Cisco Cyber Vision Center VM Installation Guide, Release 5.3.x

First Published: 2021-01-01

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 installation guide shows how to connect, configure and install Cisco Cyber Vision on a virtual machine running on VMware ESXi, Microsoft Hyper-V, and Nutanix.

You will also find the upgrade procedures for an architecture with a Global Center and for an architecture with one Center only.

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

Information and characteristics

Information and Characteristics

The Cisco Cyber Vision solution can have a 2-tier or 3-tier architecture made of:

- **Edge sensors** which are installed in the industrial network. These sensors are dedicated to capture network traffic, decode protocols using the Cisco Deep Packet Inspection engine and send meaningful information to the Cisco Cyber Vision Center.
- The Cisco Cyber Vision **Center**, a central platform gathering data from all the Edge Sensors and acting as the monitoring, detection and management platform for the whole solution.
- Optionally, a third-tier **Global Center** to which all Centers are connected, to provide a central view of all Centers deployed within an organization for alerting, reporting and management functions.

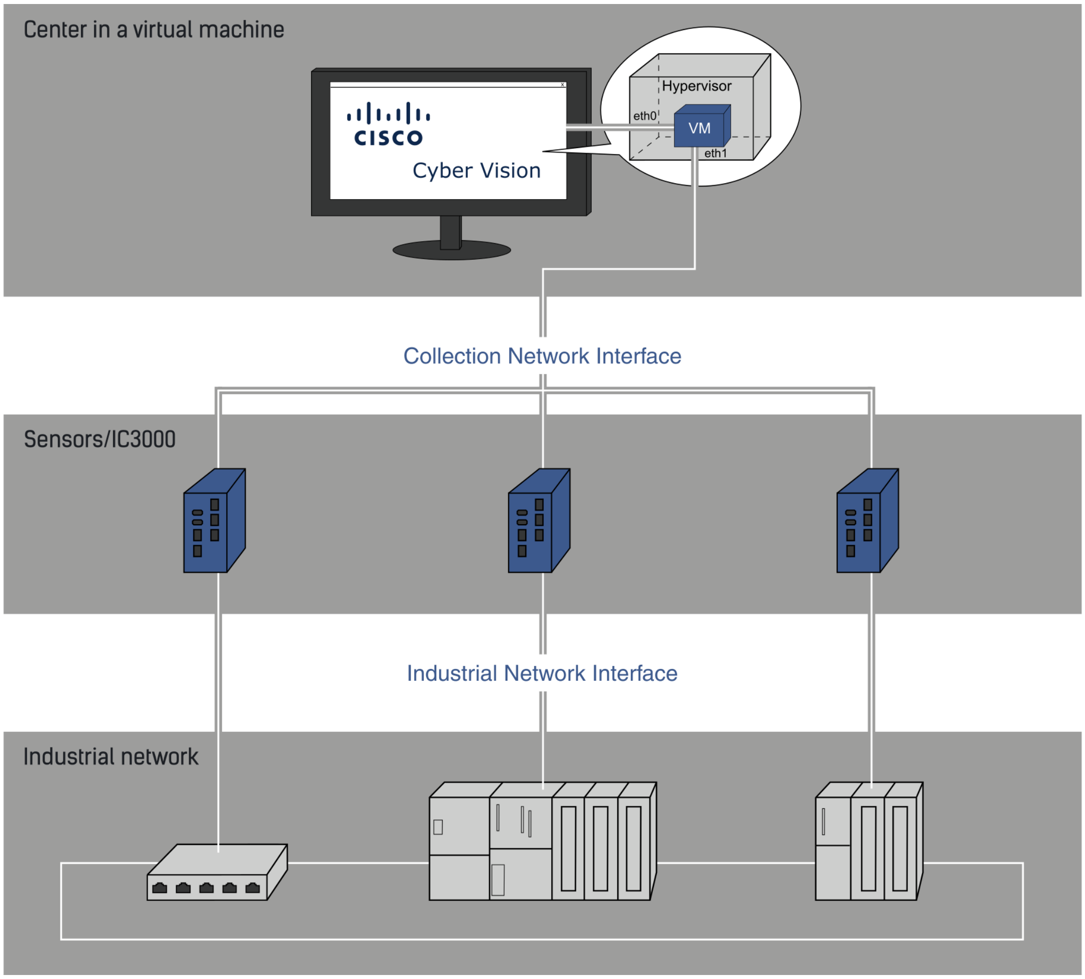
During the installation of the Center, you will have the opportunity to set up Center data synchronization to a Global Center. However, if you choose to set up a global infrastructure, you must install the Global Center first, then the Centers, and finally, the sensors.

Networks or segments involved

From Cisco Cyber Vision perspective, three important networks will be involved with the platform:

- The **Administration network**, used to access the Center User Interface (UI) and interact with authorized external services (NTP, DNS, API, SIEM, etc.).
- The **Collection network**, used to manage all Cisco Cyber Vision sensors. This network must be isolated from the operational traffic plant (separated VLAN/subnet).
- The **Acquisition/Industrial network**, used for all industrial plant traffic and/or external interconnection under consideration that will be analyzed by the sensors (SPAN traffic collected).

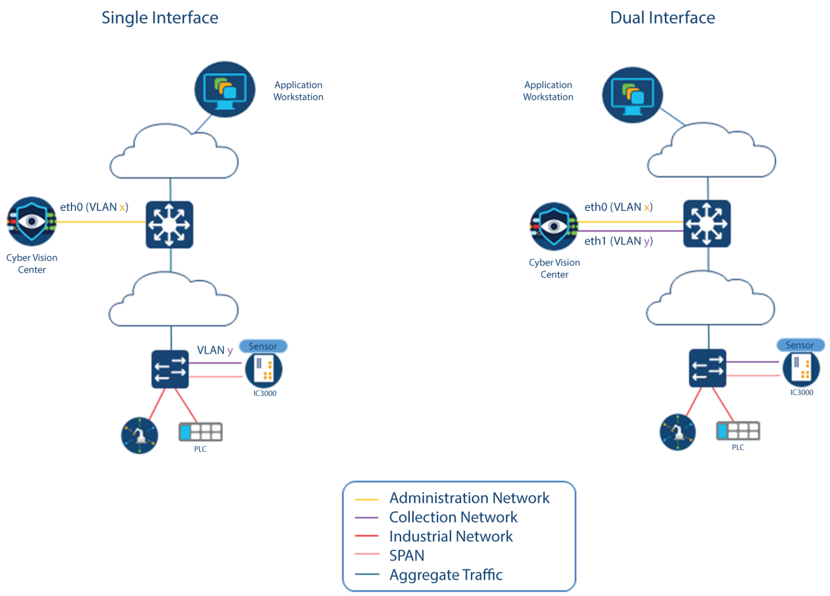
Example of a Cisco Cyber Vision installation (without Global Center):


Center in a virtual machine
cisco
Cyber Vision
Hypervisor
eth0
VM
eth1
Collection Network Interface
Sensors/IC3000
Industrial Network Interface
Industrial network

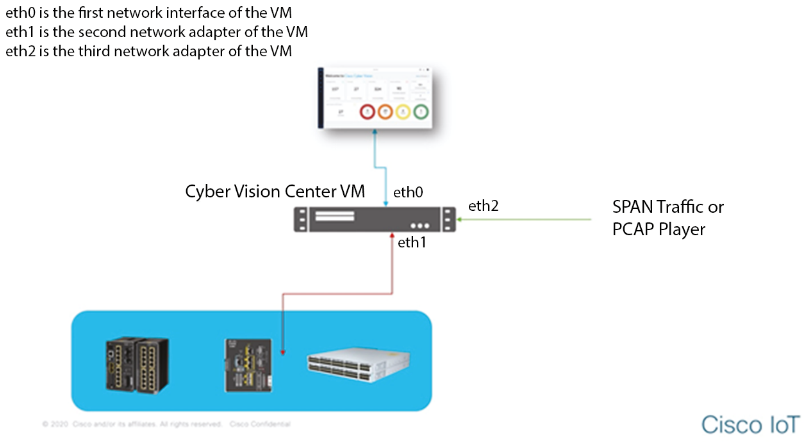
Configuring single or dual interface (not applicable to a Global Center)

For security reasons, it is recommended to use the Center on **two separate networks**, respectively connected to the following interfaces:

- The **Administration network interface (eth0)**, which gives access to the user interface.
- The **Collection network interface (eth1)**, which connects the Center to the sensors.



- An additional interface dedicated to DPI (eth2) is required to deploy a Center with sensor function on ESXi.


eth0 is the first network interface of the VM
eth1 is the second network adapter of the VM
eth2 is the third network adapter of the VM
Cyber Vision Center VM
eth0
eth2
eth1
SPAN Traffic or
PCAP Player
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Cisco IoT

However, in case of incompatibility with the industrial network infrastructure or for limited environments, you can use a single network interface (eth0).

Refer to the Cisco Cyber Vision Architecture Guide for more information about defining Cisco Cyber Vision environment configuration.

CHAPTER 3

Requirements for installation

Installation Prerequisites

Ensure the following conditions are met before installing Cisco Cyber Vision as a virtual machine.

Supported Hypervisors

Use one of these hypervisors.

- VMware vSphere 6.x or later
- Microsoft Hyper-V Server 2016 or later
- Nutanix Acropolis OS 6.10 or later

Note The hypervisor must have permissions configured to create a new virtual machine.

Virtual Machine Sizing

Minimum (up to 500 components)

- CPU: Intel Xeon, 8 cores
- RAM: 16 GB
- Storage: 500 GB SSD

Recommended (10,000 components without Center DPI):

- CPU: Intel Xeon, 10 cores
- RAM: 32 GB
- Storage: 1 TB SSD, RAID-10

For over 10,000 components or with Center DPI:

- CPU: Intel Xeon, 16 cores
- RAM: 64 GB
- Storage: 1 TB SSD, RAID-10

Network Requirements

IP Addresses

- 1–2 IP addresses for the Center, based on single or dual interface configuration:
  - Single interface: One IP for web interface and SSH administration.
  - Dual interface: One IP for protocol data from sensors (Collection network) and one for web interface/SSH (Administration network).
  - One IP address per sensor, ideally on a dedicated LAN or VLAN (Industrial network interface). Not applicable for Global Center.
  - An additional interface for DPI if deploying a Center with sensor functionality on ESXi.
- NTP Server: Accessible from the Center (typically configured via a router).
- Machine Name: A unique name, configured in DNS or on each client, required for secure communication between clients (users or APIs) and the Center.

CHAPTER 4

Install the Virtual Center

To install Cisco Cyber Vision Center, follow these steps:

1. Retrieve the Cisco Cyber Vision installation file.
2. Create a virtual machine.
   - For VMware ESXi: Create a virtual machine and deploy the Cisco Cyber Vision OVA file.
   - For Microsoft Hyper-V: Create a virtual machine, configure the disk size, and map the required network interfaces.
   - For Nutanix: Import the OVA file in Nutanix via PRISM Central.
3. Configure the Cisco Cyber Vision Center to finalize the installation.

Retrieve the installation file

Before starting the VM installation, you must retrieve the virtual machine installation ova file.

To retrieve the virtual machine installation file:

Procedure

Step 1 Access Cisco Cyber Vision Software Download platform.

Step 2 Download the latest OVA file for your hypervisor. OVA files with the DPI option are also available.

To verify that the file you just downloaded is healthy, it is recommended to use the SHA512 checksum provided by Cisco.

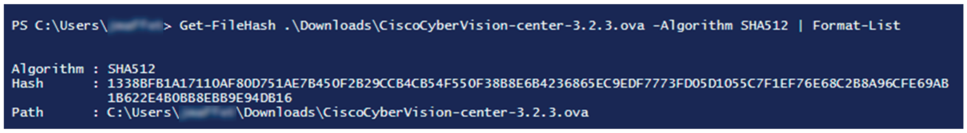
To do so (Windows users):

Step 3 Access Cisco Cyber Vision download page.

Step 4 Download the file.

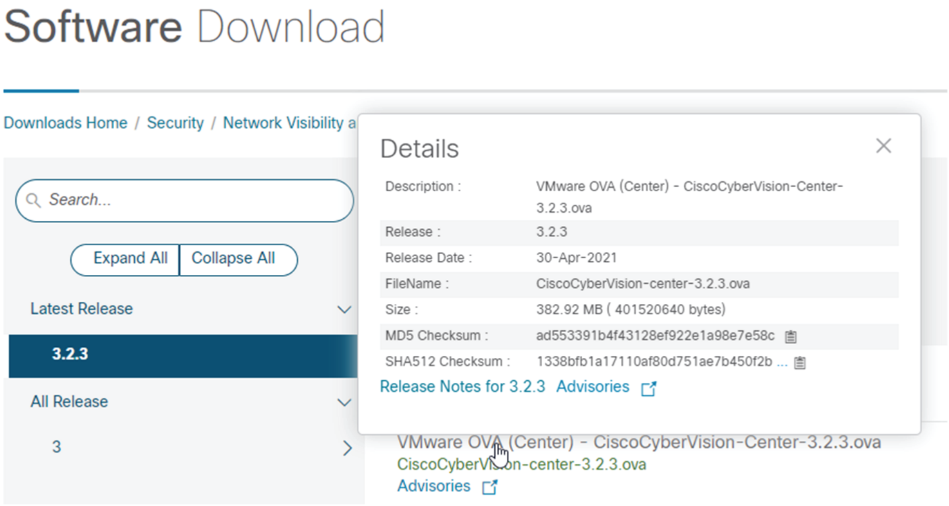
Step 5 Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

```
Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List
```



```
PS C:\Users\[redacted]> Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List

Algorithm : SHA512
Hash      : 1338BFB1A17110AF80D751AE7B450F2B29CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
            1B622E4B0BB8EBB9E94DB16
Path      : C:\Users\[redacted]\Downloads\CiscoCyberVision-center-3.2.3.ova
```

Step 6 In the download page, mouse over the file and copy the SHA512 checksum.



Software Download

Downloads Home / Security / Network Visibility a

Details

Description :	VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova
Release :	3.2.3
Release Date :	30-Apr-2021
FileName :	CiscoCyberVision-center-3.2.3.ova
Size :	382.92 MB (401520640 bytes)
MD5 Checksum :	ad553391b4f43128ef922e1a98e7e58c
SHA512 Checksum :	1338bfb1a17110af80d751ae7b450f2b ...

Release Notes for 3.2.3 Advisories

VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova
CiscoCyberVision-center-3.2.3.ova
Advisories

Step 7 Compare both checksums.

- If both checksums are identical it means the file is healthy.
- If the checksums do not match try to download the file again.
- If, after downloading the file again the checksums still don’t match, please contact Cisco support.

ESXi

Create a Virtual Machine

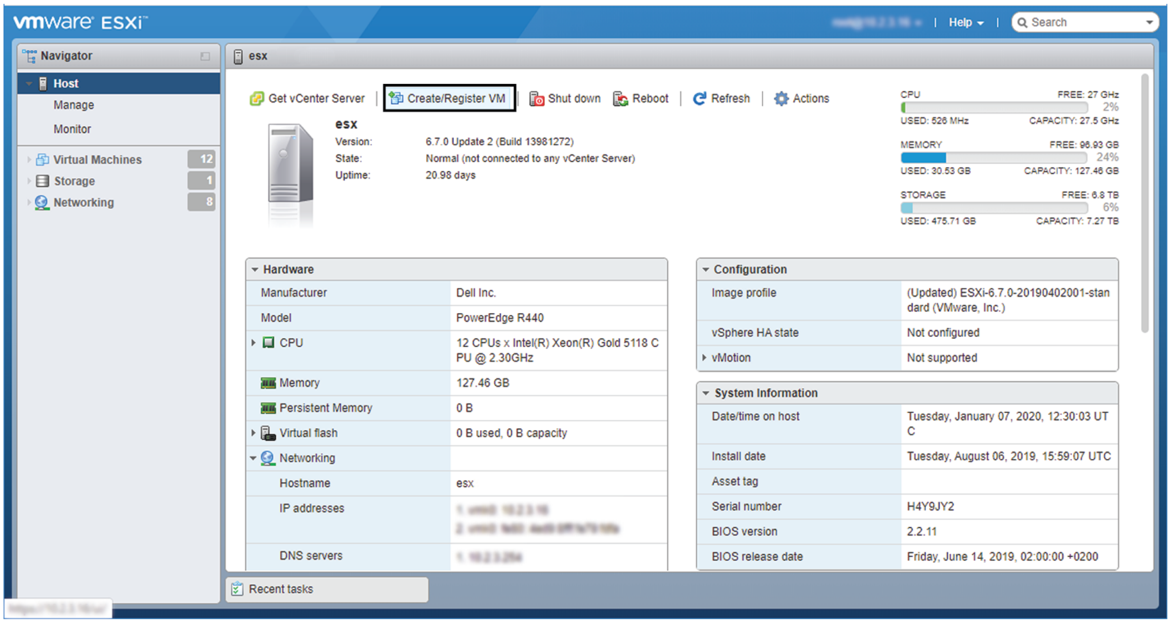
Before taking the steps below to create a VM on ESXi, **you must set two network interfaces** (the Administration and the Collection network interfaces), and a third if deploying a Center with DPI (the DPI network interface), accordingly to the infrastructure of the network. To do so, refer to VMware ESXi documentation.

To create the Virtual Machine and deploy Cisco Cyber Vision:

Procedure

Step 1 Login to VMware ESXi.

