation ID: c73f8b6d-935e-4576-b881-5dcff6

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
userIdentitykhnz3neba4aeg	Microsoft.ManagedIdentity/userAssignedIdentities	Created
pid-00000000-0000-0000-0000-000000000000	Microsoft.Resources/deployments	OK

Next steps

If you have used the serial console to configure the Azure virtual machine, proceed with the Basic Center configuration, on page 15.

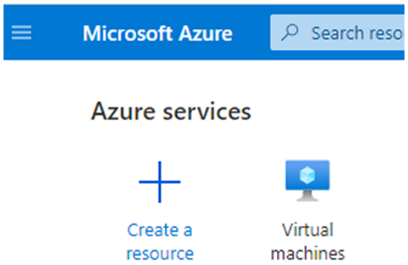
Basic Center configuration

Access the Basic Center Configuration

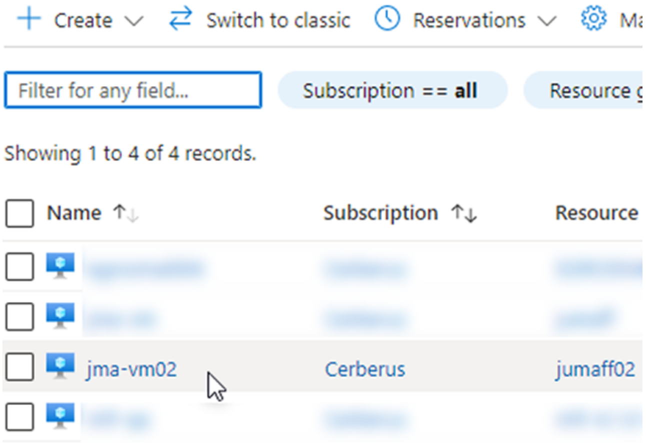
To access the Basic Center Configuration and setup the Cisco Cyber Vision Center or Global Center:

Procedure

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



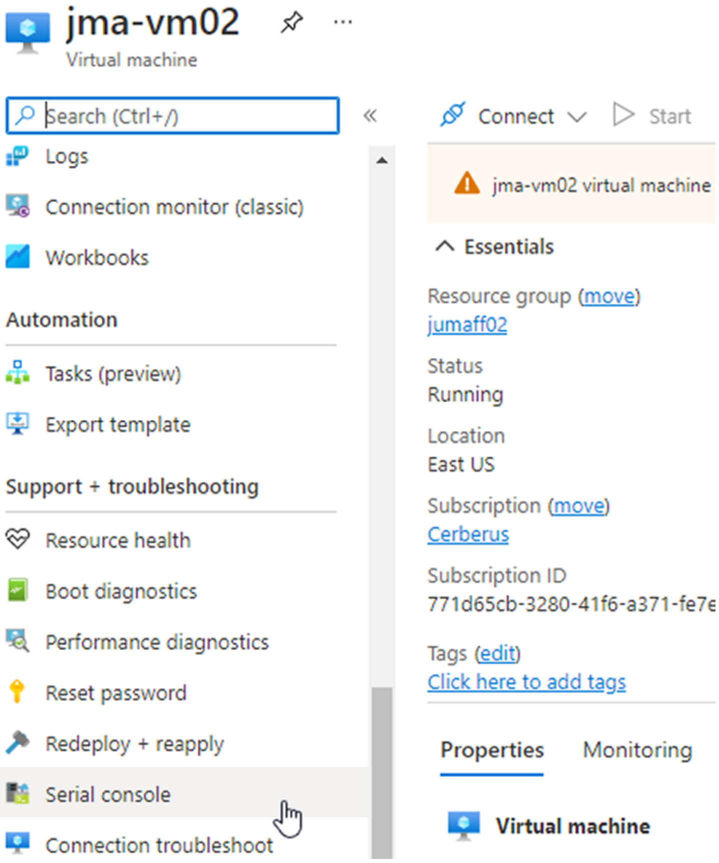
Step 2 Click the VM to configure via the serial console.



Showing 1 to 4 of 4 records.

□	Name ↑↓	Subscription ↑↓	Resource
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	jma-vm02	Cerberus	jumaff02
□	[redacted]	[redacted]	[redacted]

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



jma-vm02 virtual machine

Resource group (move)
jumaff02

Status
Running

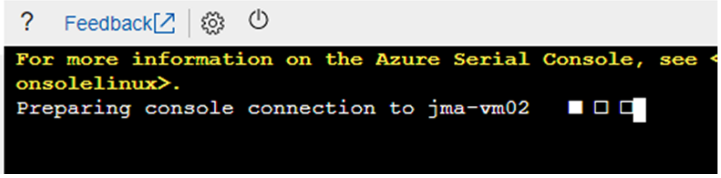
Location
East US

Subscription (move)
Cerberus

Subscription ID
771d65cb-3280-41f6-a371-fe7e

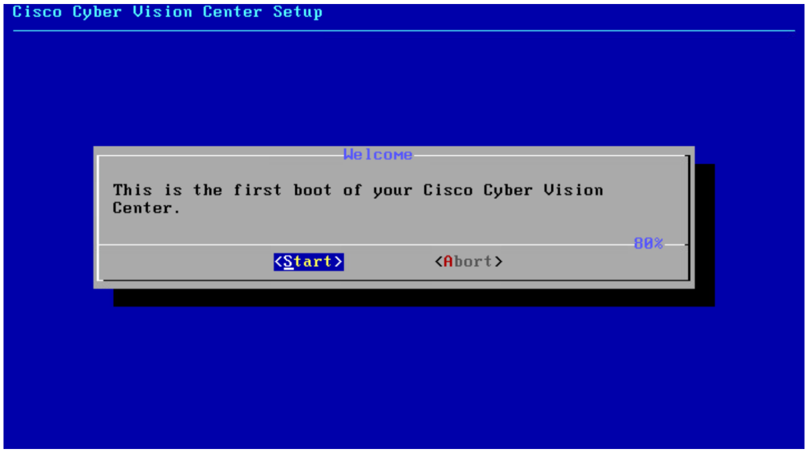
Tags (edit)
Click here to add tags

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



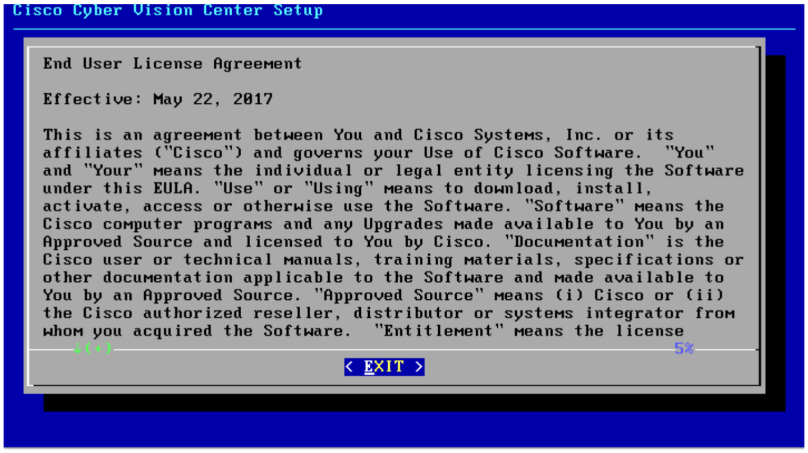
```
For more information on the Azure Serial Console, see <
onsolelinux>.
Preparing console connection to jma-vm02  ■ □ □
```

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

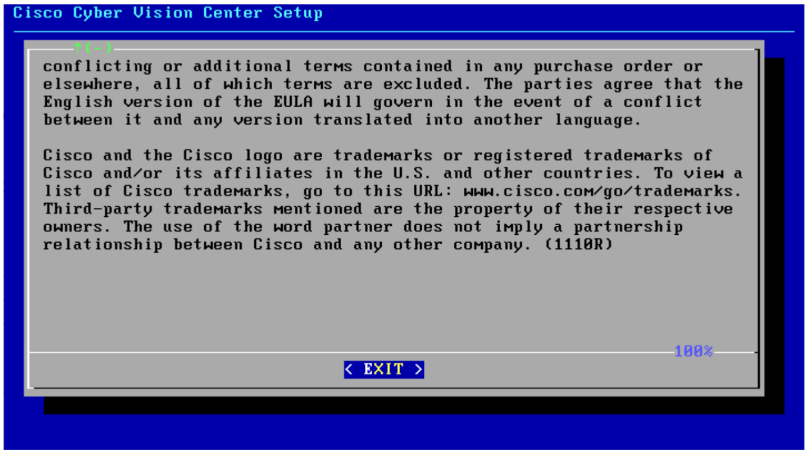


This is the first boot of your Cisco Cyber Vision Center.