Step 2 Click Create/Register VM.



esx

Version: 6.7.0 Update 2 (Build 13981272)
State: Normal (not connected to any vCenter Server)
Uptime: 20.98 days

CPU FREE: 27 GHz 2% USED: 526 MHz CAPACITY: 27.5 GHz
MEMORY FREE: 96.93 GB 24% USED: 30.53 GB CAPACITY: 127.46 GB
STORAGE FREE: 6.8 TB 6% USED: 475.71 GB CAPACITY: 7.27 TB

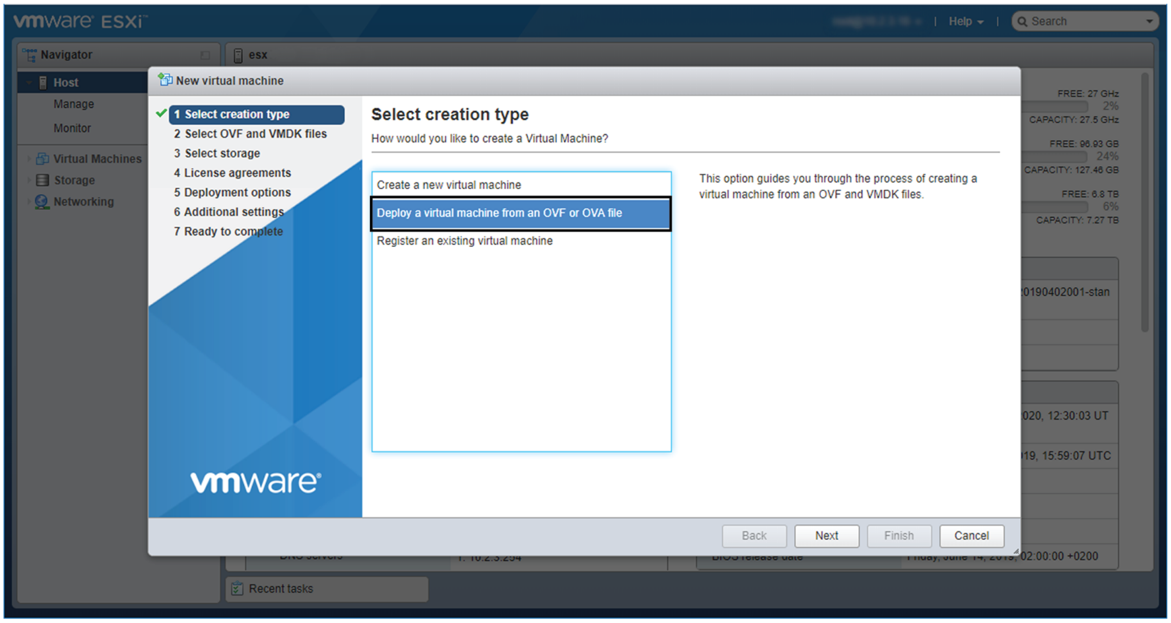
Hardware	
Manufacturer	Dell Inc.
Model	PowerEdge R440
CPU	12 CPUs x Intel(R) Xeon(R) Gold 5118 CPU @ 2.30GHz
Memory	127.46 GB
Persistent Memory	0 B
Virtual flash	0 B used, 0 B capacity
Networking	
Hostname	esx
IP addresses	[redacted]
DNS servers	[redacted]

Configuration	
Image profile	(Updated) ESXi-6.7.0-20190402001-standard (VMware, Inc.)
vSphere HA state	Not configured
vMotion	Not supported

System Information	
Date/time on host	Tuesday, January 07, 2020, 12:30:03 UTC
Install date	Tuesday, August 06, 2019, 15:59:07 UTC
Asset tag	
Serial number	H4Y9JY2
BIOS version	2.2.11
BIOS release date	Friday, June 14, 2019, 02:00:00 +0200

The wizard to create a new virtual machine opens.

Step 3 Click Deploy a virtual machine from an OVF or OVA file.



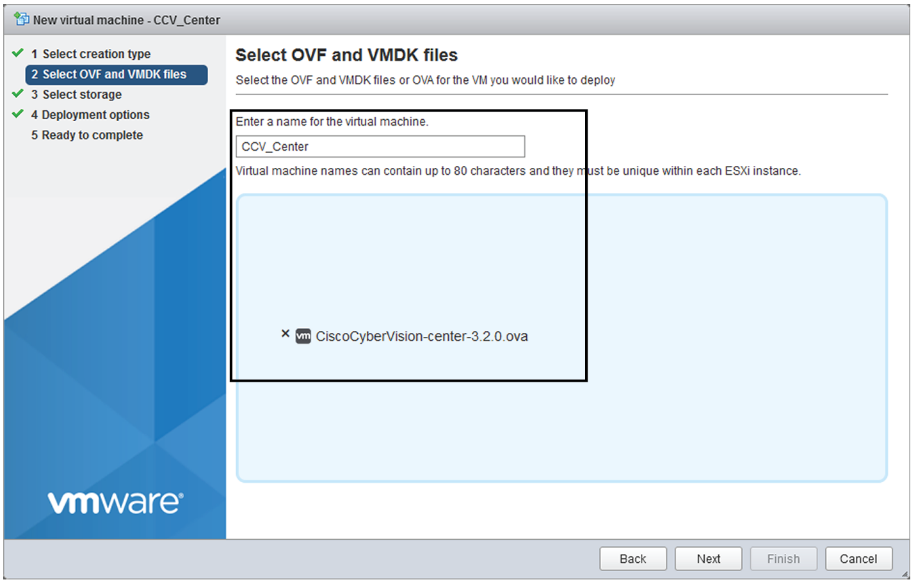
Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Step 4 Give a name to the virtual machine and select the Cisco Cyber Vision OVA file. Select the DPI OVA file to enable the sensor function on the Center VM.


New virtual machine - CCV_Center

Select OVF and VMDK files

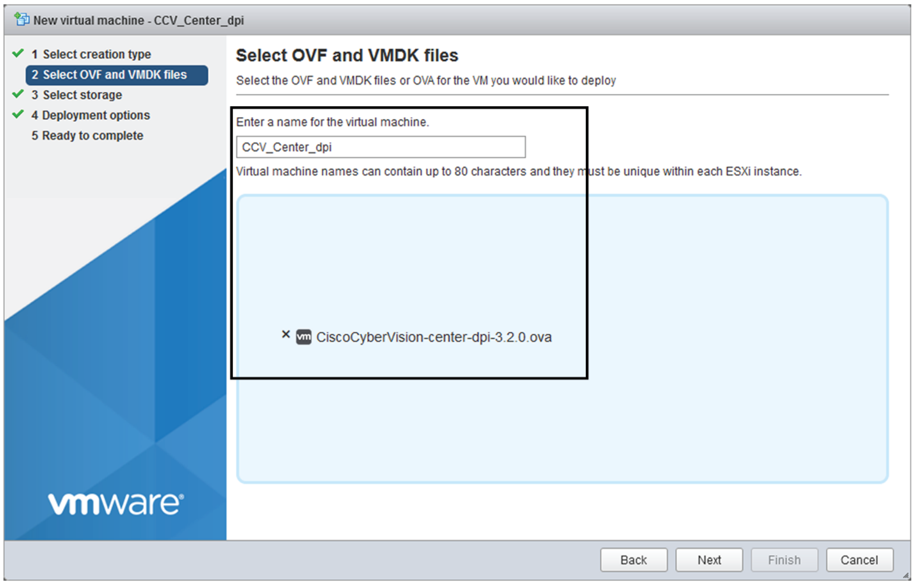
Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

CCV_Center

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

CiscoCyberVision-center-3.2.0.ova


New virtual machine - CCV_Center_dpi

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

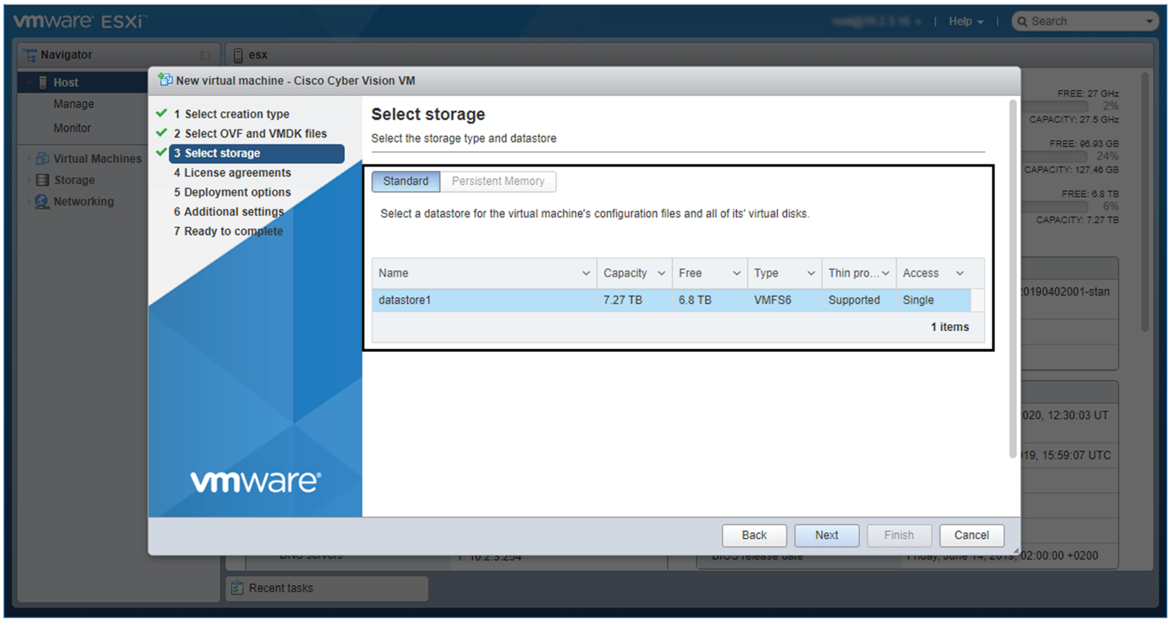
Enter a name for the virtual machine.

CCV_Center_dpi

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

CiscoCyberVision-center-dpi-3.2.0.ova

Step 5 Select a disk with sufficient storage. Refer to Installation Prerequisites, on page 7.



New virtual machine - Cisco Cyber Vision VM

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the storage type and datastore

Standard | Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	7.27 TB	6.8 TB	VMFS6	Supported	Single

1 items

Back | Next | Finish | Cancel

Step 6 Map the network interfaces you have previously created to the VM's ports **(1)**, as shown below:

- The Administration network interface as eth0.
- The Collection network interface as eth1.
- If deploying a Center with DPI, the DPI network interface as eth2.

Step 7 Set disk provisioning as Thin **(2)**.

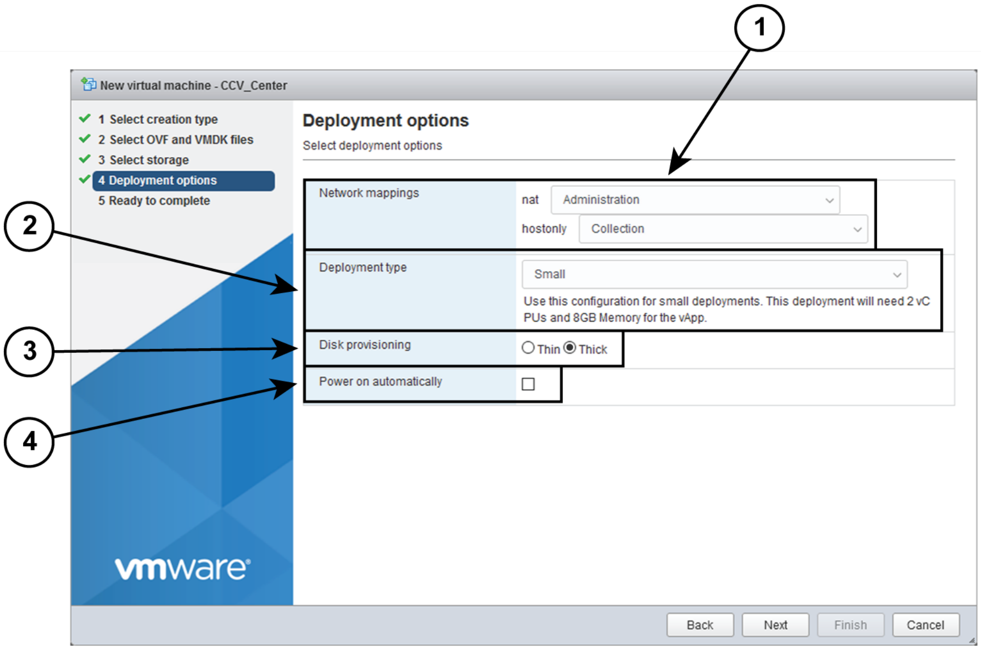
Step 8 Set the Deployment type as Small, Medium or Large **(3)**. The deployment size for an OVA DPI file is Large by default.

Small: Intel Xeon, 8 cores, 16GB RAM

Medium: Intel Xeon, 10 cores, 32GB RAM

Large: Intel Xeon, 16 cores, 64GB RAM

Step 9 Disable the virtual machine's automatic start **(4)**.



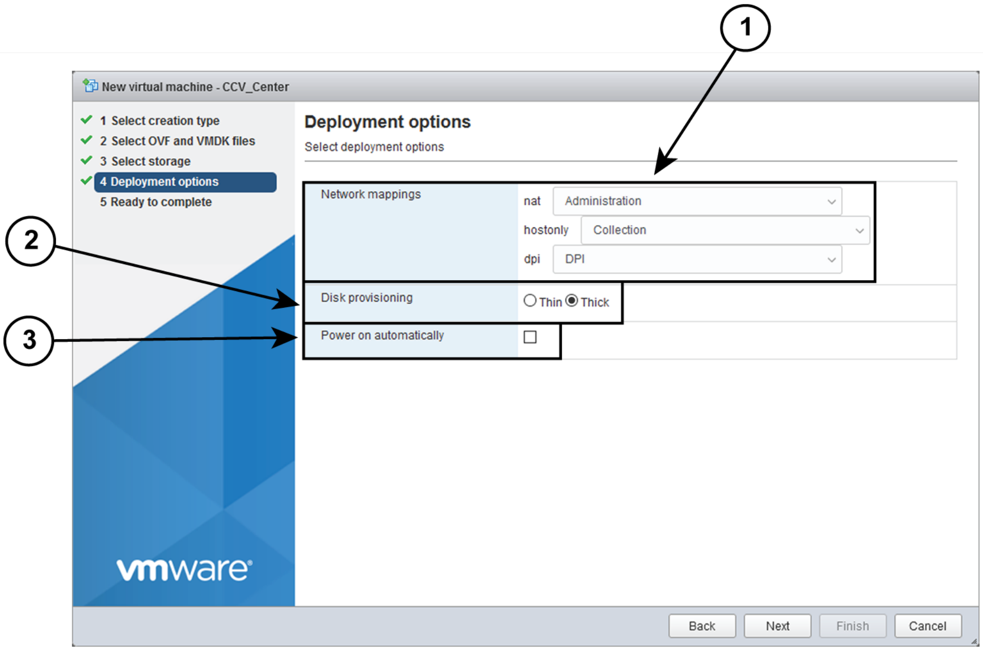
New virtual machine - CCV_Center

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

Network mappings	nat: Administration hostonly: Collection
Deployment type	Small Use this configuration for small deployments. This deployment will need 2 vCPUs and 8GB Memory for the vApp.
Disk provisioning	○ Thin ● Thick
Power on automatically	□



New virtual machine - CCV_Center

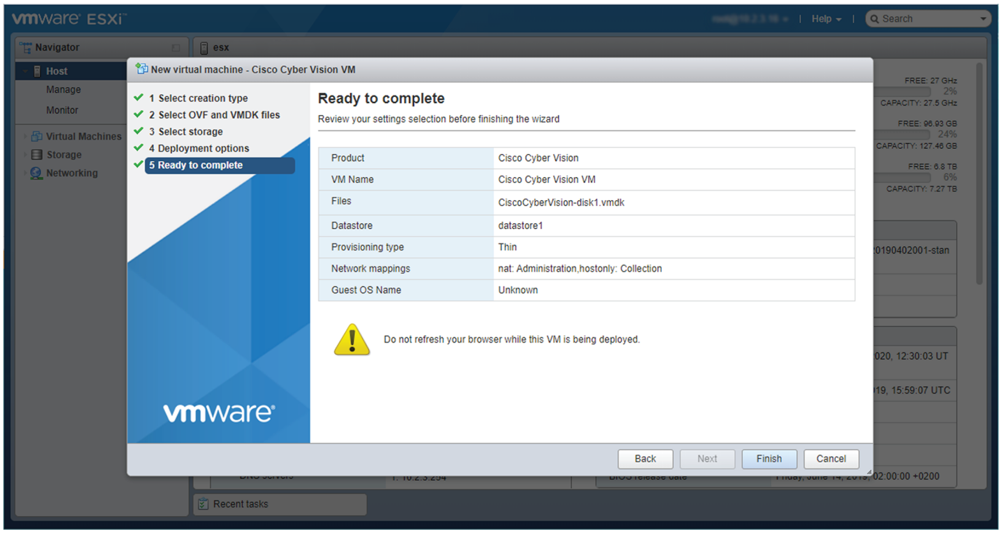
- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

Network mappings	nat: Administration hostonly: Collection dpi: DPI
Disk provisioning	○ Thin ● Thick
Power on automatically	□

Step 10 Check the new VM's settings before clicking Finish.



New virtual machine - Cisco Cyber Vision VM

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

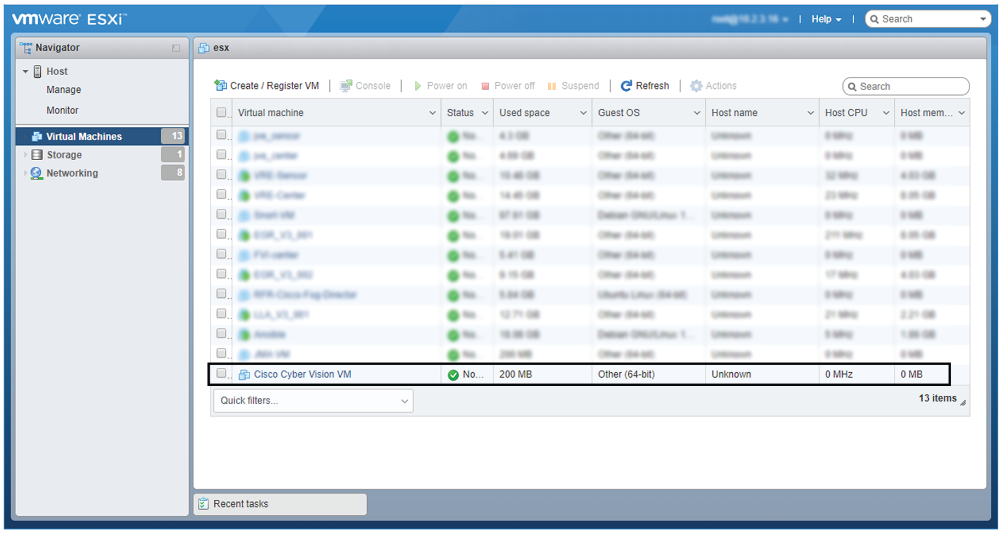
Ready to complete

Review your settings selection before finishing the wizard

Product	Cisco Cyber Vision
VM Name	Cisco Cyber Vision VM
Files	CiscoCyberVision-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	nat: Administration,hostonly: Collection
Guest OS Name	Unknown

Do not refresh your browser while this VM is being deployed.