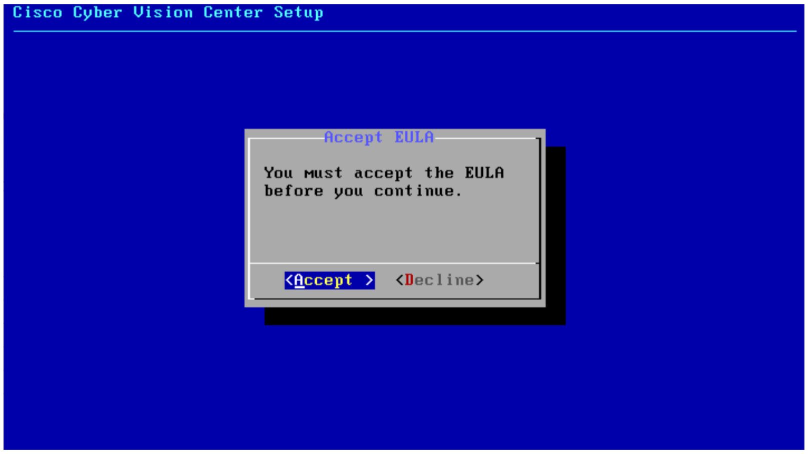
Accept the End User License Agreement



```
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
```



```
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)
```



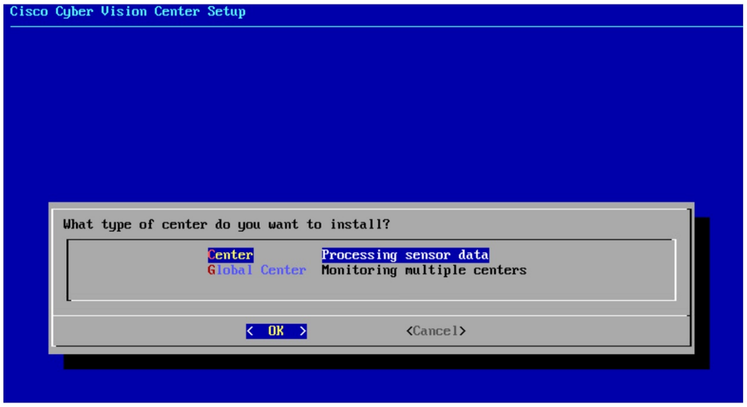
```
Cisco Cyber Vision Center Setup

Accept EULA
You must accept the EULA
before you continue.
```

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.

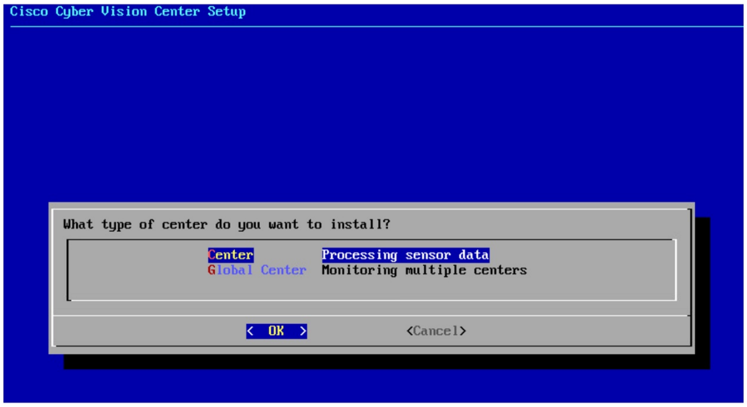
Select the type of Center you want to install.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?
Center          Processing sensor data
Global Center   Monitoring multiple centers
```

Center

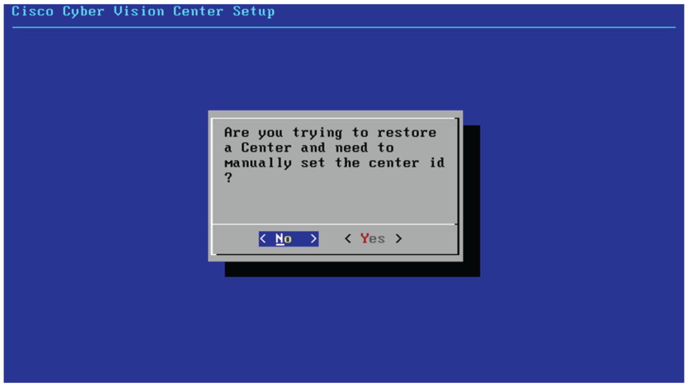
If installing a Center, select the first option.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

        Center          Processing sensor data
        Global Center   Monitoring multiple centers

           <  OK  >             <Cancel>
```

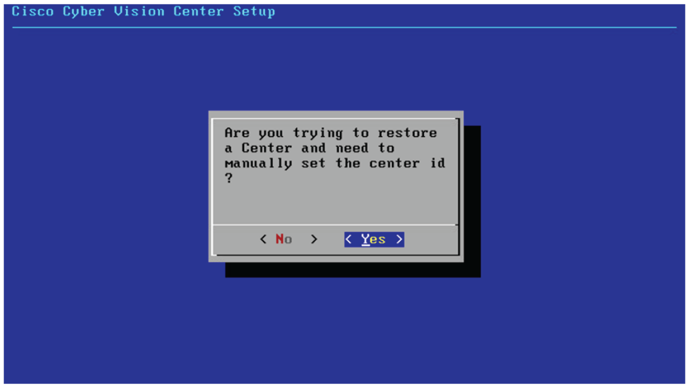
Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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



```
Cisco Cyber Vision Center Setup

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

   <  No  >    < Yes >
```

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

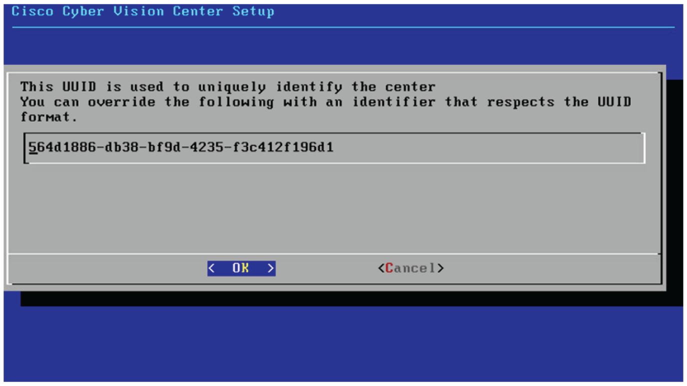


```
Cisco Cyber Vision Center Setup

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

   < No  >    < 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.

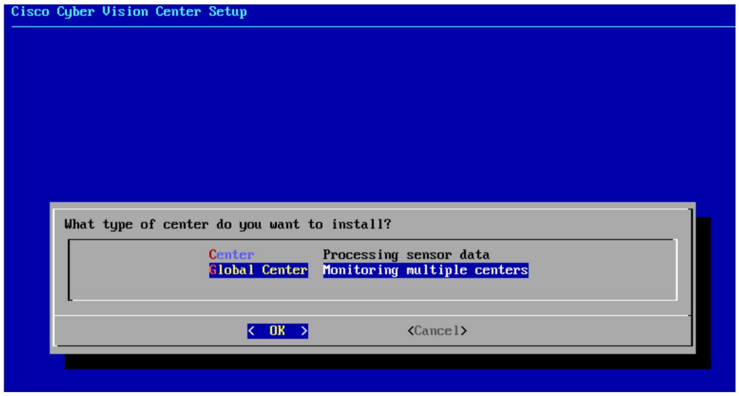


```
Cisco Cyber Vision Center Setup

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

564d1886-db38-bf9d-4235-f3c412f196d1
```

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

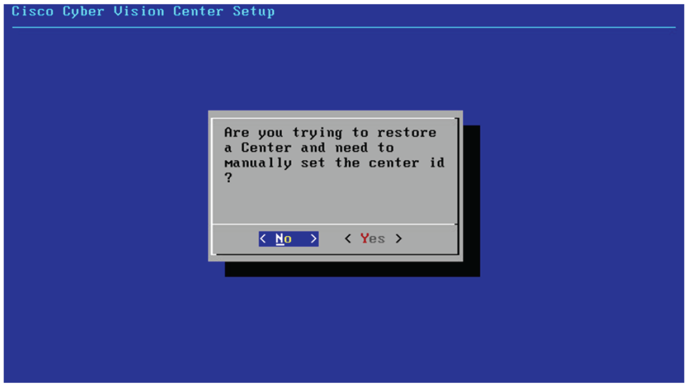
Global Center

If installing a Global Center, select the second option.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

Center          Processing sensor data
Global Center   Monitoring multiple centers
```

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

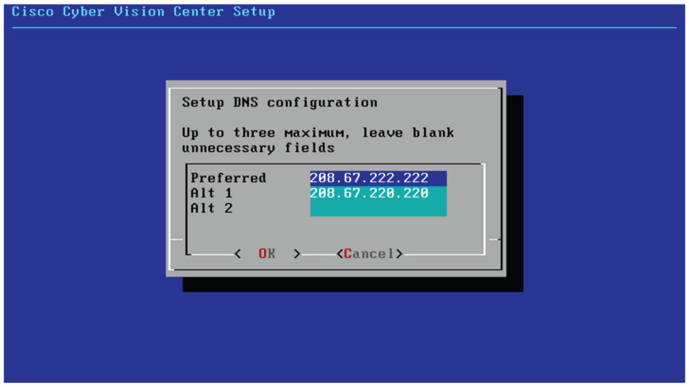


```
Cisco Cyber Vision Center Setup

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

You will be directed to the next step.

Configure the Center's DNS

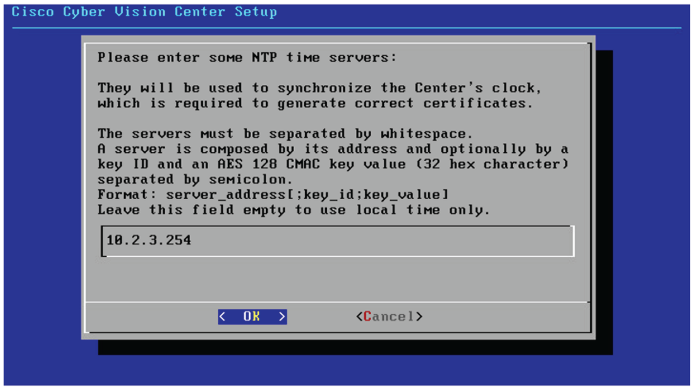
Type a DNS server address and optional fallbacks.



```
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
```

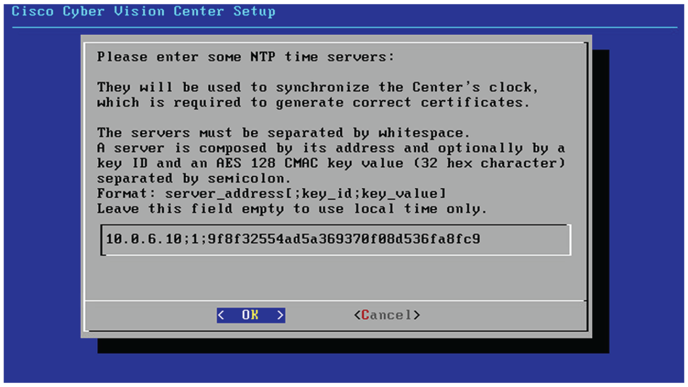
Synchronize the Center and the sensors to NTP servers

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
```

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

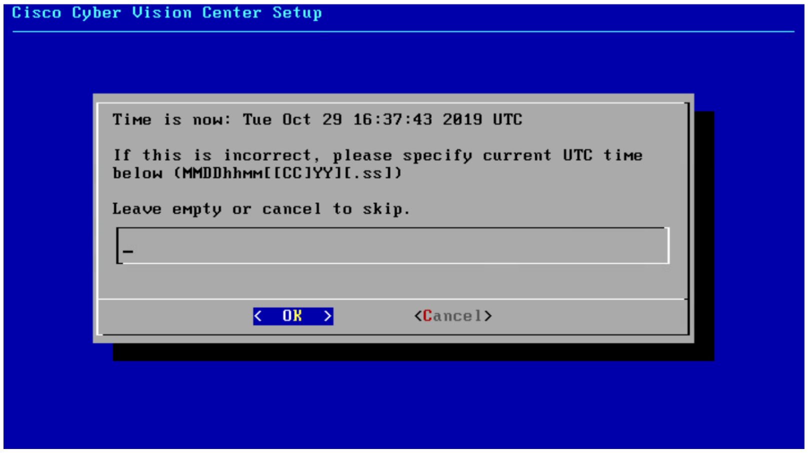


```
Cisco Cyber Vision Center Setup

Please enter some NTP time servers:

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

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

10.0.6.10;1;9f8f32554ad5a369370f08d536fa8fc9

< OK >        <Cancel>
```

The synchronization takes a few seconds.

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

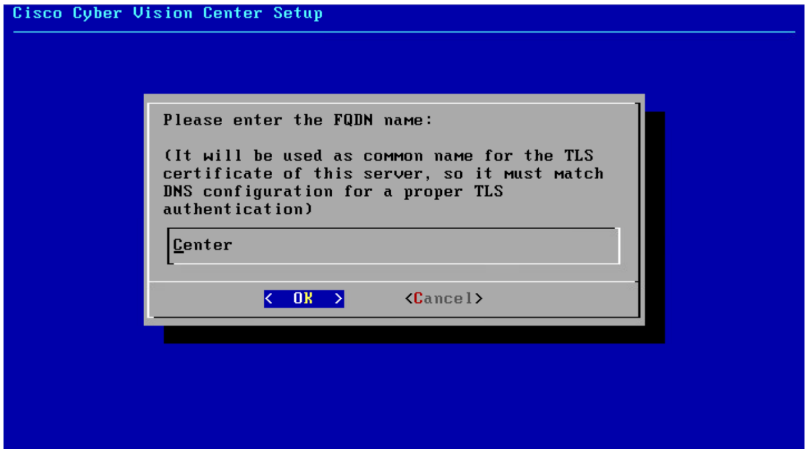
Note The time is set in UTC standard.



```
Cisco Cyber Vision Center Setup

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

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

Leave empty or cancel to skip.

_

< OK >        <Cancel>
```

Give the Center a name

Note This name will be used in the Center certificate.



```
Cisco Cyber Vision Center Setup

Please enter the FQDN name:

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

Center
```

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.

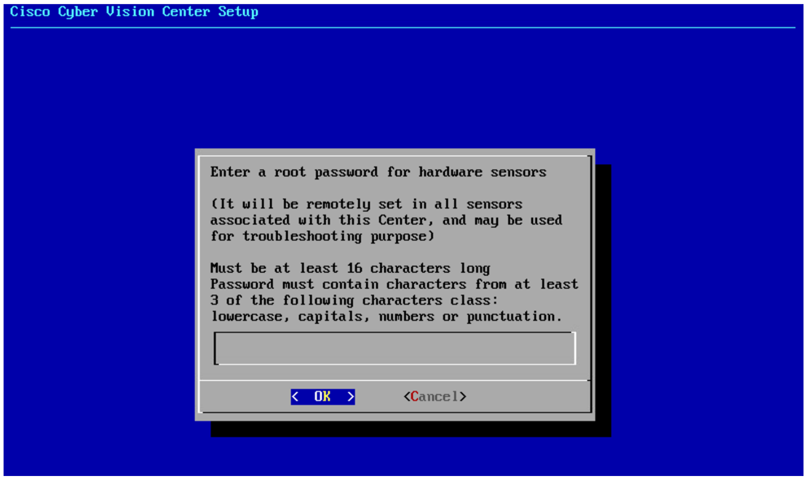
Configure the sensors' password

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.