Your new VM is displayed in the virtual machine list.



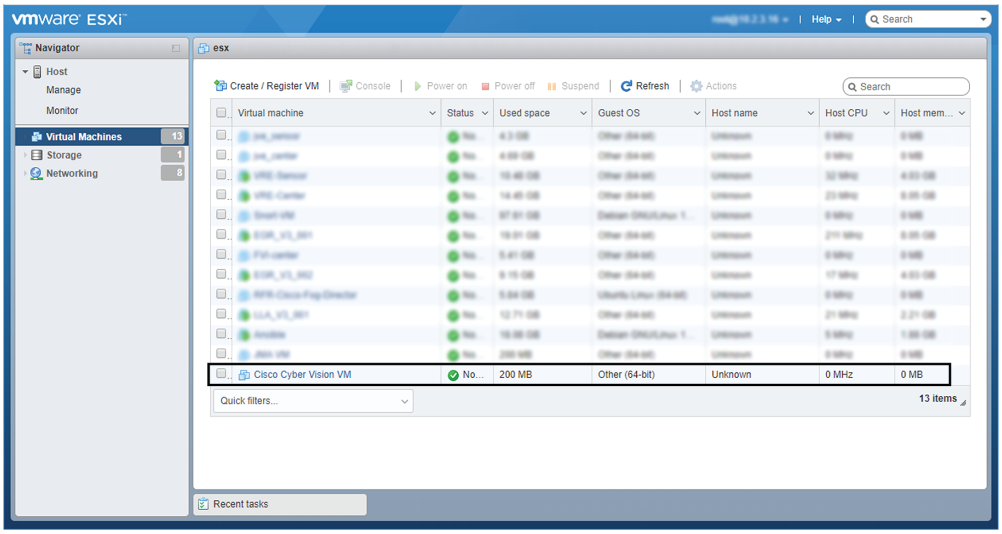
Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host mem...
Cisco Cyber Vision VM	✓ No...	200 MB	Other (64-bit)	Unknown	0 MHz	0 MB

13 items

Boot the Virtual Machine

After creating the VM, you can proceed to its first boot.

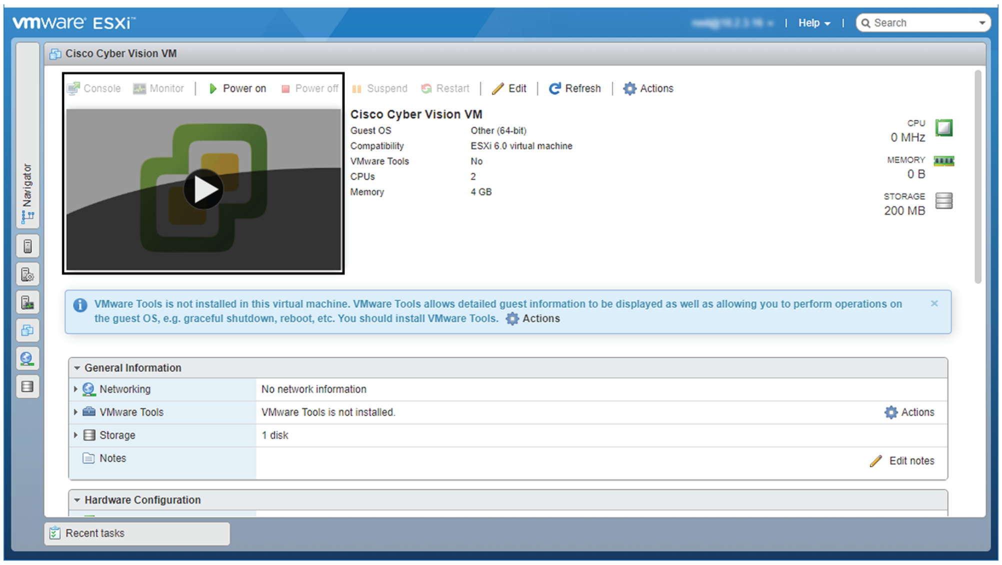
1. Click the VM in the list.



Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host mem...
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	No...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Cisco Cyber Vision VM	No...	200 MB	Other (64-bit)	Unknown	0 MHz	0 MB

13 items

2. Power on the VM.



Cisco Cyber Vision VM

Guest OS	Other (64-bit)
Compatibility	ESXi 6.0 virtual machine
VMware Tools	No
CPUs	2
Memory	4 GB

CPU 0 MHz
MEMORY 0 B
STORAGE 200 MB

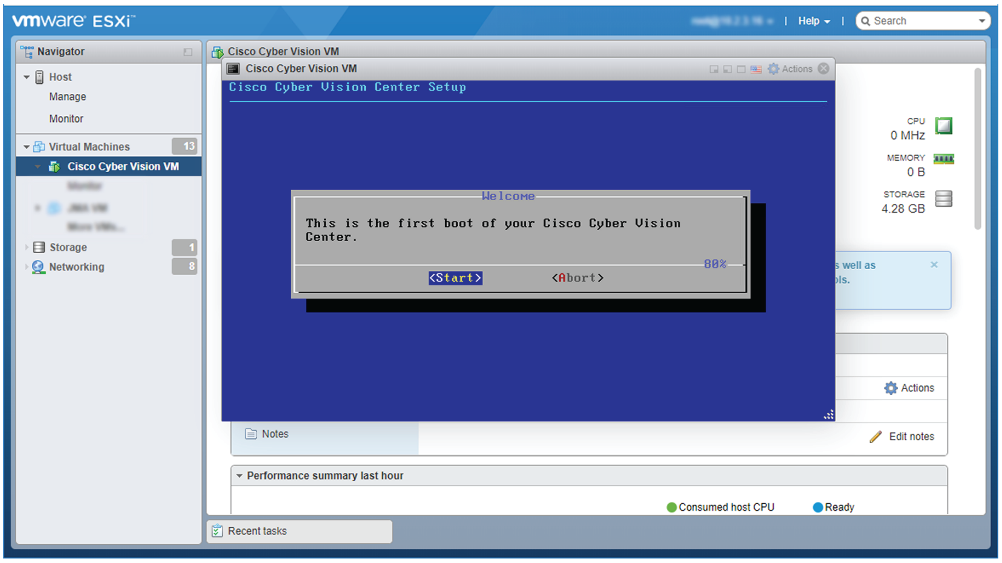
VMware Tools is not installed in this virtual machine. VMware Tools allows detailed guest information to be displayed as well as allowing you to perform operations on the guest OS, e.g. graceful shutdown, reboot, etc. You should install VMware Tools. Actions

General Information

Networking	No network information
VMware Tools	VMware Tools is not installed. Actions
Storage	1 disk
Notes	Edit notes

Hardware Configuration

3. Wait a few moments for the VM initiation to complete. The following screen is displayed:



```
Cisco Cyber Vision Center Setup

                      Welcome
This is the first boot of your Cisco Cyber Vision
Center.
                                          80%
        <Start>          <Abort>
```

4. Press Ctrl+Alt to retrieve the control of your keyboard and mouse.

   The Virtual Center is now ready for basic configuration.

Hyper-V

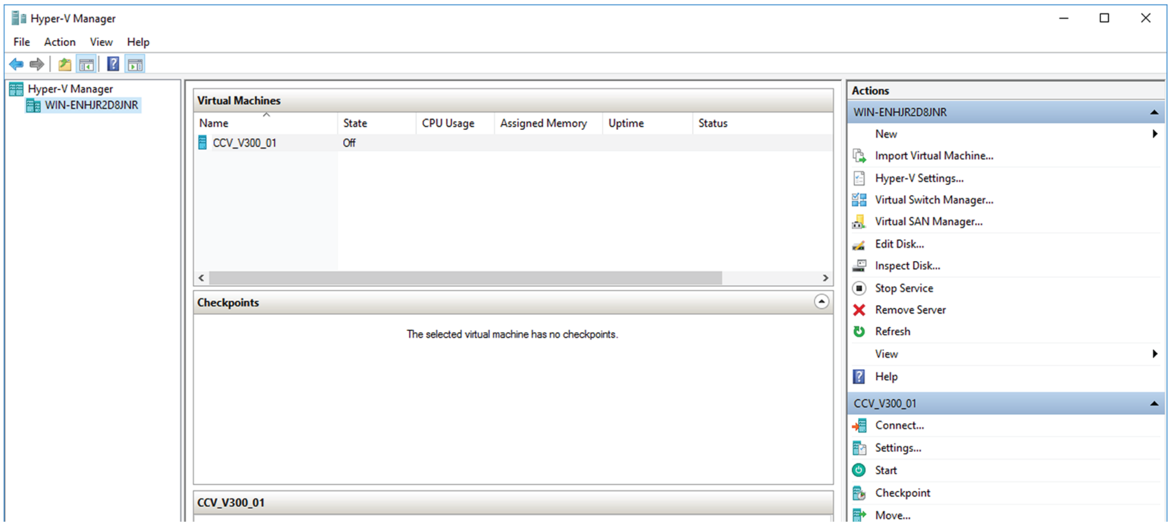
Create a Virtual Machine

To create a new VM:

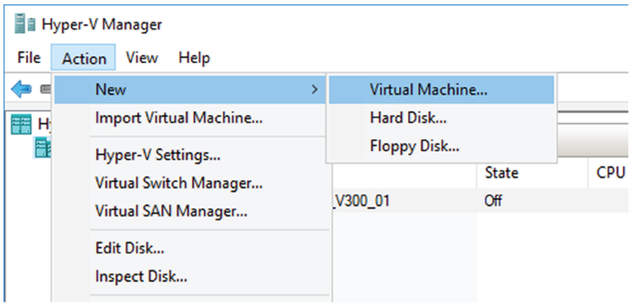
Procedure

Step 1 Open Hyper-V Manager.

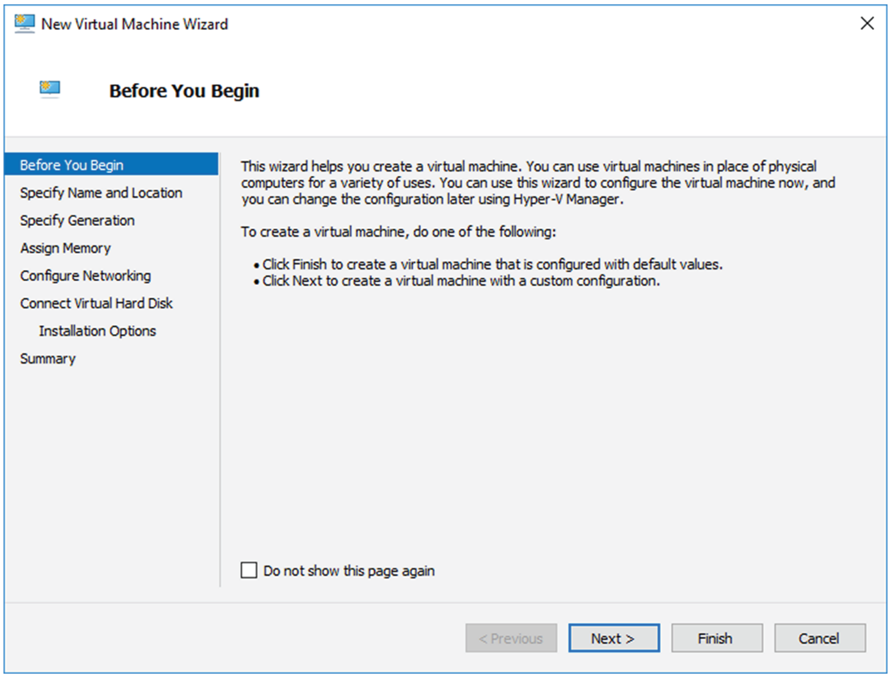
The following home screen appears:



Step 2 Access the New Virtual Machine Wizard by clicking Action > New > Virtual Machine.



The New Virtual Machine Wizard is displayed.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

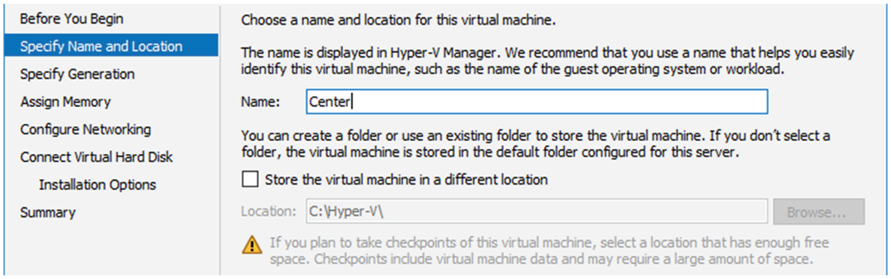
- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

□ Do not show this page again

Step 3 Click Next to start.

Step 4 Give the new VM a name (e.g. 'Center').

Step 5 If necessary, give the Virtual Center a different location on the server than the one set by default. In any case, the location chosen must have enough remaining space in case you plan to create snapshots (i.e. VM backups).



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Center

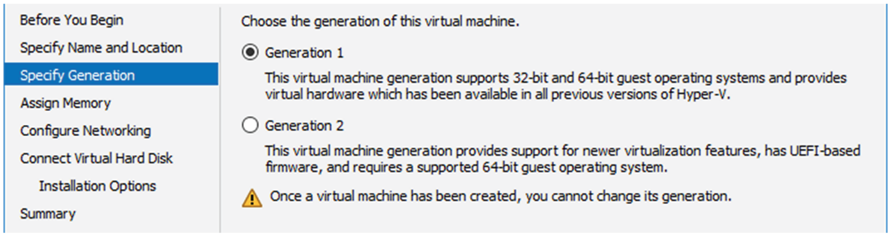
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

□ Store the virtual machine in a different location

Location: C:\Hyper-V\

⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

Step 6 Set the VM as Generation 1.



Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

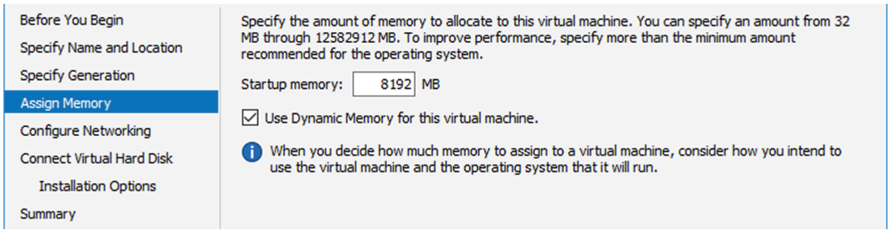
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

Step 7 Assign memory to the VM.

Note
The minimum configuration required is 8192 MB.



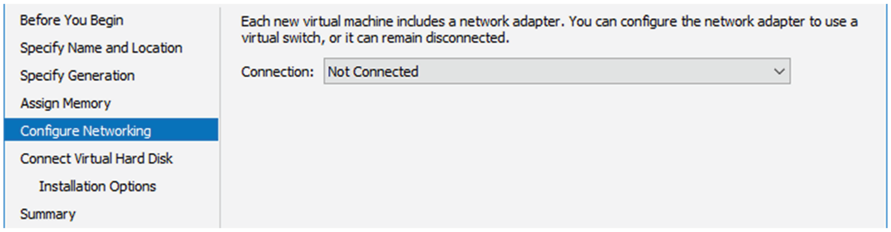
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 8192 MB

☑ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

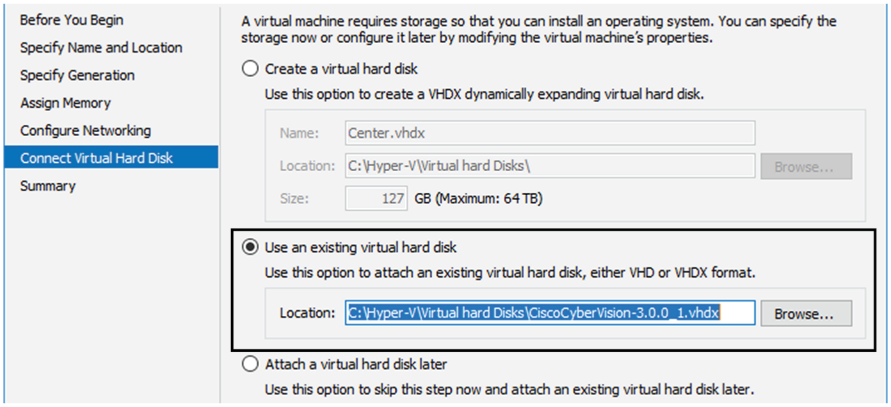
Step 8 Leave the network connection disconnected.



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

Step 9 Select 'Use an existing hard disk' and choose the VHDX file.



A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: Center.vhdx

Location: C:\Hyper-V\Virtual hard Disks\ Browse...

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

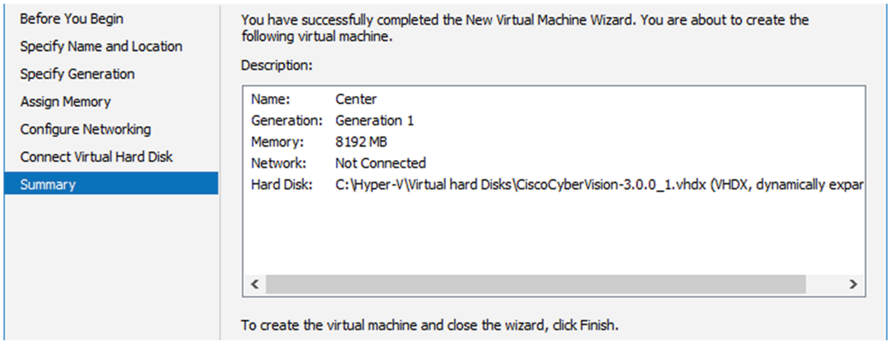
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Hyper-V\Virtual hard Disks\CiscoCyberVision-3.0.0_1.vhdx Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

Step 10 Click 'Finish' to create the VM and close the wizard.