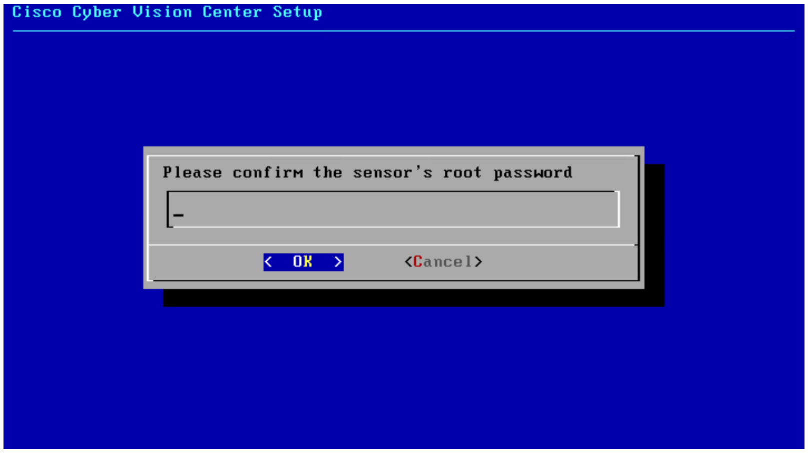
This password must be different than the one used for the Center, otherwise you will get an error message.



```
Cisco Cyber Vision Center Setup

Enter a root password for hardware sensors

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

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

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

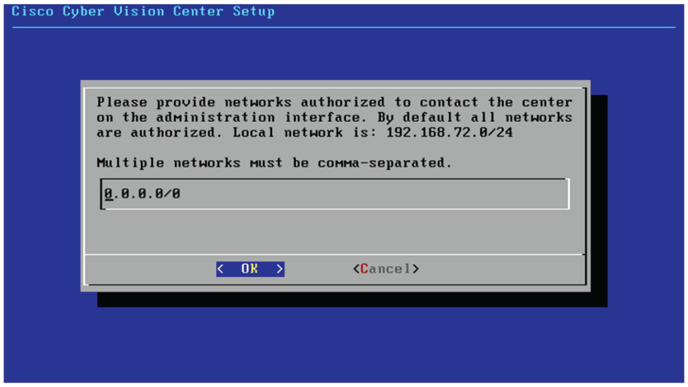
Confirm the password.



```
Cisco Cyber Vision Center Setup

Please confirm the sensor's root password

_

< OK >        <Cancel>
```

Authorize networks

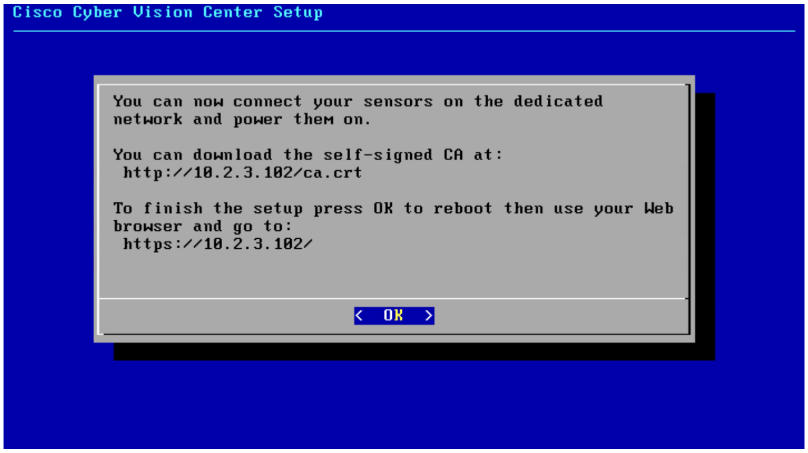
This step allows you to restrict IP addresses that can connect to the Administration interface. If no IP is entered, all networks are authorized by default.



```
Cisco Cyber Vision Center Setup

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

Multiple networks must be comma-separated.

0.0.0.0/0

< OK >        <Cancel>
```

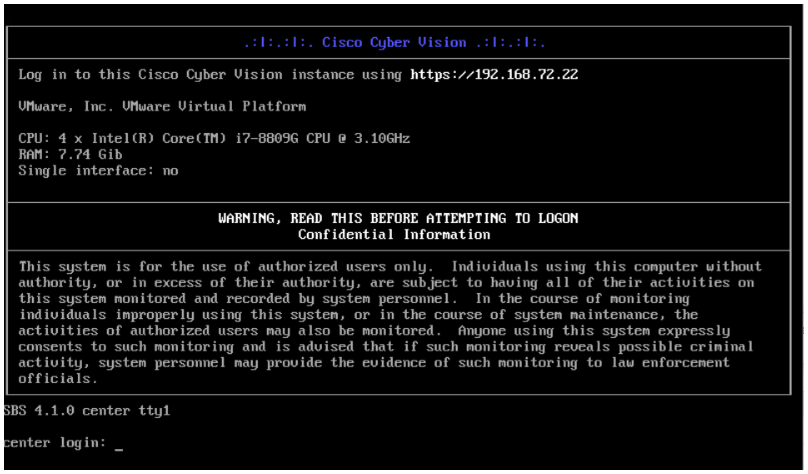
Complete the basic Center configuration

Next is the last screen of the basic Center configuration. It reminds you the addresses set to be used to download the CA certificate and access Cisco Cyber Vision. Save these addresses somewhere, you will need them later to access the user interface.



```
Cisco Cyber Vision Center Setup

  You can now connect your sensors on the dedicated
  network and power them on.

  You can download the self-signed CA at:
   http://10.2.3.102/ca.crt

  To finish the setup press OK to reboot then use your Web
  browser and go to:
   https://10.2.3.102/