You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name: Center
Generation: Generation 1
Memory: 8192 MB
Network: Not Connected
Hard Disk: C:\Hyper-V\Virtual hard Disks\CiscoCyberVision-3.0.0_1.vhdx (VHDX, dynamically expar

To create the virtual machine and close the wizard, click Finish.

The Virtual Center created is displayed inside Hyper-V Manager home screen.

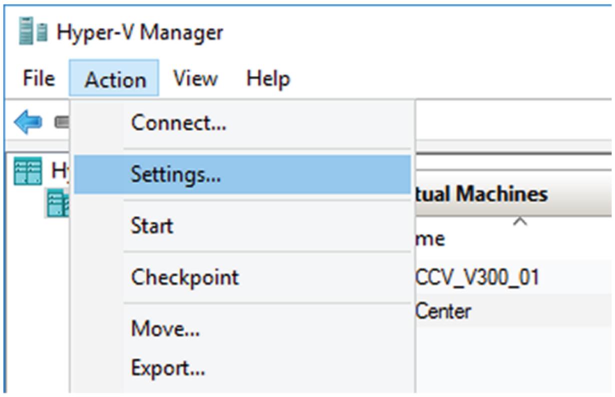
Configure the disk size

To configure the disk size:

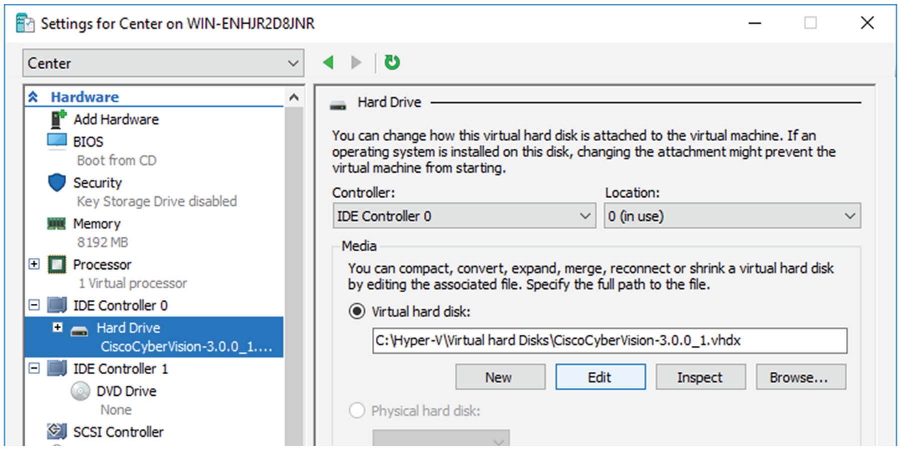
Procedure

Step 1 In the Hyper-V Manager select the Center.

Step 2 Click **Action** > **Settings**.



Step 3 Click **Hard Drive**, then **Edit**.



Settings for Center on WIN-ENHJR2D8JNR

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 0 (in use)

Media

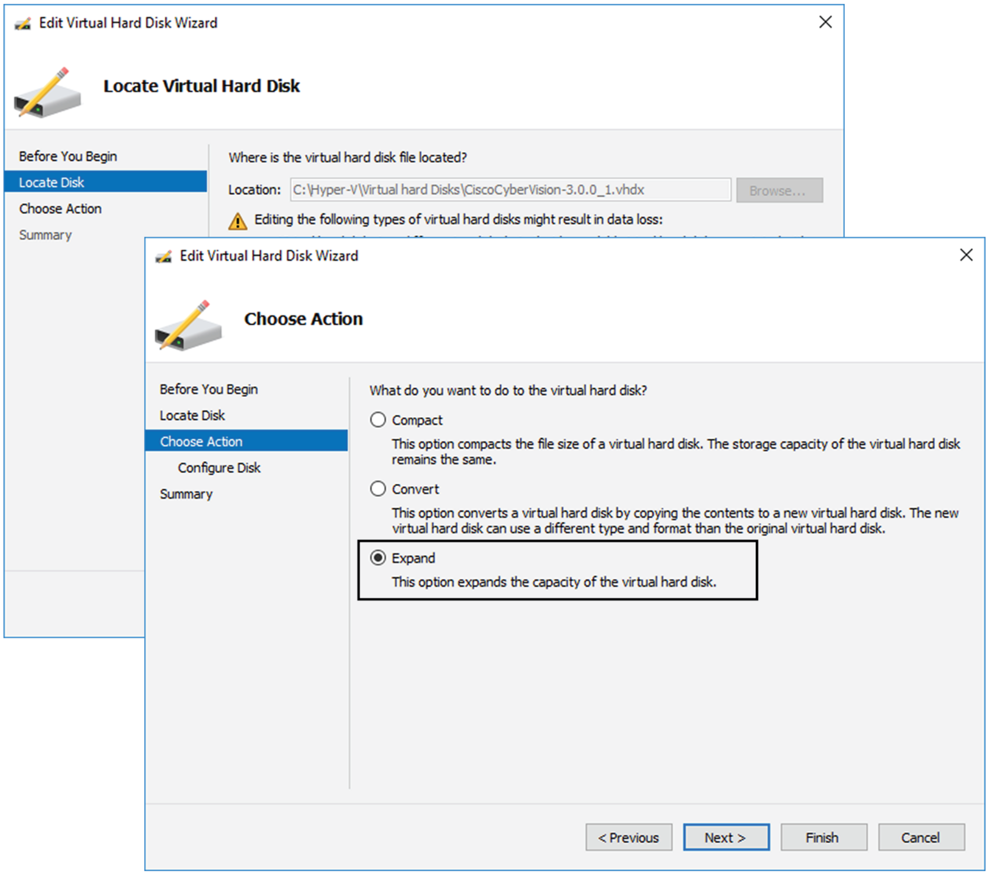
You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk: C:\Hyper-V\Virtual hard Disks\CiscoCyberVision-3.0.0_1.vhdx

○ Physical hard disk:

The Edit Virtual Hard Disk Wizard displays.

Step 4 Click **Next** to proceed until the Choose Action tab.



Edit Virtual Hard Disk Wizard

Locate Virtual Hard Disk

Where is the virtual hard disk file located?

Location: C:\Hyper-V\Virtual hard Disks\CiscoCyberVision-3.0.0_1.vhdx

Editing the following types of virtual hard disks might result in data loss:

Edit Virtual Hard Disk Wizard

Choose Action

What do you want to do to the virtual hard disk?

○ Compact

This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard disk remains the same.

○ Convert

This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk.

● Expand

This option expands the capacity of the virtual hard disk.

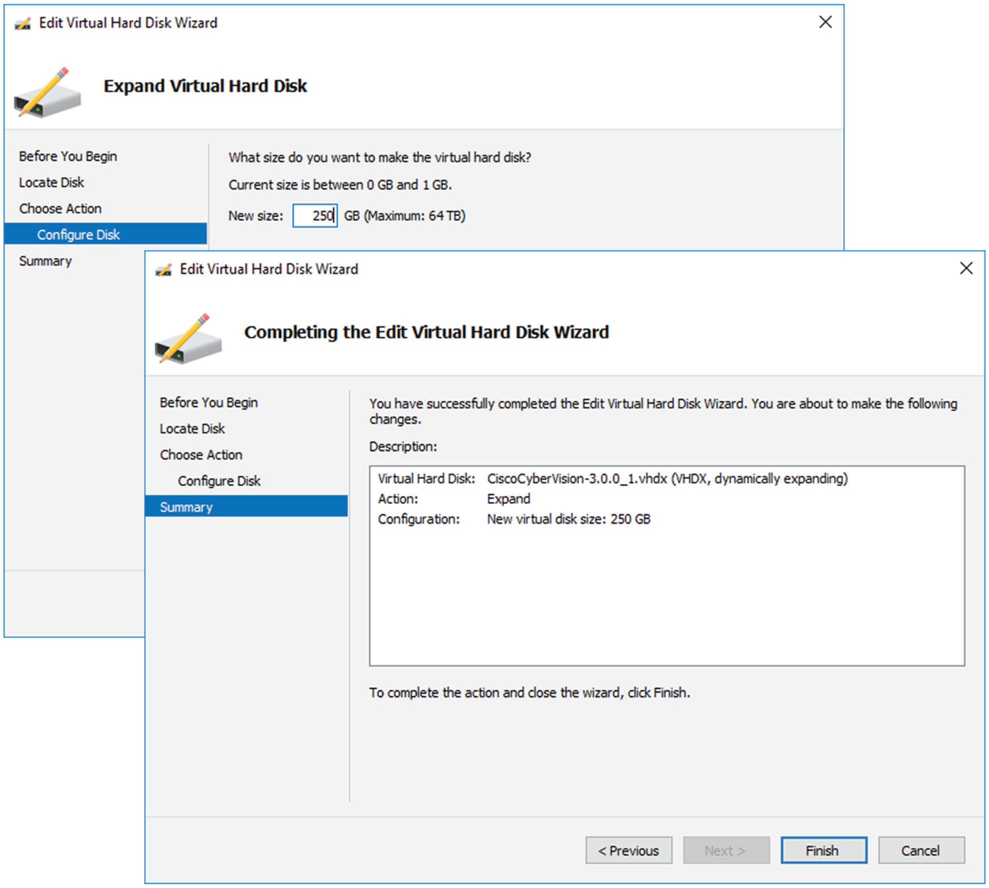
Step 5 As you are on the Choose Action tab select the **Expand** option.

Step 6 Configure a new size for the virtual hard disk.

It is recommended:

- that you set the minimum size at 100GB for a demo installation with small amounts of data.
- that you set the minimum size at 250GB for a cartography.
- that you set the minimum size at 800GB for a Center with sync or 1.5TB for a Global Center for a production environment.

  The size you set here is a minimum. The virtual drive will expand as data is written on the virtual disk.



Expand Virtual Hard Disk

What size do you want to make the virtual hard disk?

Current size is between 0 GB and 1 GB.

New size: 250 GB (Maximum: 64 TB)

Completing the Edit Virtual Hard Disk Wizard

You have successfully completed the Edit Virtual Hard Disk Wizard. You are about to make the following changes.

Description:

Virtual Hard Disk:	CiscoCyberVision-3.0.0_1.vhdx (VHDX, dynamically expanding)
Action:	Expand
Configuration:	New virtual disk size: 250 GB

To complete the action and close the wizard, click Finish.

Step 7 Click **Finish**.

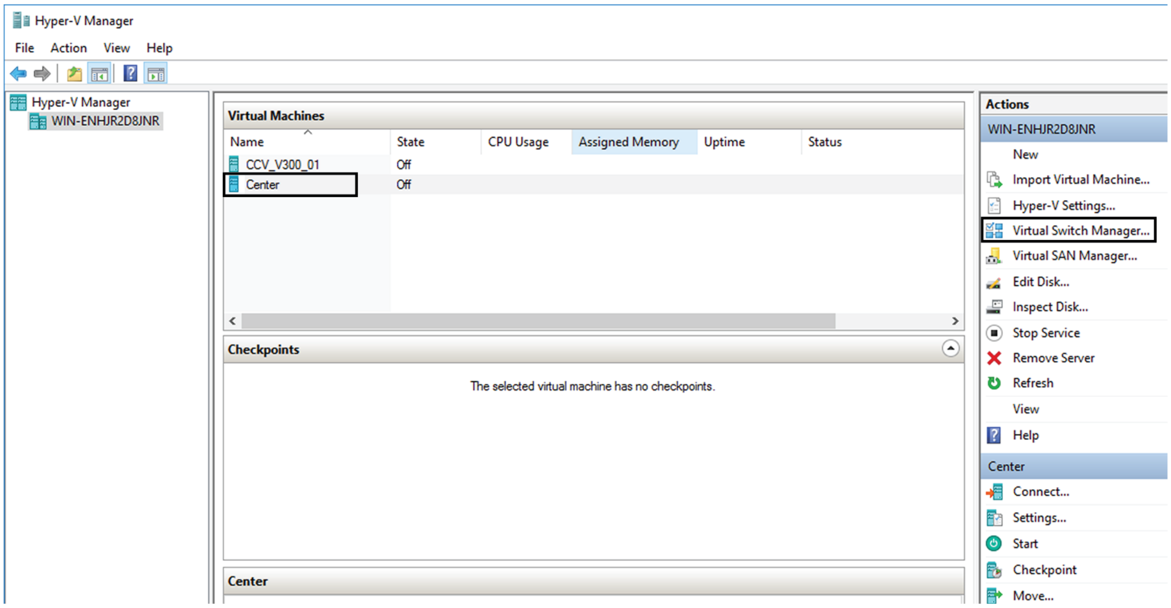
Create the network interfaces

To create the Admin and Collection network interfaces:

Procedure

Step 1 Select the Center.

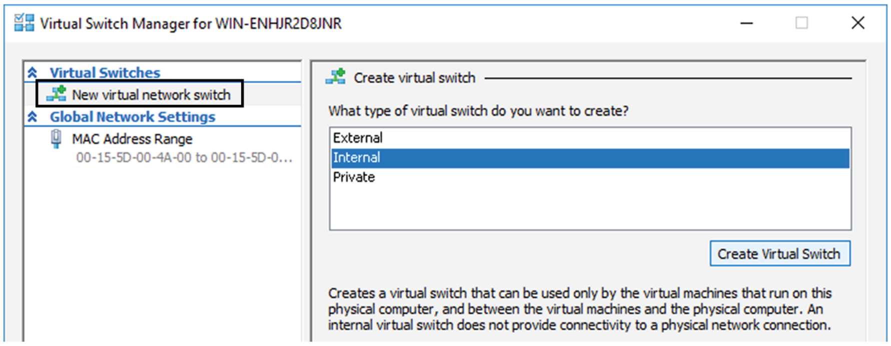
Step 2 On the Actions menu, open the Virtual Switch Manager.



Name	State	CPU Usage	Assigned Memory	Uptime	Status
CCV_V300_01	Off				
Center	Off				

The selected virtual machine has no checkpoints.

The Virtual switch manager opens.



What type of virtual switch do you want to create?

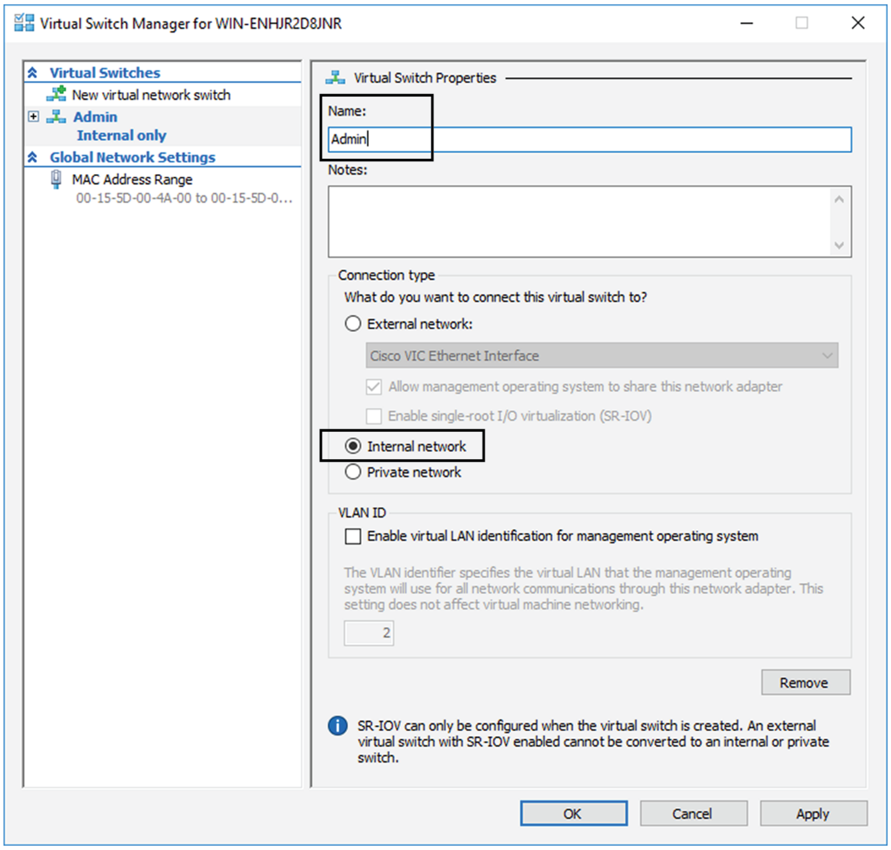
Creates a virtual switch that can be used only by the virtual machines that run on this physical computer, and between the virtual machines and the physical computer. An internal virtual switch does not provide connectivity to a physical network connection.

Step 3 Click 'New virtual network switch'.

Step 4 The new virtual switch displays.

Step 5 Name it 'Admin'.

Step 6 Select 'Internal network'.



Virtual Switch Manager for WIN-ENHJR2D8JNR

- Virtual Switches
  - New virtual network switch
  - Admin
    Internal only
- Global Network Settings
  - MAC Address Range
    00-15-5D-00-4A-00 to 00-15-5D-0...

Virtual Switch Properties

Name: Admin

Notes:

Connection type

What do you want to connect this virtual switch to?