                       <  OK  >
```

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).

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

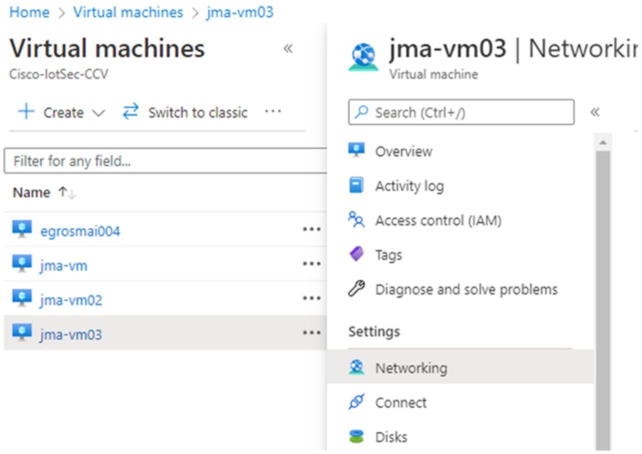
Configure communication ports

To configure a communication port:

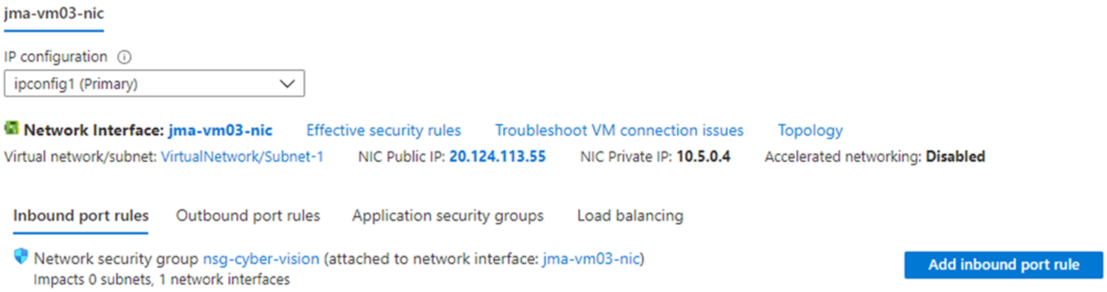
Procedure

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.

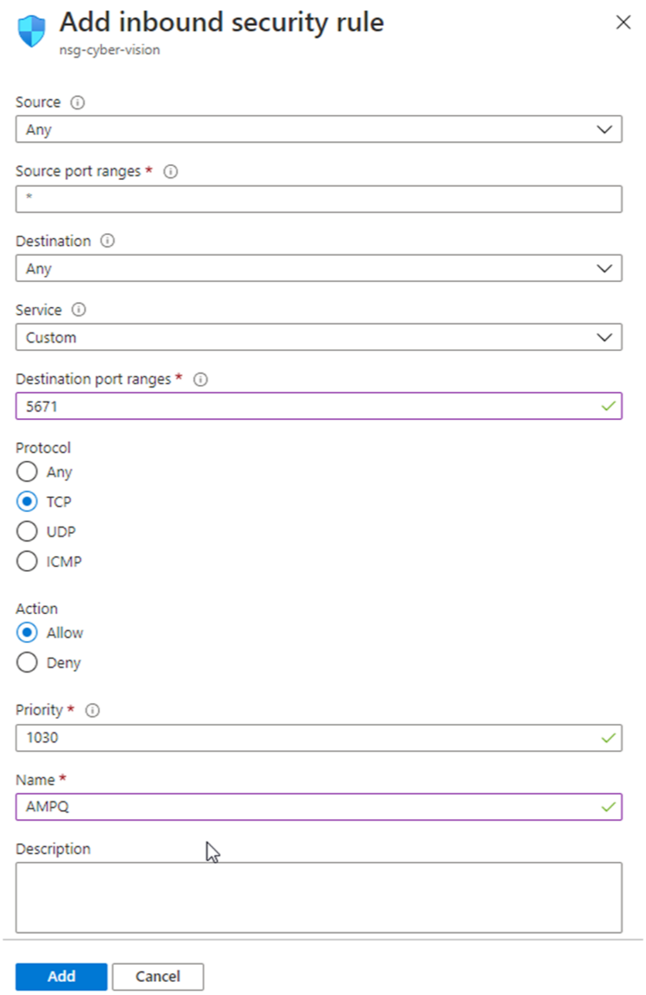

jma-vm03-nic
IP configuration
ipconfig1 (Primary)
Network Interface: jma-vm03-nic
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: VirtualNetwork/Subnet-1
NIC Public IP: 20.124.113.55
NIC Private IP: 10.5.0.4
Accelerated networking: Disabled
Inbound port rules
Outbound port rules
Application security groups
Load balancing
Network security group nsg-cyber-vision (attached to network interface: jma-vm03-nic)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule

Step 4 Fill in the settings according to the ports listed in Communication ports list, on page 27.

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

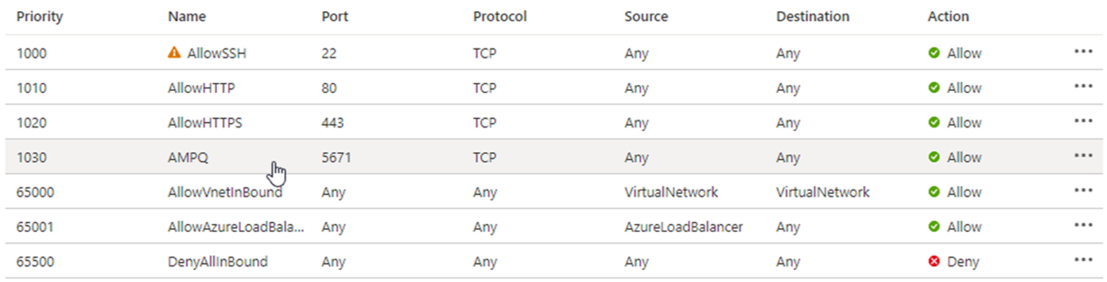
Priority *: 1030

Name *: AMPQ

Description:

Step 5 Click **Add**.

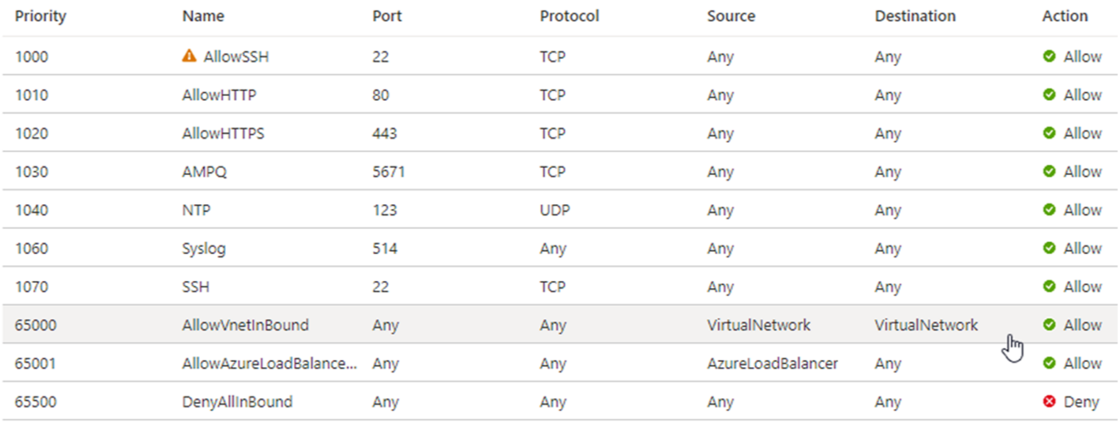
The added port appears in the Inbound port rules list.



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

CHAPTER 4

Configure the Cisco Cyber Vision Center synchronization

Global Center Configuration

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

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

Enrollment and unenrollement will be described below.

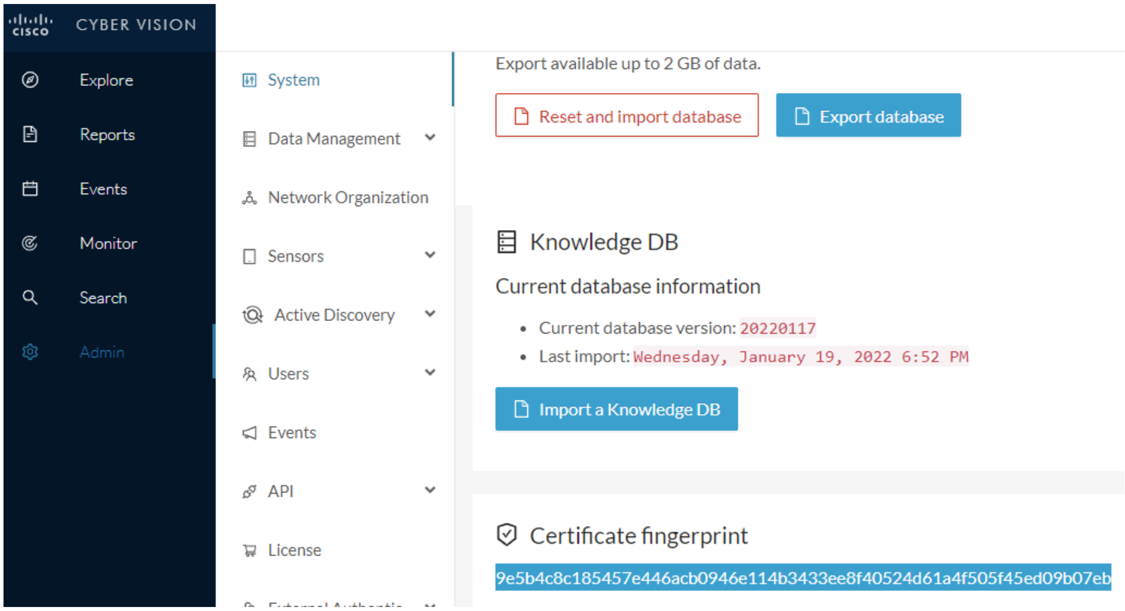
Center enrollment

Before you begin

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

Procedure

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



Export available up to 2 GB of data.

Knowledge DB

Current database information

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

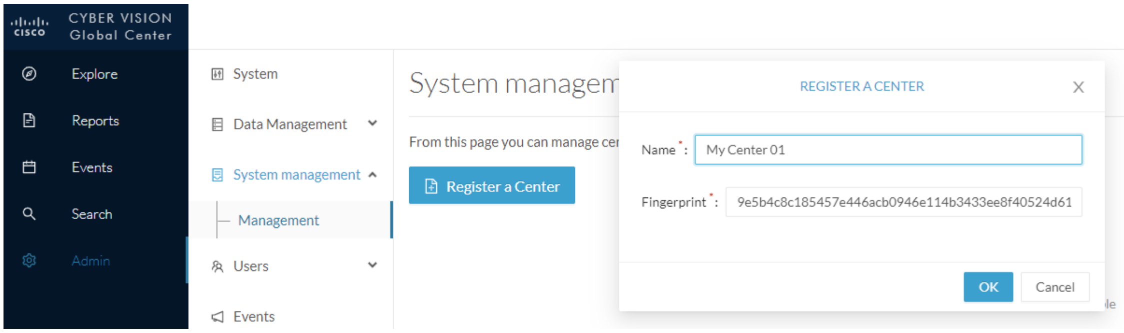
Certificate fingerprint

9e5b4c8c185457e446acb0946e114b3433ee8f40524d61a4f505f45ed09b07eb

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

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

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

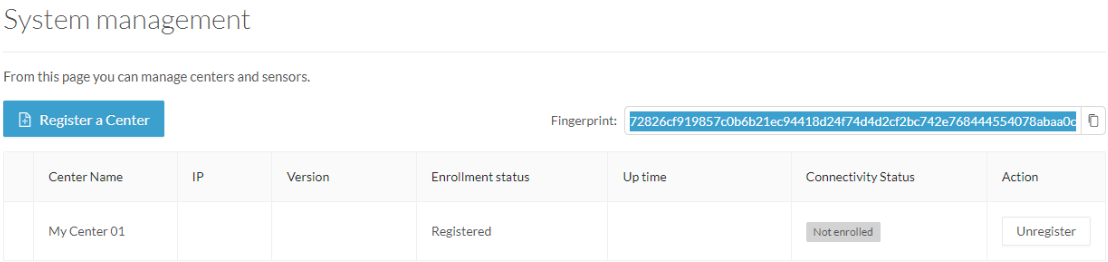


From this page you can manage cer

Name * : My Center 01

Fingerprint * : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61

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



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

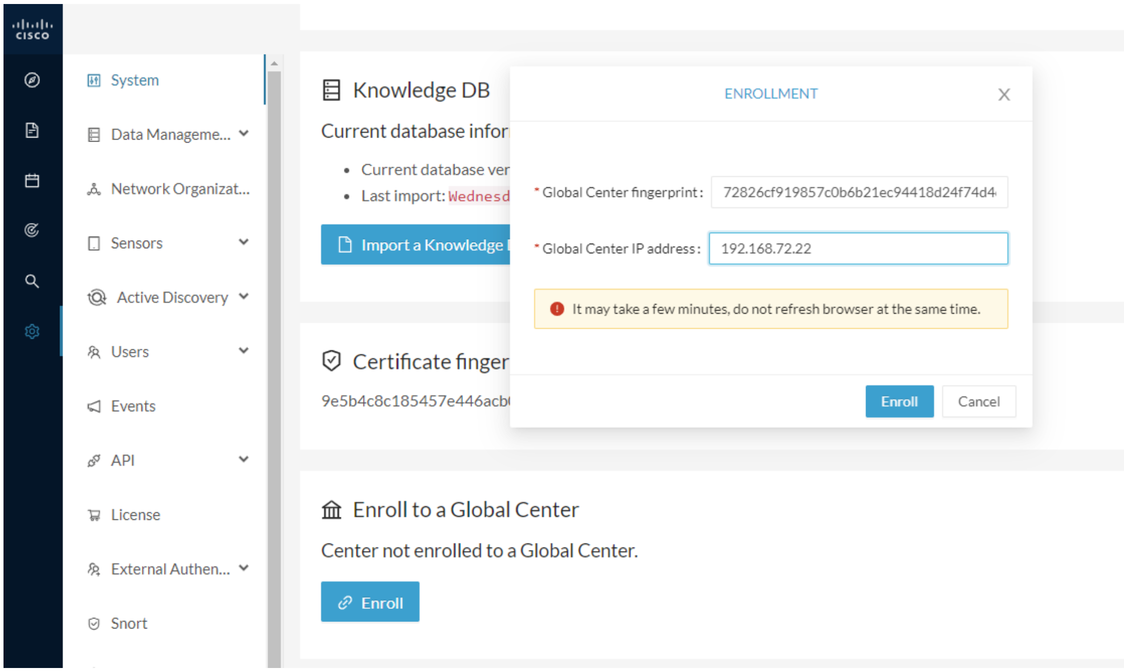
Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
My Center 01			Registered		Not enrolled	Unregister

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

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

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

c) press on **Enroll**



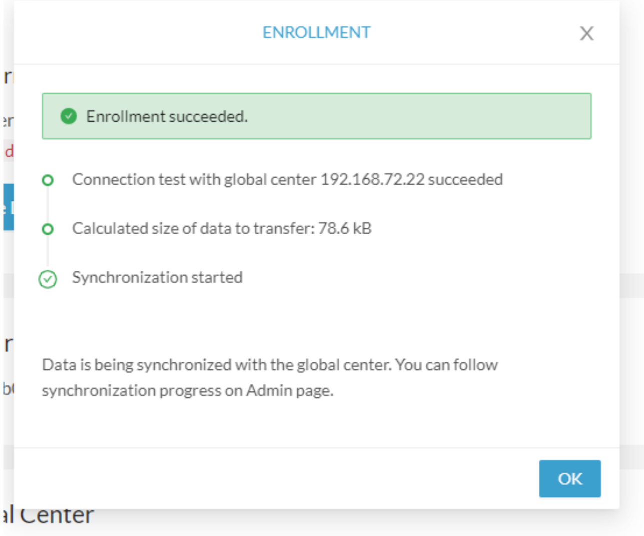
ENROLLMENT

* Global Center fingerprint: 72826cf919857c0b6b21ec94418d24f74d4

* Global Center IP address: 192.168.72.22

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

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