○ External network:

Cisco VIC Ethernet Interface

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

● Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

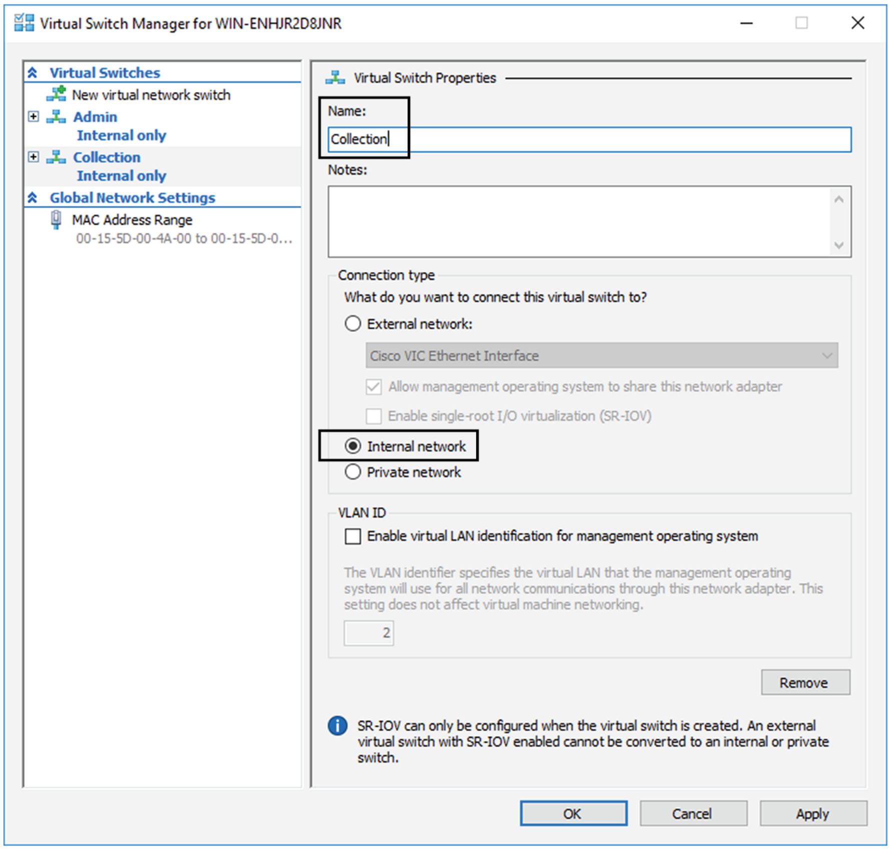
Remove

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

OK Cancel Apply

Step 7 Create a second virtual switch and name it 'Collection'.

Step 8 Select 'Internal network'.



Virtual Switch Manager for WIN-ENHJR2D8JNR

Virtual Switches
- New virtual network switch
- Admin
  Internal only
- Collection
  Internal only

Global Network Settings
- MAC Address Range
  00-15-5D-00-4A-00 to 00-15-5D-0...

Virtual Switch Properties

Name: Collection

Notes:

Connection type

What do you want to connect this virtual switch to?

○ External network:

Cisco VIC Ethernet Interface

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

● Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

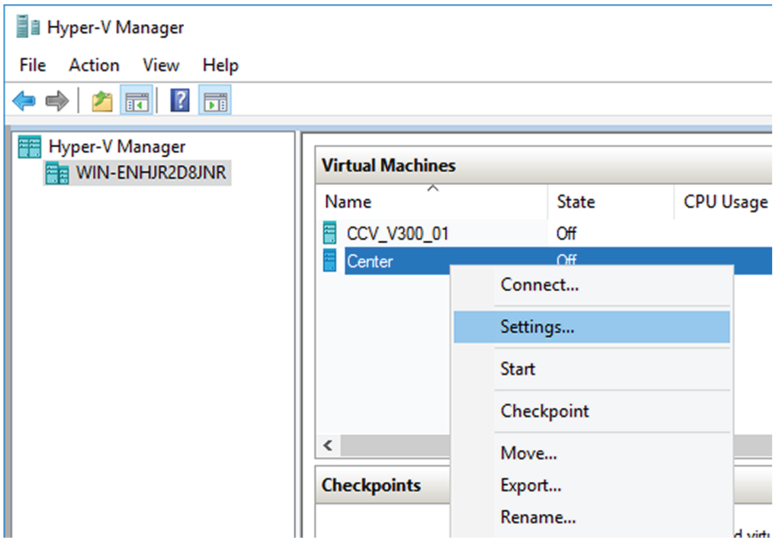
Map the network interfaces

To add a network card:

ICS CyberVision needs two network adapters (i.e. network card) to which the Admin and Collection network interfaces will be assigned. Each new VM includes a network card when created which is available within the hardware list. Therefore, you need to create another one during this step.

Procedure

Step 1 Right click the Center and click again 'Settings'.

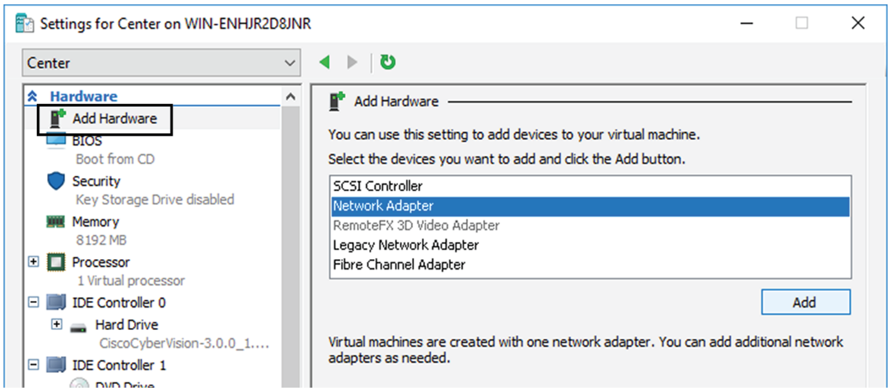


The settings window for the Virtual Center is displayed.

Step 2 Click 'Add Hardware'.

Step 3 Select 'Network Adapter'.

Step 4 Click 'Add'.



You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

The second network adapter needed is created. Now you need to map each network adapter to a Virtual Switch.

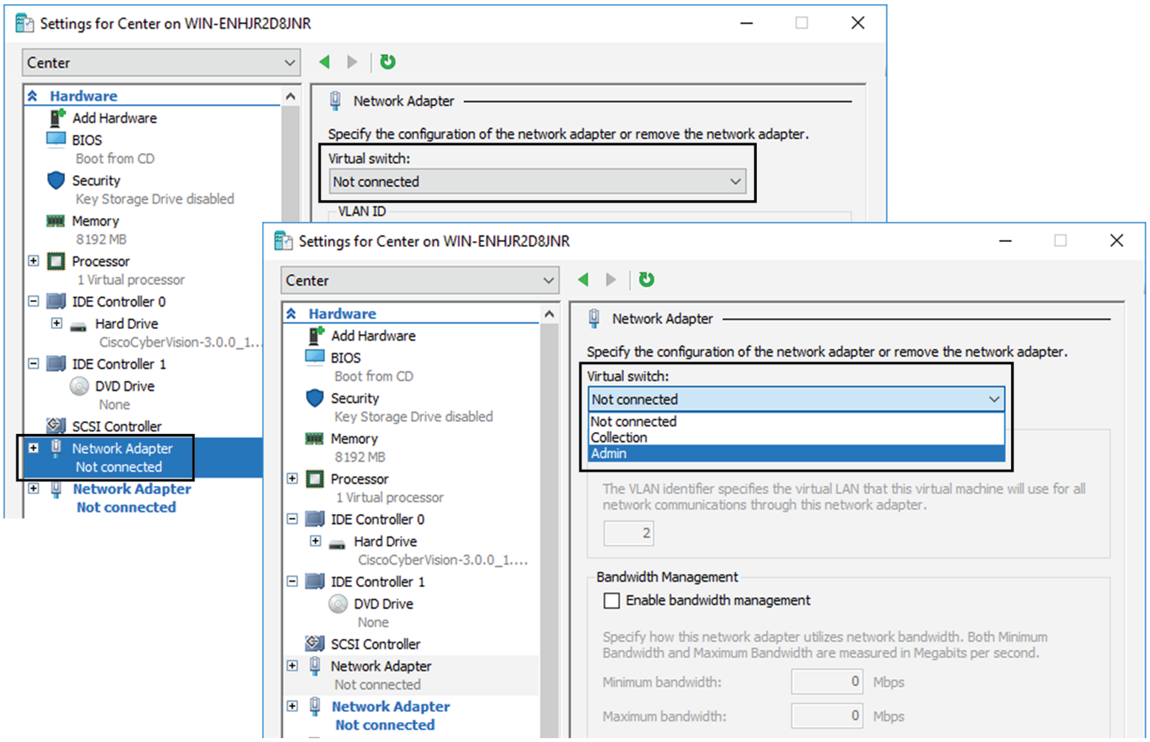
To proceed to the network mapping:

Step 5 Select the first network adapter.

Step 6 Select 'Admin' as Virtual Switch.

Note
You must configure network interfaces in order of appearance inside the network list to avoid confusion:

- The first network card as the Administration network interface (eth0).
- The second one as the Collection network interface (eth1).



Settings for Center on WIN-ENHJR2D8JNR

Center

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  8192 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    CiscoCyberVision-3.0.0_1....
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  Not connected
- **Network Adapter**
  Not connected

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:
Not connected

Not connected
Collection
Admin

VLAN ID

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

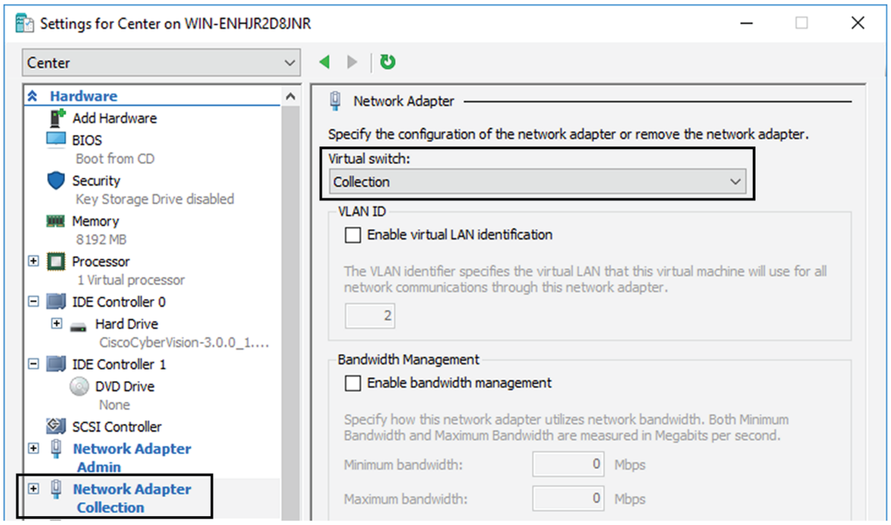
☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

Step 7 Repeat the previous action for the second network adapter and select 'Collection' as Virtual Switch.



Settings for Center on WIN-ENHJR2D8JNR

Center

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  8192 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    CiscoCyberVision-3.0.0_1....
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- **Network Adapter**
  Admin
- **Network Adapter**
  Collection

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:
Collection

VLAN ID

☐ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

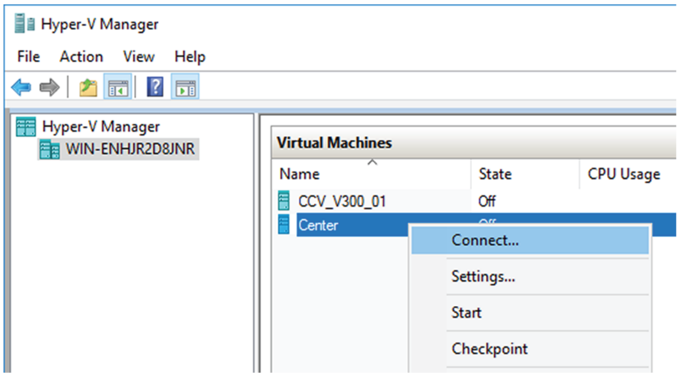
Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

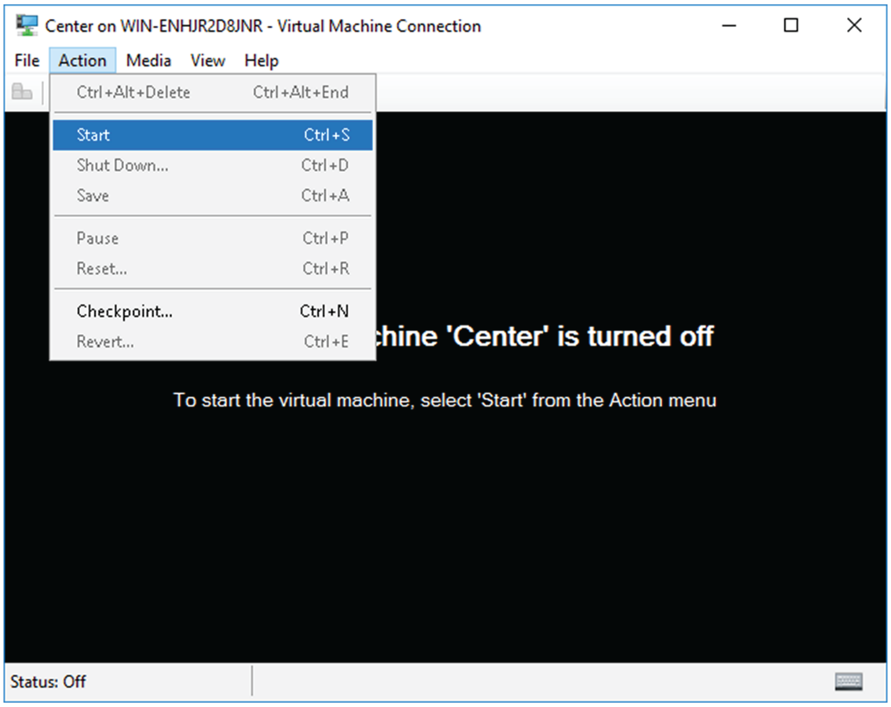
Boot the Virtual Machine

You can now proceed to the Virtual Center first boot.

1. Click Center on Hyper-V Manager and click 'Connect'.



2. Start the Virtual Center.

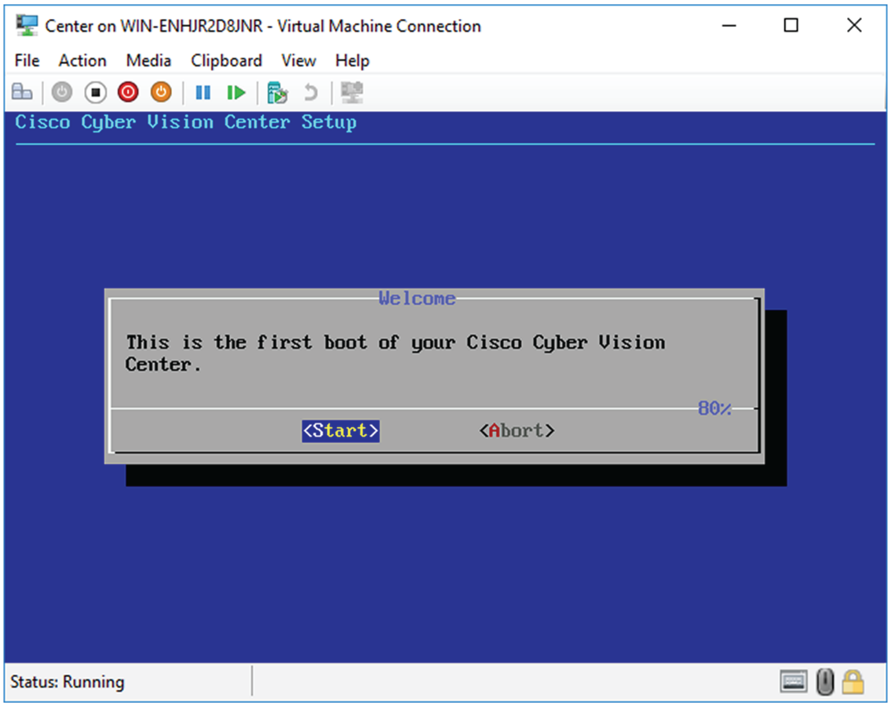

Center on WIN-ENHJR2D8JNR - Virtual Machine Connection
File Action Media View Help
Ctrl+Alt+Delete Ctrl+Alt+End
Start Ctrl+S
Shut Down... Ctrl+D
Save Ctrl+A
Pause Ctrl+P
Reset... Ctrl+R
Checkpoint... Ctrl+N
Revert... Ctrl+E

chine 'Center' is turned off

To start the virtual machine, select 'Start' from the Action menu

Status: Off

Once the VM configuration completed successfully, the following screen appears:


Center on WIN-ENHJR2D8JNR - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

Cisco Cyber Vision Center Setup

Welcome

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

80%

<Start> <Abort>

Note To retrieve the control of your keyboard and mouse, press Ctrl+Alt.

The Virtual Center is now ready for basic configuration.

Note Keeping your Virtual environment safe and clean. Once the VM first boot has completed successfully, Cisco recommends to shut down the Virtual Center and delete the Virtual Disk from Hyper-V hardware list. Keeping interfaces to the minimum lowers possible access doors for attackers.

Nutanix

Create Virtual Machines

Before creating a virtual machine for Cisco Cyber Vision on Nutanix, configure the required network interfaces based on your network infrastructure.

- **Administration network interface:** This is essential for managing your VM.
- **Collection network interface:** This interface is used for data collection.
- **DPI network interface:** If you're deploying a Center with Deep Packet Inspection (DPI) capabilities, you'll also need to set up a dedicated DPI network interface.

For detailed guidance on setting up the network interfaces, refer to the official Nutanix documentation.

Procedure

Step 1 Log in to the Nutanix Prism Central as an administrator.

Step 2 On the left sidebar, select **Compute** > **OVAs**.

All your uploaded Cisco Cyber Vision OVA files are listed in the right pane. To upload a new one, click **Upload OVA**.

Step 3 Select an OVA file by checking the box next to its name. Then, click the **Actions** menu and choose **Deploy as VM**.

The deployment wizard guides you through these configuration stages for your VM: Configuration, Resources, Management, and Review.

Step 4 In the **Configuration** stage:

a. Enter a name for the VM in the **Name** field and optionally enter a description in the **Description** field.

b. Enter the hardware details in the **VM Properties** section, and click **Next**. For more details, see the Installation Prerequisites, on page 7.