ENROLLMENT

Enrollment succeeded.

Connection test with global center 192.168.72.22 succeeded

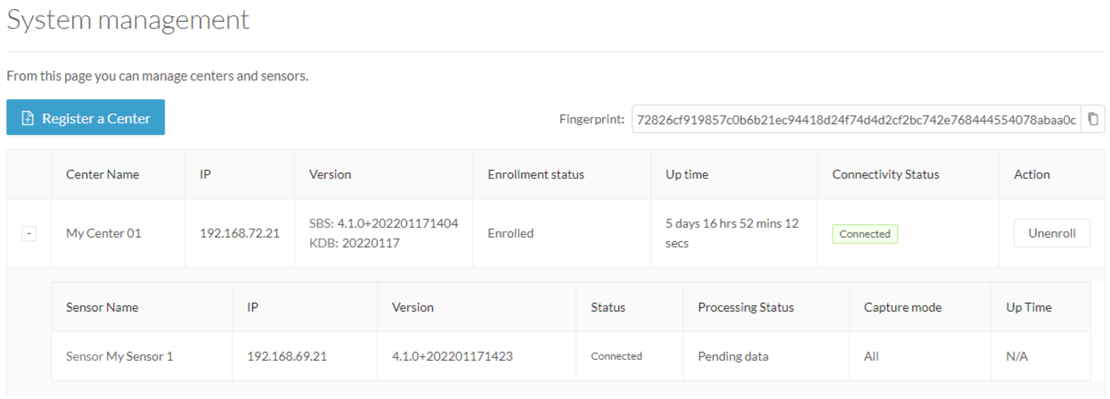
Calculated size of data to transfer: 78.6 kB

Synchronization started

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

What to do next

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



System management

From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

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

Center unenrollment

Before you begin

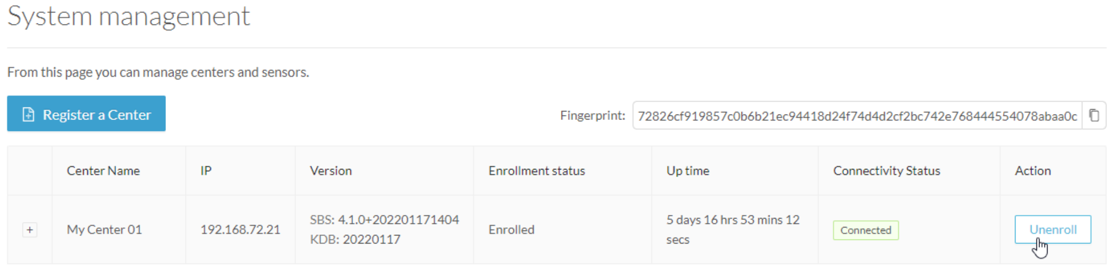
A Center can be unenrolled whenever it is needed, for example as a maintenance operation to replace the Center or the Global Center. This will delete all the Center's data in the Global Center.

Procedure

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

All Centers of the Global Center are listed.

Step 2 Click Unenroll on the Center required.



System management

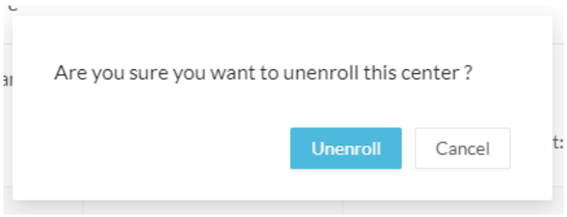
From this page you can manage centers and sensors.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

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

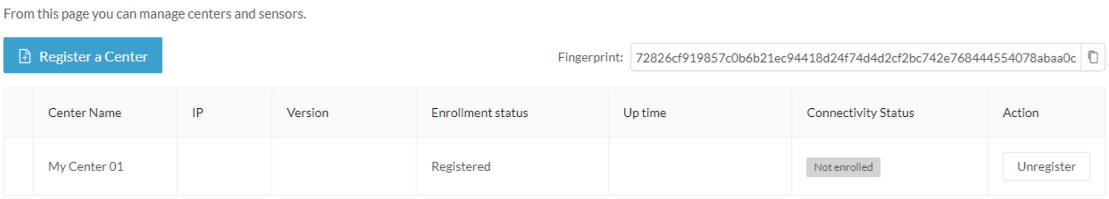
Step 3 A popup asking for confirmation appears. Click **Unenroll** to start the process.



Are you sure you want to unenroll this center ?

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

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



From this page you can manage centers and sensors.

Register a Center

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

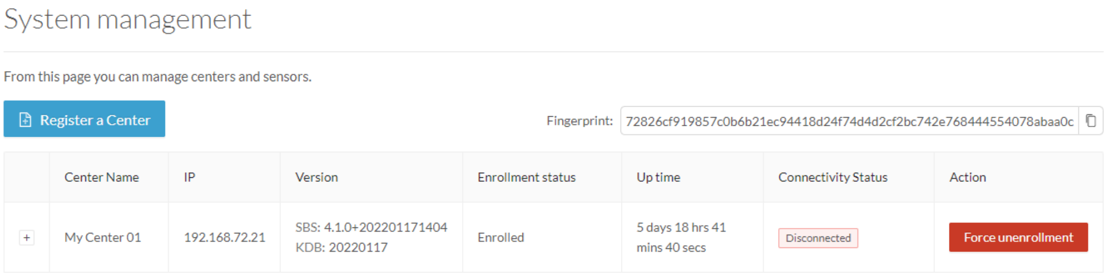
Force the unenrollement of a Center

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

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

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

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



System management

From this page you can manage centers and sensors.

Register a Center

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

CHAPTER 5

Annex – Setup Center json file

Annex – Setup Center json file

- keys:

  SSH public keys to add in the authorized keys.

- dns:

  DNS used by Cisco Cyber Vision. If not specified, Cisco Umbrella is used by default: https://docs.umbrella.com/mssp-deployment/docs/point-dns-to-cisco-umbrella.

- dhcpd-enabled:

  Enable or not DHCPD on the Collection network interface. Accepts "true" or "false" as string.

- single-interface:

  Deploy Cisco Cyber Vision in single interface mode as default mode.

- center-type:

  Type of Cisco Cyber Vision Center to deploy: Standalone (default), Local Center or Global Center.

- center-id:

  Specify Center ID. If not provided, a new one is generated at first boot.

- fqdn:

  FQDN to access the Cisco Cyber Vision web application. Public IPv4 DNS is used by default.

- ipset:

  Configure allowed networks. 169.254.0.0/16 and 0.0.0.0/0 (all networks) are used by default.

Examples:

- To deploy a standalone Center, leave the textbox empty.

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

  ```
  {
  ```

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

}
```

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

  ```
  {

  "center-type": "Global Center",

  }
  ```

CHAPTER 6

Center Backup and Restore

A new Command Line Interface (CLI) command is available to back up and restore a center. It will help the user to migrate a center from one appliance to another. For example, migrating a center from a virtual machine to a UCS appliance. The feature is designed to backup all settings and data, including:

- Operating system settings (such as IP addresses, names, certificates, etc.)
- Cyber Vision Settings
- Cyber Vision Data

After restoration, the new center will function on the network just like the old center.

Backup and Restore Constraints

list of the constraints:

- The new appliance requires an equal number of network interfaces as the center backed up.
- Set up the new appliance with Cyber Vision configuration. (Achieve the center setup, at least for the eth0 IP address, which needs to be configured to transfer the center archive.
- The new center interface configuration (single or dual) needs to match the backed-up center.
- As the new center adopts all old center settings like the IP address, the old appliance needs to be powered off.
- The Cyber Vision License cannot be copied.
  1. Return the license to the smart account server.
  2. After restoring, the new center needs to be licensed.
- Install the report extension on the restored center.

1. Report configuration and old report versions are copied.

Backup Cyber Vision Center

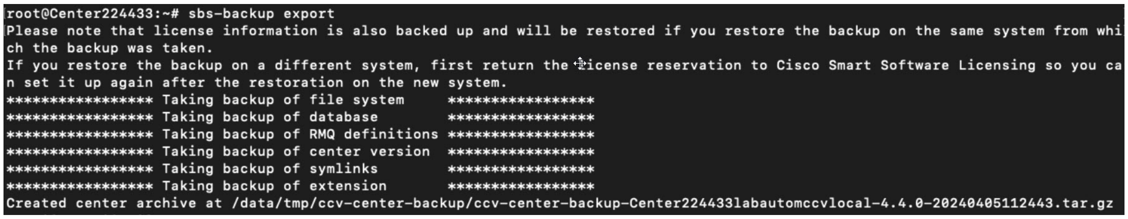
Procedure

Step 1 Connect to the center in SSH.

Step 2 Type the following command:

```
sbs-backup export
```

A file will be generated in the folder: `'/data/tmp/ccv-center-backup'`



```
root@Center224433:~# sbs-backup export
Please note that license information is also backed up and will be restored if you restore the backup on the same system from whi
ch the backup was taken.
If you restore the backup on a different system, first return the license reservation to Cisco Smart Software Licensing so you ca
n set it up again after the restoration on the new system.
***************** Taking backup of file system     *****************
***************** Taking backup of database        *****************
***************** Taking backup of RMQ definitions *****************
***************** Taking backup of center version  *****************
***************** Taking backup of symlinks        *****************
***************** Taking backup of extension       *****************
Created center archive at /data/tmp/ccv-center-backup/ccv-center-backup-Center224433labautomccvlocal-4.4.0-20240405112443.tar.gz
```

In the above given example, the created file is called::

```
ccv-center-backup-Center224433labautomccvlocal-4.4.0-20240405112443.tar.gz
```

Step 3 Copy the file to the new appliance for the restore.