Step 5 In the **Resources** stage:

a. In the **Disks** section, modify the disk size to suit your requirements. The default value is 250 GB. For more details, see the "Virtual Machine Sizing" section in Installation Prerequisites, on page 7.

b. In the **Networks** section, configure a VLAN for the management and collection interfaces.

Step 6 In the **Management** stage:

a. (Optional) Enable the default storage policy by checking **Enable Default Storage Policy**. This allows you to manage the storage configurations across all VM disks.

b. Select your timezone from the **Timezone** drop-down list, and click **Next**.

Step 7 In the **Review** stage:

a. Review the settings and modify them if required by clicking **Edit** next to the section you want to modify.

b. Click **Create VM**.

The new VM is listed under **Compute** > **VMs**.

Step 8 (Optional) To modify VM settings at any time, select the VM and choose **Update** from the **Action** drop-down list.

Boot Virtual Machines

This section guides you to start the VM in Nutanix Prism Central to configure the Cisco Cyber Vision Center for initial setup.

Procedure

Step 1 Log in to the Nutanix Prism Central.

Step 2 On the left sidebar, select **Compute > VMs**.

Step 3 On the right pane, select the VM you want to boot, and choose **Power Operations** > **Power On** from the **Actions** menu.

Step 4 Wait a few moments for the VM initiation to complete.

A green dot appears to the left of the VM name, indicating that the VM is powered on.

CHAPTER 5

Configure the Center

You will need to complete two steps to configure the Center:

1. The basic Center configuration through a VGA display and a keyboard or a console, to:
    - Set the Center and the sensor passwords.
    - Synchronize the Center to the NTP server.
    - Configure the Administration and Collection interfaces (n/a for a Global Center or a Center using a single interface).
2. The Cisco Cyber Vision configuration, through a browser, to:
    - Create an admin account.
    - Configure the Center's data synchronization (Global Center and synchronized Centers only).

Basic Center configuration

This step will allow you to configure the Center network settings before using it with the user interface.

Required information:

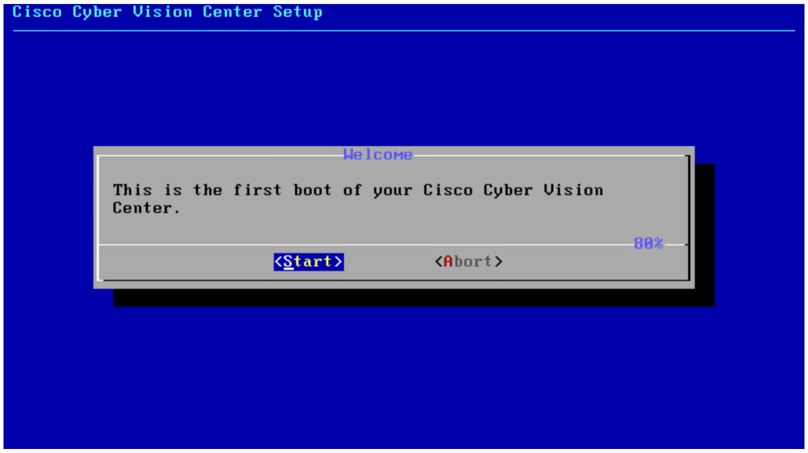
- Local NTP and DNS IP addresses.
- The Collection interface network address (n/a for a Global Center or a Center using a single interface).

In the case of manual Administration network interface configuration:

- Its IP address.
- Its netmask (in a two-number format, e.g. 192.168.1.0/24).
- Its default gateway (to reach devices located outside the local network).

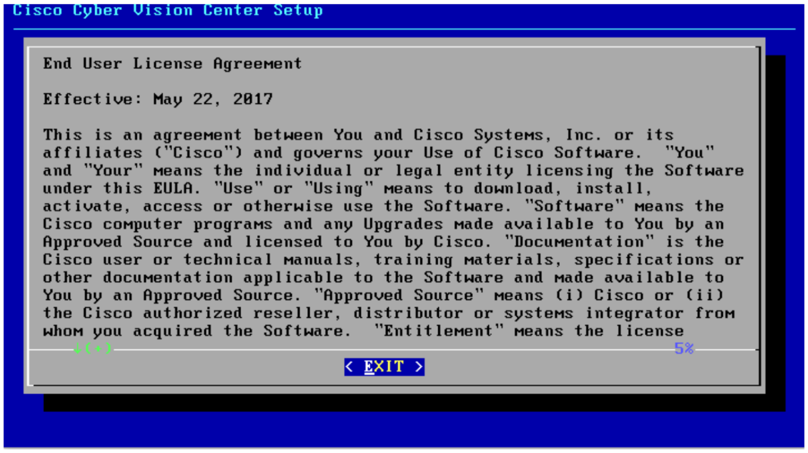
Access the basic Center configuration

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

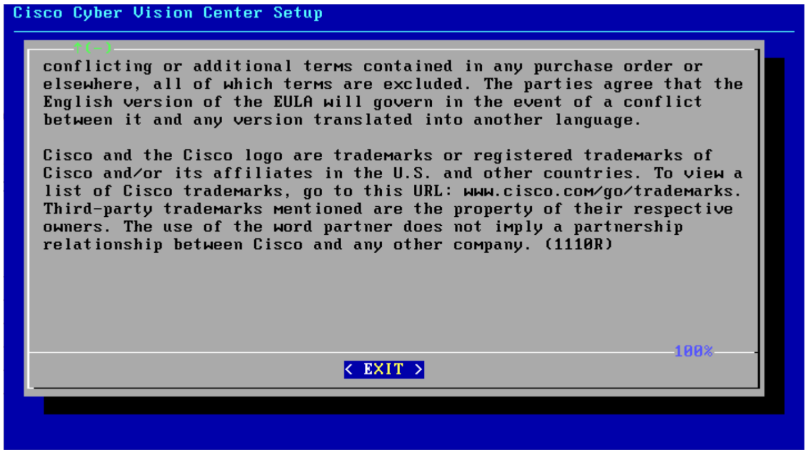


```
This is the first boot of your Cisco Cyber Vision
Center.
```

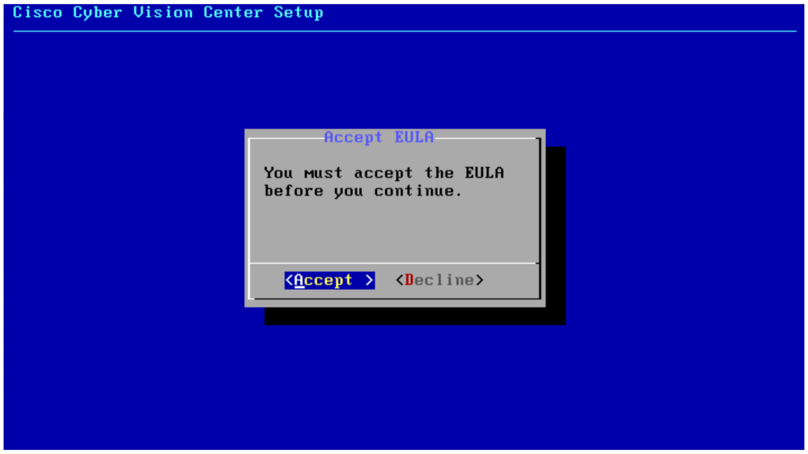
Accept the End User License Agreement



```
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
```



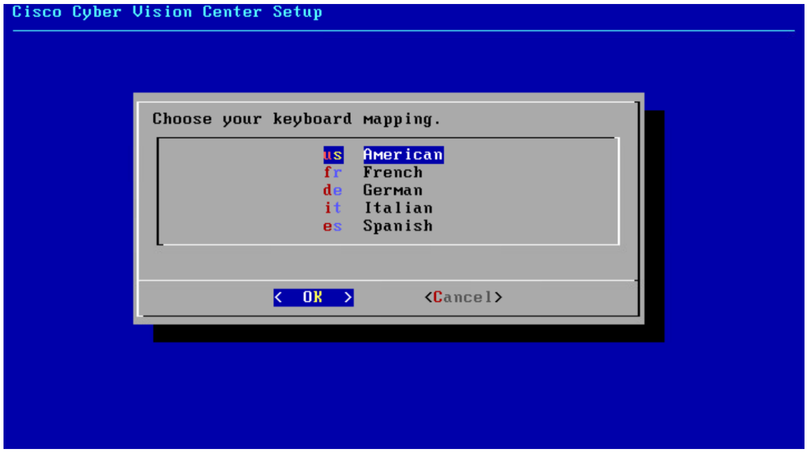
```
conflicting or additional terms contained in any purchase order or
elsewhere, all of which terms are excluded. The parties agree that the
English version of the EULA will govern in the event of a conflict
between it and any version translated into another language.

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.

          <Accept >   <Decline>
```

Select the language to match your keyboard

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



```
Cisco Cyber Vision Center Setup

     Choose your keyboard mapping.

                us   American
                fr   French
                de   German
                it   Italian
                es   Spanish

            <  OK  >          <Cancel>
```

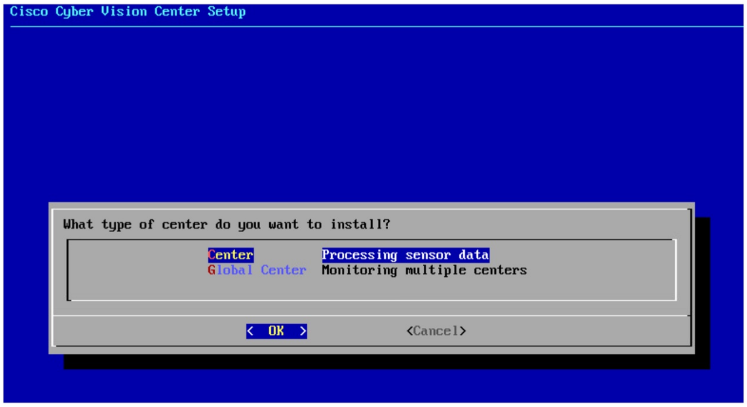
Select the Center type

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.

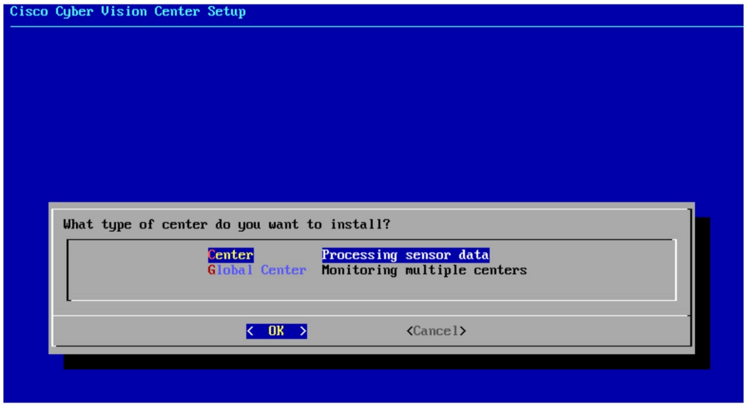
Select the type of Center you want to install.



```
Cisco Cyber Vision Center Setup

What type of center do you want to install?

Center          Processing sensor data
Global Center   Monitoring multiple centers

< OK >          <Cancel>
```

Center

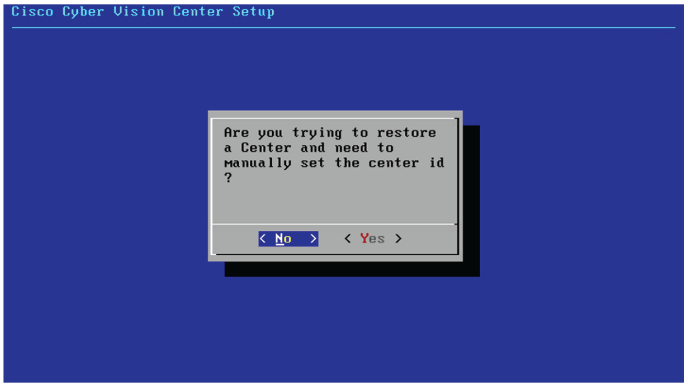
If installing a Center, select the first option.



```
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>
```

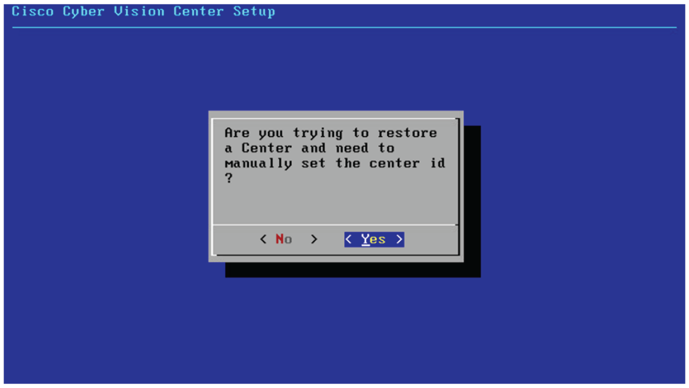
Then, you will have the opportunity to set the Center id. It can be used in case of Center restoration to reuse the same id previously set in the Global Center. Thus, some data can be retrieved.

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.



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

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

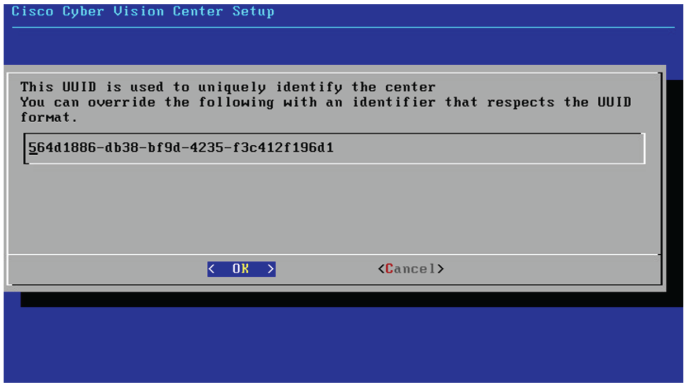


```
Are you trying to restore
a Center and need to
manually set the center id
?
```

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.

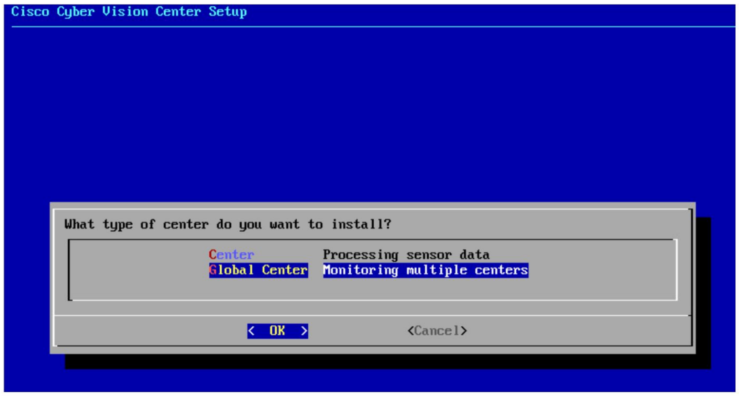


```
This UUID is used to uniquely identify the center
You can override the following with an identifier that respects the UUID
format.

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

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

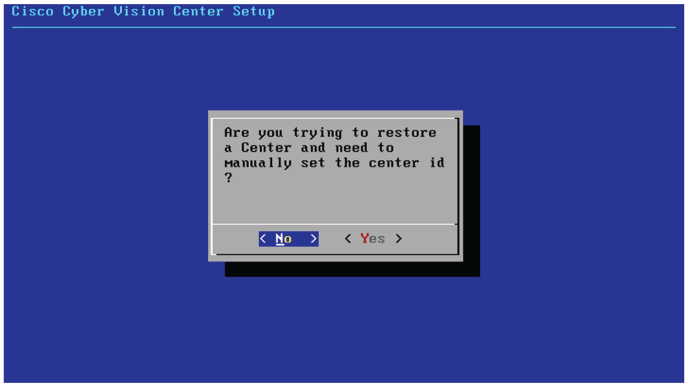
Global Center

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

         <  OK  >              <Cancel>
```

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
?