Restore Cyber Vision Center

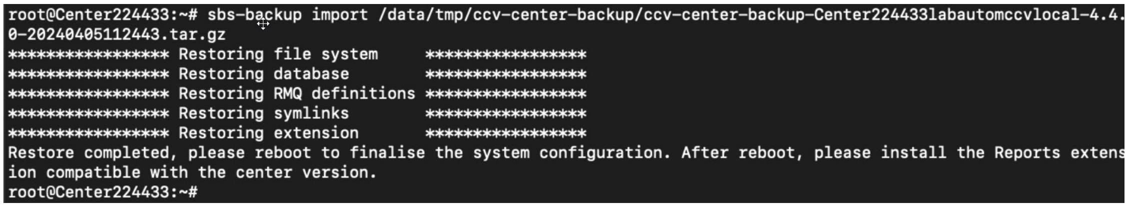
Copy the center backup file to the new center's **/data/tmp/ folder**.

Procedure

Step 1 Connect to the center in SSH.

Step 2 Type the following command:

```
sudo -i

sbs-backup import path-to center-backup
```



```
root@Center224433:~# sbs-backup import /data/tmp/ccv-center-backup/ccv-center-backup-Center224433labautomccvlocal-4.4.
0-20240405112443.tar.gz
***************** Restoring file system     *****************
***************** Restoring database        *****************
***************** Restoring RMQ definitions *****************
***************** Restoring symlinks        *****************
***************** Restoring extension       *****************
Restore completed, please reboot to finalise the system configuration. After reboot, please install the Reports extens
ion compatible with the center version.
root@Center224433:~#
```

Step 3 Type reboot to restart the sensor.

Step 4 Install the report management extension if necessary.

Step 5 Install a license on your center.

Automate the Backup of the Cyber Vision Center

Many tools are available to automate the Cyber Vision center backup.

rclone: It is a command line program to manage files. You can use it to synchronize your center backup with a remote drive.

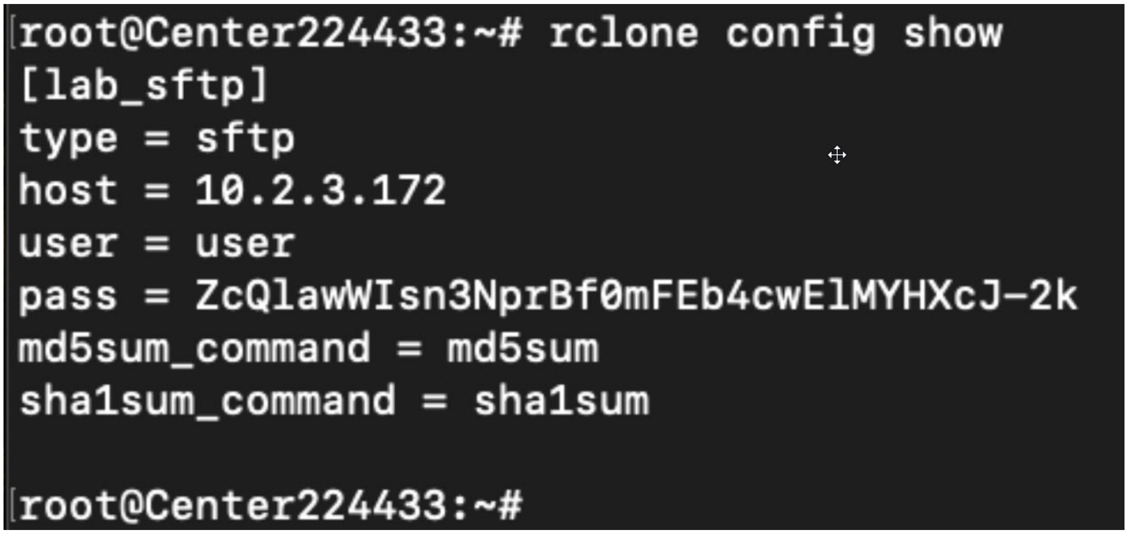
Procedure

Step 1 To handle the complex authentication of object storage systems, rclone requires configuration due to the information being stored in a config file. The simplest way to create this config is by running rclone with the config option:

```
sudo -i

rclone config
```

Various options are available, as mentioned here: https://rclone.org/docs/

Example of config file:



```
root@Center224433:~# rclone config show
[lab_sftp]
type = sftp
host = 10.2.3.172
user = user
pass = ZcQlawWIsn3NprBf0mFEb4cwElMYHXcJ-2k
md5sum_command = md5sum
sha1sum_command = sha1sum

root@Center224433:~#
```

Step 2 Rclone syncs a directory tree between storage systems. Here's the syntax:

```
Syntax: [options] subcommand <parameters> <parameters...>:
```

For example:

```
sudo -i
rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
```

With the example above, rclone will move the backup file stored in '`/data/tmp/ccv-center-backup/`' to the `remote drive 'lab_sftp'`.

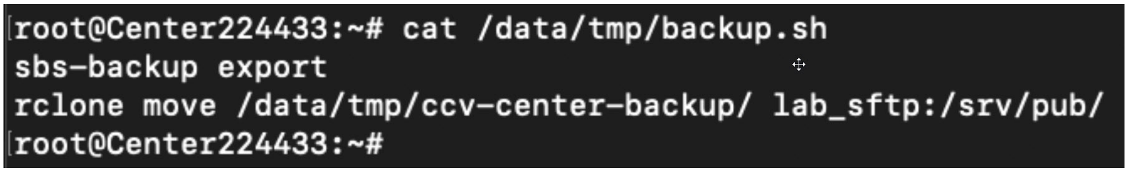
Bash Script

You can use bash script to execute the two necessary commands mentioned below:

- Generate the backup
- Transfer the backup archive to a remote location

For example:

```
sbs-backup export

rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
```



```
[root@Center224433:~# cat /data/tmp/backup.sh
sbs-backup export
rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
[root@Center224433:~#
```

Cron

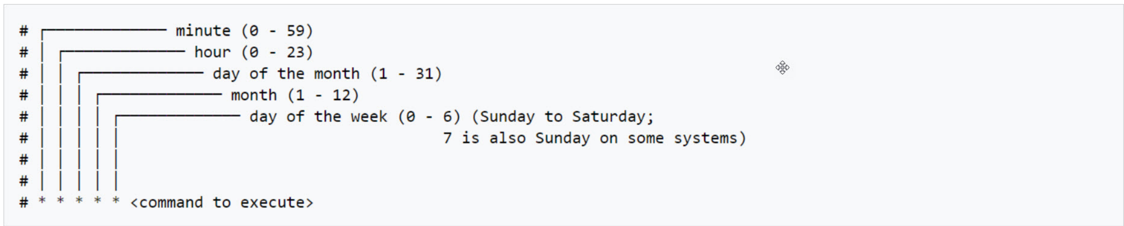
You can schedule a bash script using cron to back up Cyber Vision data and send the backup file to a remote drive.

Usages are as follows:

1. Edit crontab launching the command:
   - `crontab -e`

     : It allows you to edit the crontab file using the vi editor, enabling you to make modifications.

2. Add the command mentioned bellow::
   - `00 01 * * 6 bash /data/tmp/backup.sh`



```
# ┌───────────── minute (0 - 59)
# │ ┌───────────── hour (0 - 23)
# │ │ ┌───────────── day of the month (1 - 31)
# │ │ │ ┌───────────── month (1 - 12)
# │ │ │ │ ┌───────────── day of the week (0 - 6) (Sunday to Saturday;
# │ │ │ │ │                                   7 is also Sunday on some systems)
# │ │ │ │ │
# │ │ │ │ │
# * * * * * <command to execute>
```