    <  No  >    <  Yes  >
```

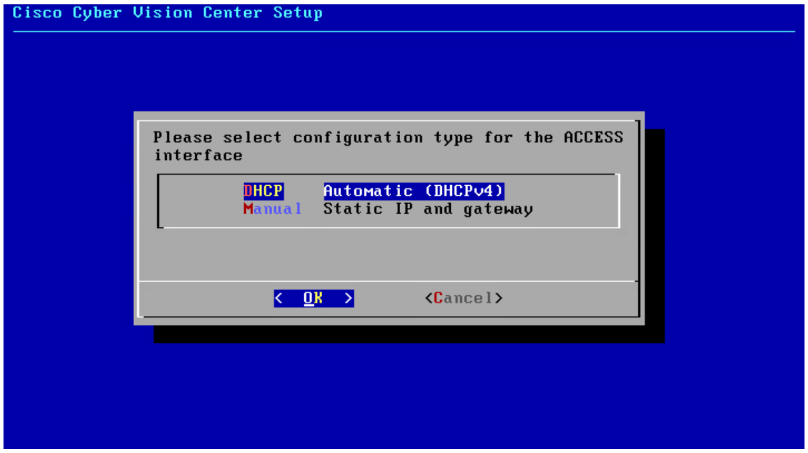
You will be directed to the next step.

Configure the Center's Administration Network Interface

The Center uses a dedicated sub-network on the Administration interface. It is possible to change it if the default one doesn't fit the environment on which the Center will be connected.

The Administration network interface configuration can be done either:

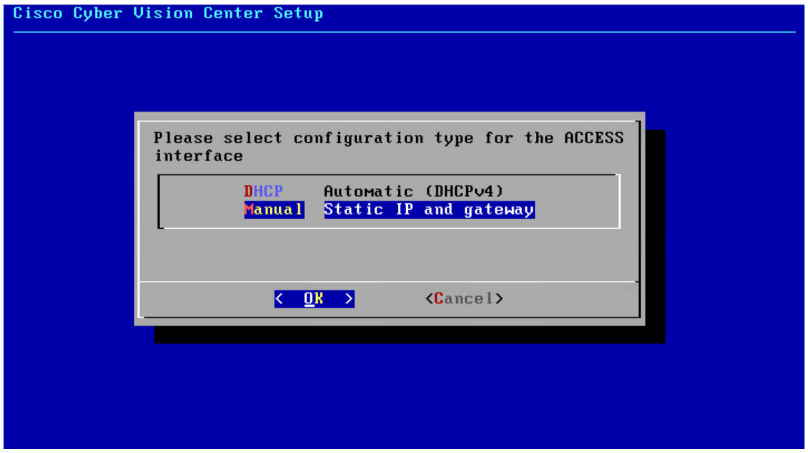
- Using a DHCP server, if there is one available on the network.



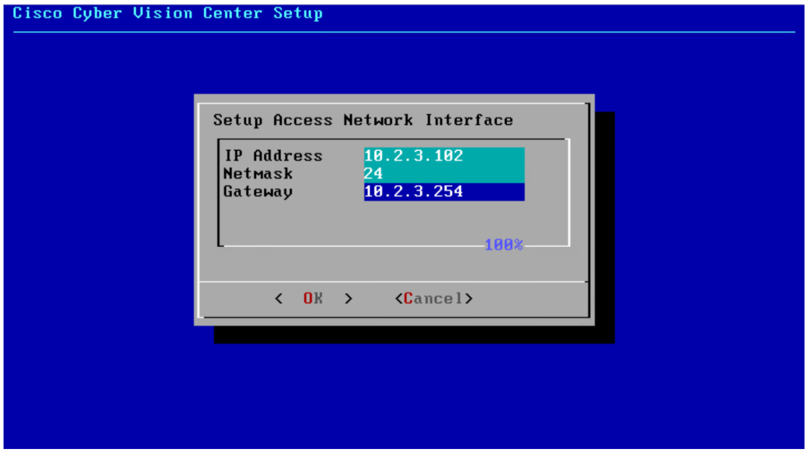
```
Cisco Cyber Vision Center Setup

Please select configuration type for the ACCESS
interface

      DHCP     Automatic (DHCPv4)
      Manual   Static IP and gateway

        <  OK  >          <Cancel>
```

In this case, enter OK. Settings will be adjusted automatically, and you will be directed to the next step.

- Manually:



```
Cisco Cyber Vision Center Setup

Please select configuration type for the ACCESS
interface

      DHCP     Automatic (DHCPv4)
      Manual   Static IP and gateway

        <  OK  >          <Cancel>
```



```
Cisco Cyber Vision Center Setup

Setup Access Network Interface

 IP Address        10.2.3.102
 Netmask           24
 Gateway           10.2.3.254

                              100%

    <  OK  >    <Cancel>
```

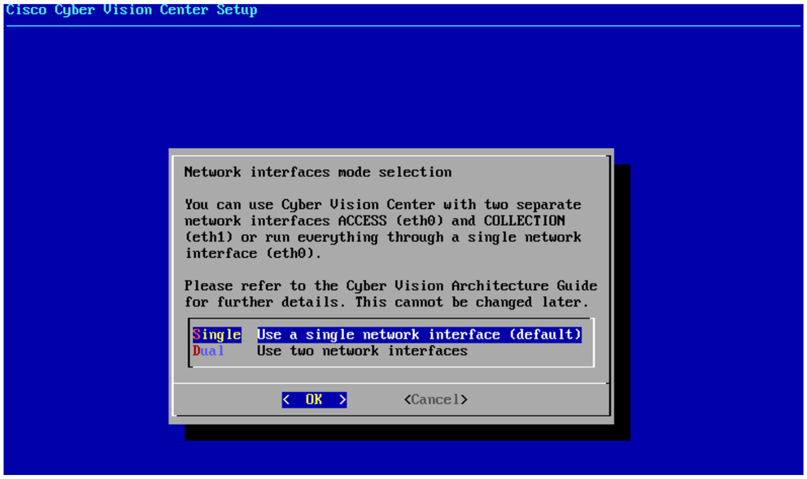
Enter the Administration network interface's IP address, netmask (in a two-number format), and gateway.

Set interfaces (dual or single)

This step is not applicable to a Global Center.

Regarding a Center, it is possible to:

- Use a single interface. In this case, select the Single option.
- Set the Administration and Collection network interfaces on two distinct interfaces (recommended for security). In this case, select the Dual option.

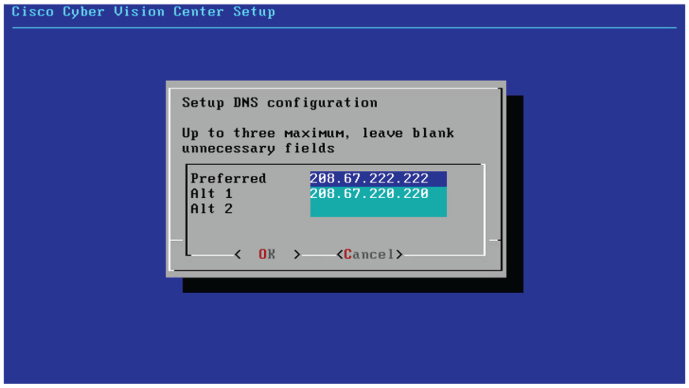


```
Cisco Cyber Vision Center Setup

Network interfaces mode selection

You can use Cyber Vision Center with two separate
network interfaces ACCESS (eth0) and COLLECTION
(eth1) or run everything through a single network
interface (eth0).

Please refer to the Cyber Vision Architecture Guide
for further details. This cannot be changed later.

Single   Use a single network interface (default)
Dual     Use two network interfaces

          <  OK  >          <Cancel>
```

If you choose the Dual option, you will later be directed to: Configure the Center's Collection network interface, on page 43.

Configure the Center's DNS

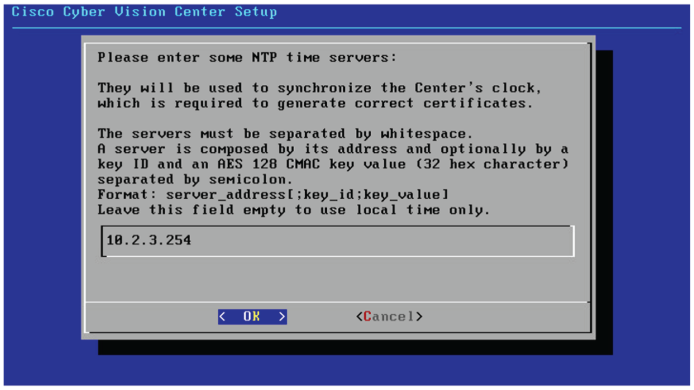
Type a DNS server address and optional fallbacks.



```
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>
```

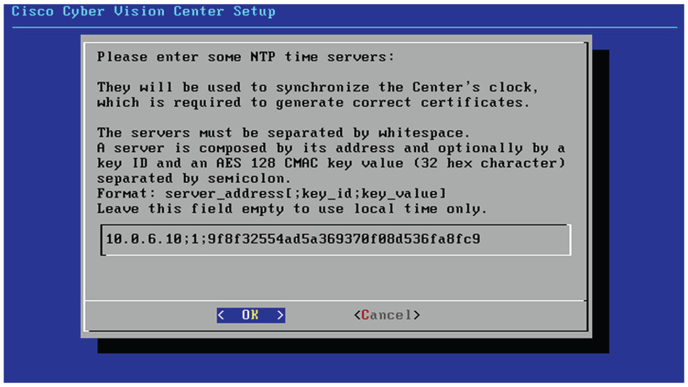
Synchronize the Center and the sensors to NTP servers

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.



```
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.

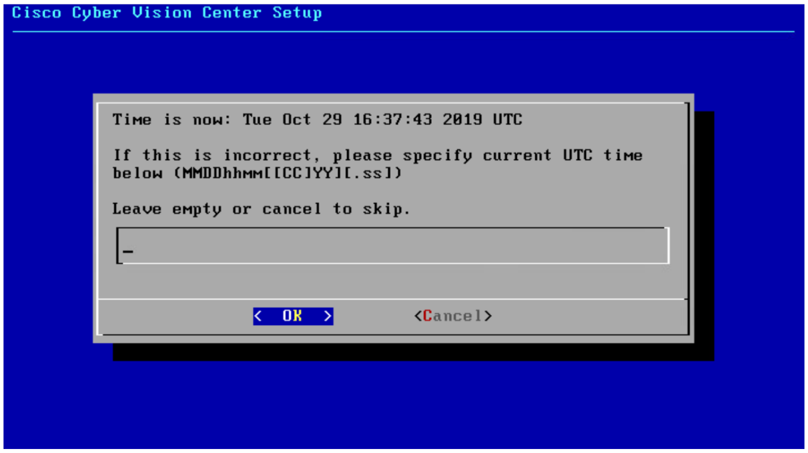


```
Please enter some NTP time servers:

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
```

The synchronization takes a few seconds.

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

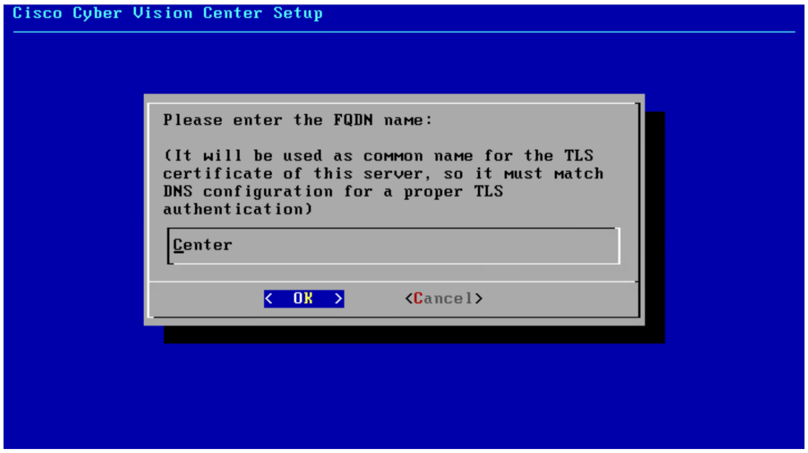
Note The time is set in UTC standard.



```
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.

_
```

Give the Center a name

Note This name will be used in the Center certificate.



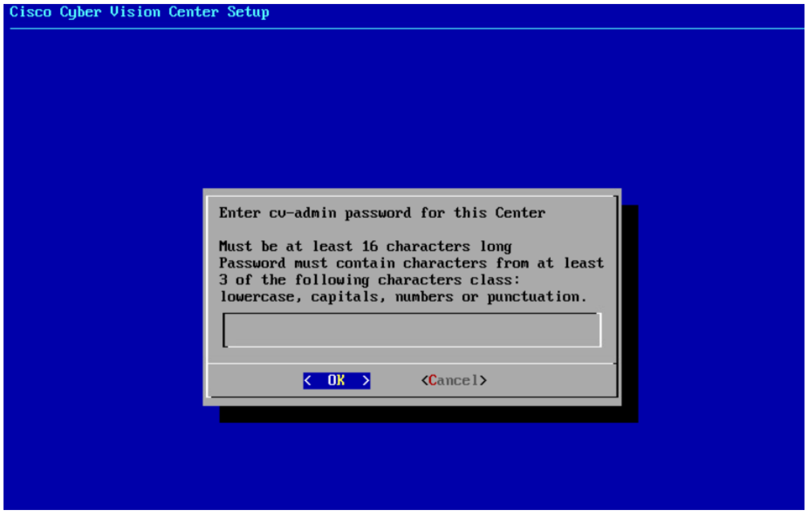
```
Cisco Cyber Vision Center Setup

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.

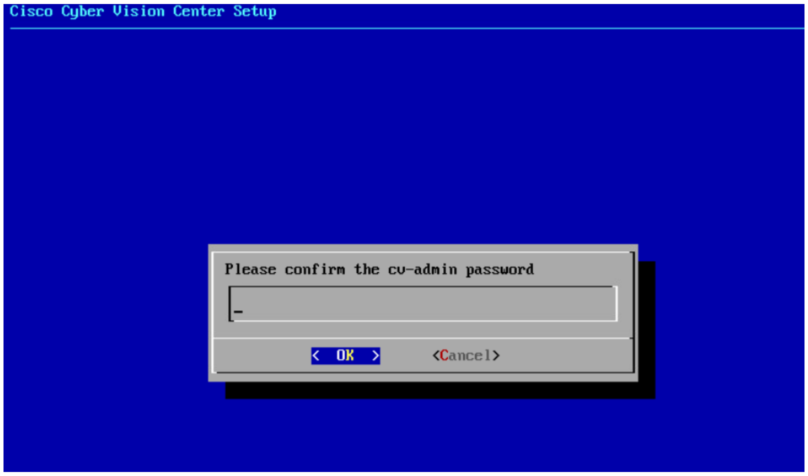
Set the Center's password

The administrator account (i.e. cv-admin) password of the Center must be set for security reasons. It is hidden for confidentiality reasons.



```
Cisco Cyber Vision Center Setup

Enter cv-admin password for this Center

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.
```

Confirm the password.



Cisco Cyber Vision Center Setup

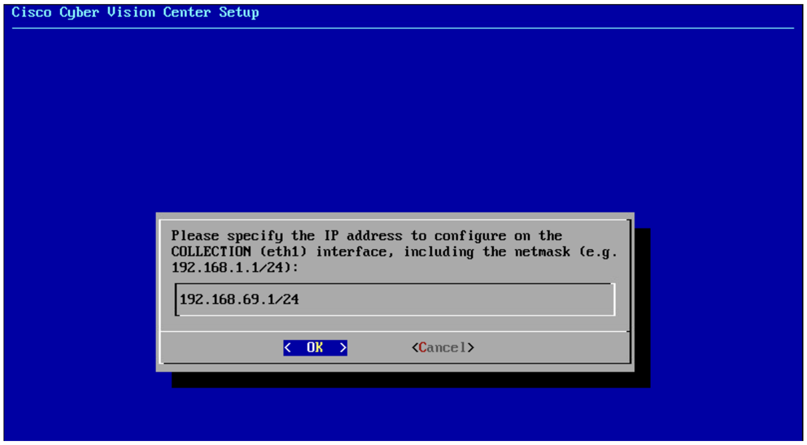
Please confirm the cv-admin password

Configure the Center's Collection network interface

This step is not applicable to a Global Center.

This step will only appear if the dual interface option has been selected during the Set interfaces (dual or single), on page 40 step.

Type the IP address of the Collection network interface:



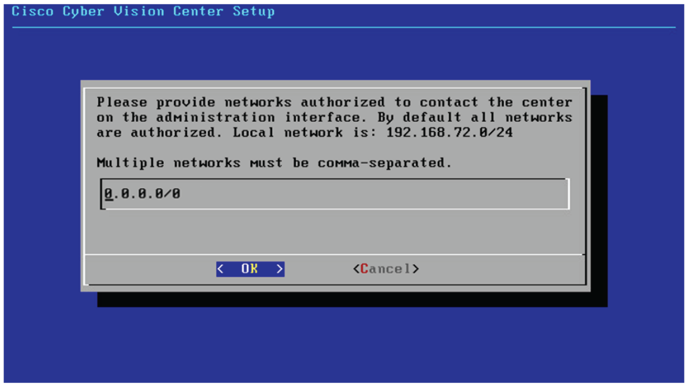
Cisco Cyber Vision Center Setup

Please specify the IP address to configure on the COLLECTION (eth1) interface, including the netmask (e.g. 192.168.1.1/24):

192.168.69.1/24

Authorize networks

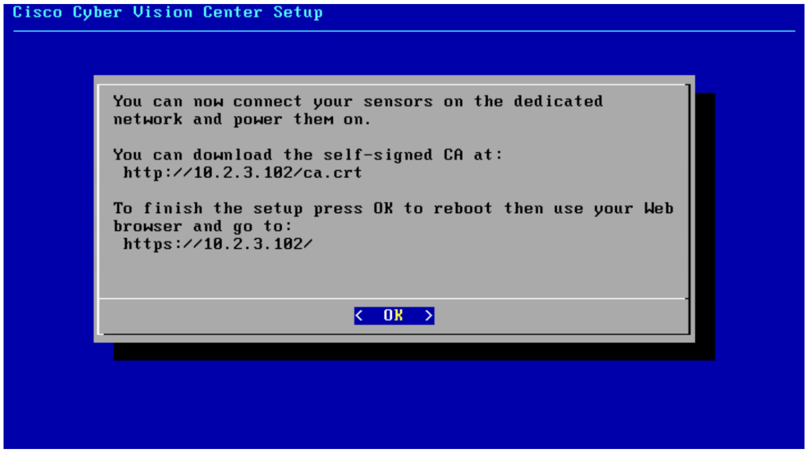
This step allows you to restrict IP addresses that can connect to the Administration interface. If no IP is entered, all networks are authorized by default.



```
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
```

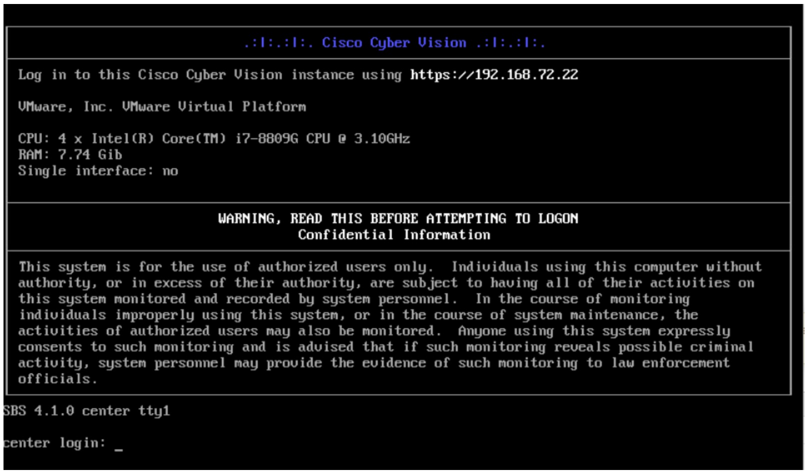
Complete the basic Center configuration

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/
```

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).

Cisco Cyber Vision configuration

Once the Basic Center configuration is done, you must connect through a web browser to the URL displayed on the last step of the basic configuration wizard (i.e. the Center's IP address). A message saying that the URL is not secure will appear.

- If you plan to use a self-signed certificate, you must Install the certificate in your browser, on page 45 and then access the user interface installation wizard to configure users and sensors.
- If you plan to use an enterprise certificate, you must ignore the security message and perform the following steps in this order:
  1. Access the user interface installation wizard to configure users and sensors.
  2. Configure the security of the user interface itself.

Then, you will configure the Centers data synchronization (Global Center and its Centers' only).

Browser requirements:

Cisco Cyber Vision supports Chrome 54, Firefox 49 and newer versions.

Install the certificate in your browser

This task explains how to intall a Cisco Cyber Vision self-signed certificate in your browser.

Before you begin

Perform this task if you aim to install a self-signed certificate. If you're planning to use an enterprise certificate, proceed directly with Install Cisco Cyber Vision, on page 51.

Procedure

Step 1 Open your browser.

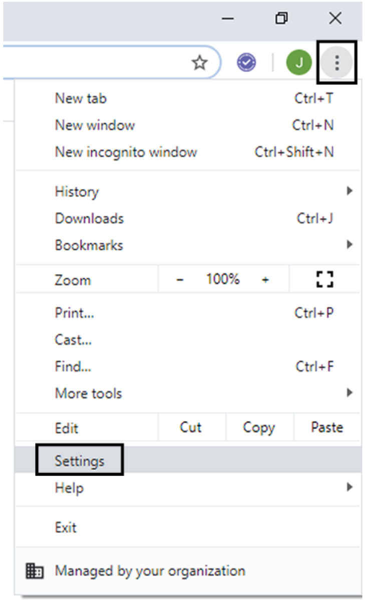
Step 2 Enter 'http://<CENTERIPADDRESS>/ca.crt' inside the search bar.

The certificate is downloaded.

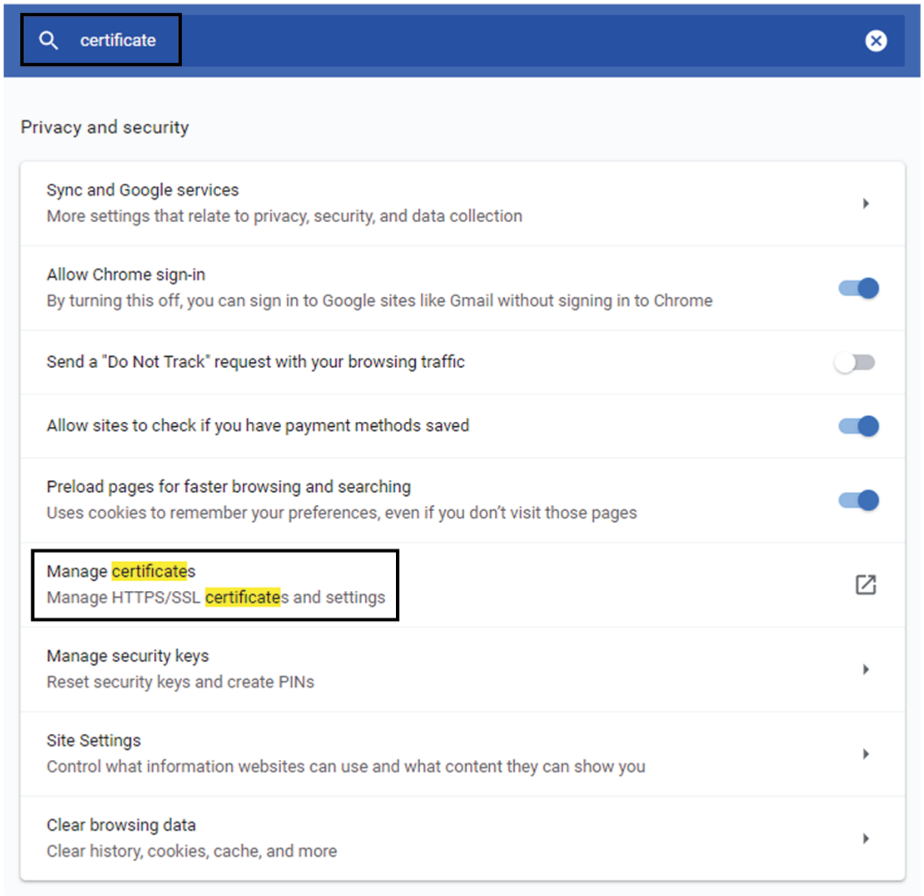
Step 3 Save the certificate on your computer.

Step 4 In the browser, access the settings.

Example: Chrome



Step 5 Type 'certificate' in the search bar and access the certificates management menu.



certificate

Privacy and security

Sync and Google services
More settings that relate to privacy, security, and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

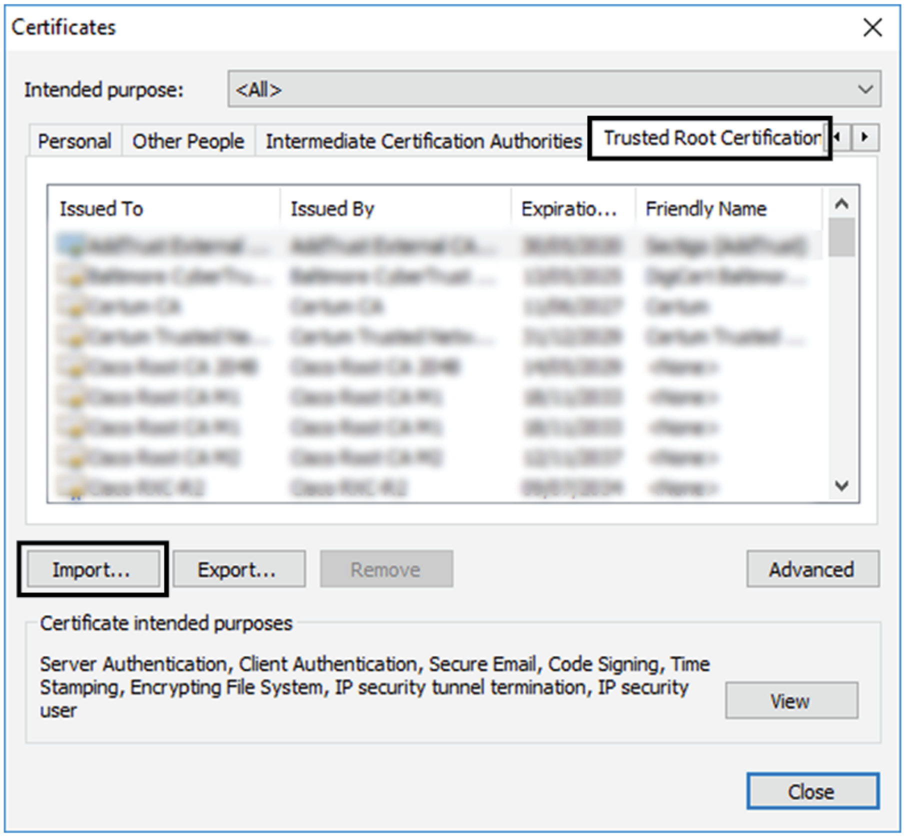
Manage certificates
Manage HTTPS/SSL certificates and settings

Manage security keys
Reset security keys and create PINs

Site Settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

Step 6 Access the Trusted Root Certification tab and click Import.



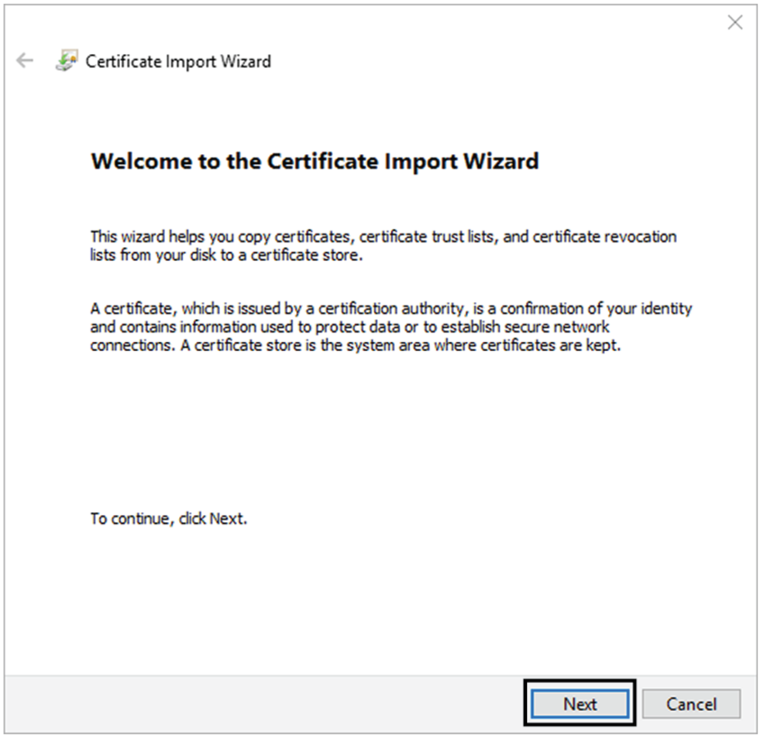
Intended purpose: <All>

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user

A certificate importation wizard opens.

Step 7 Go to the next step.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

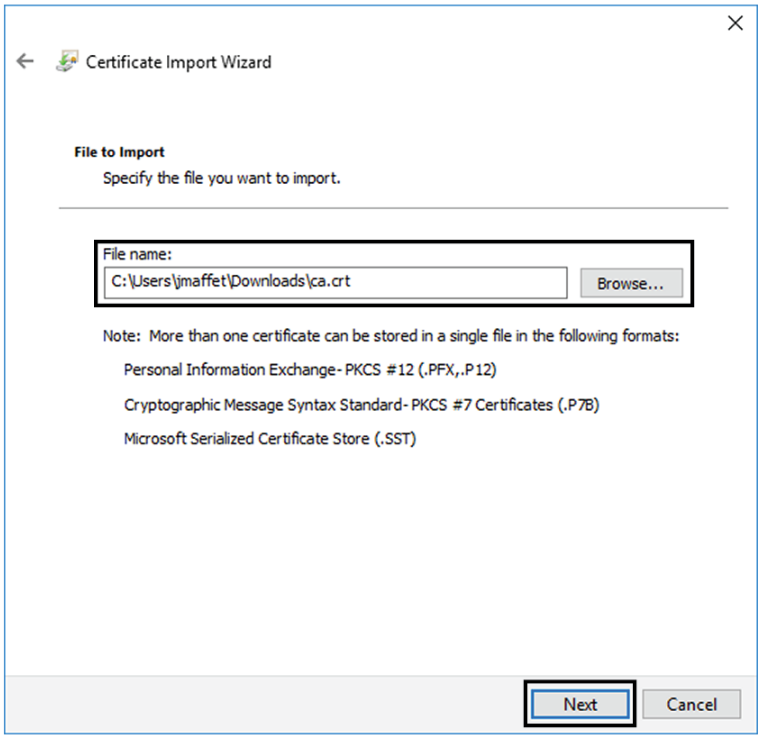
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 8 Search for the certificate you downloaded earlier.

Step 9 Go to the next step.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:
C:\Users\jmaffet\Downloads\ca.crt

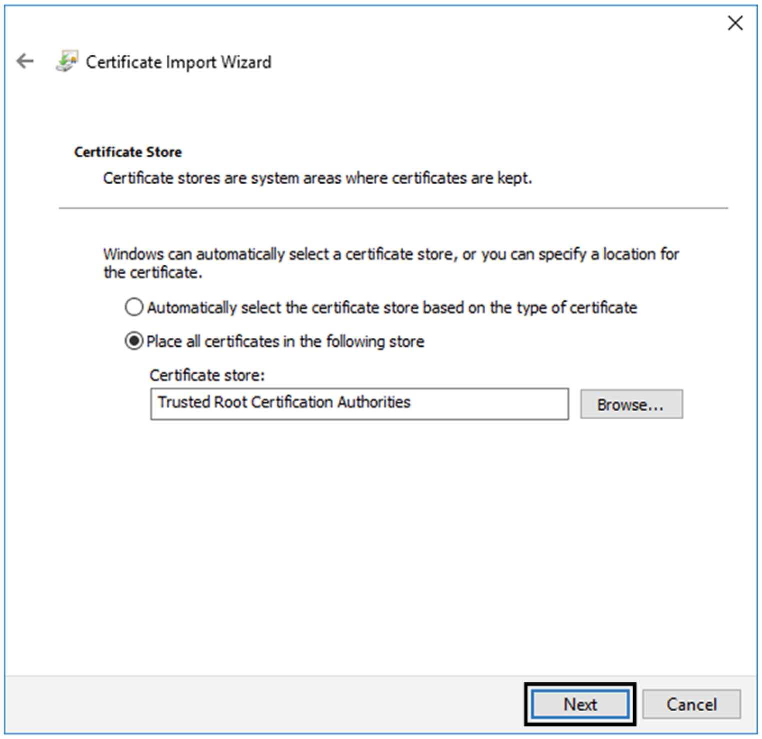
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Step 10 Accept the default values by accessing the next step.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

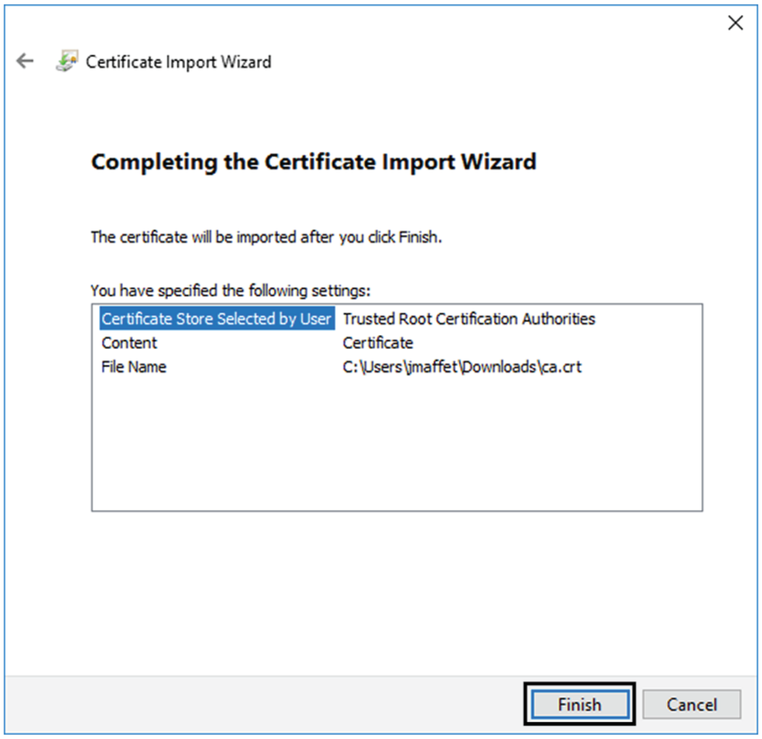
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

Step 11 The certificate is now considered as trusted by the browser. It will be imported as soon as you will click Finish.



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\jmaffet\Downloads\ca.crt

What to do next

Install Cisco Cyber Vision, on page 51

Install Cisco Cyber Vision

Access the Cisco Cyber Vision installation wizard:

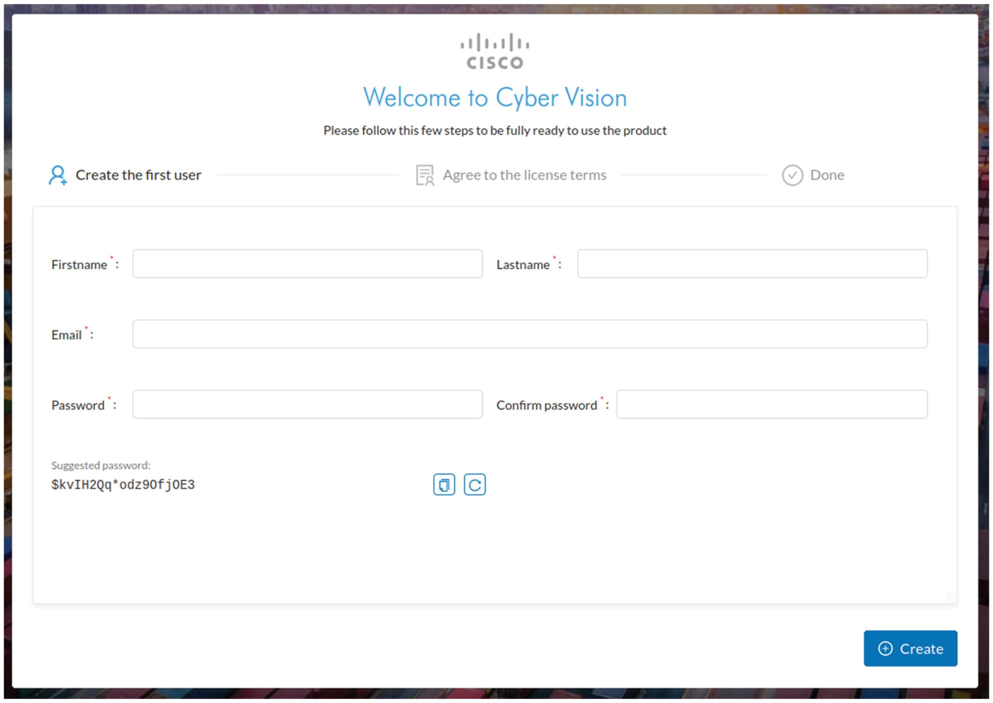
Procedure

Step 1 With your browser, access https://**<CENTERNAME>**/.

Note
Accessing the Center using its name enables HTTPS secure interface. Yet, this requires a DNS or local host configuration to associate the name and the IP address. The Center access through its IP address is possible but the connection is not secure.

Step 2 The setup wizard used for the first access to Cisco Cyber Vision is displayed:

Step 3 **Create an admin account:**



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

Firstname * :

Lastname * :

Email * :

Password * :

Confirm password * :

Suggested password:
$kvIH2Qq*odz9OfjOE3

Step 4

Step 5 Enter the information required.

Note
Email will be asked for login access.

Note
Passwords must contain at least 6 characters and comply with the rules below. Passwords:

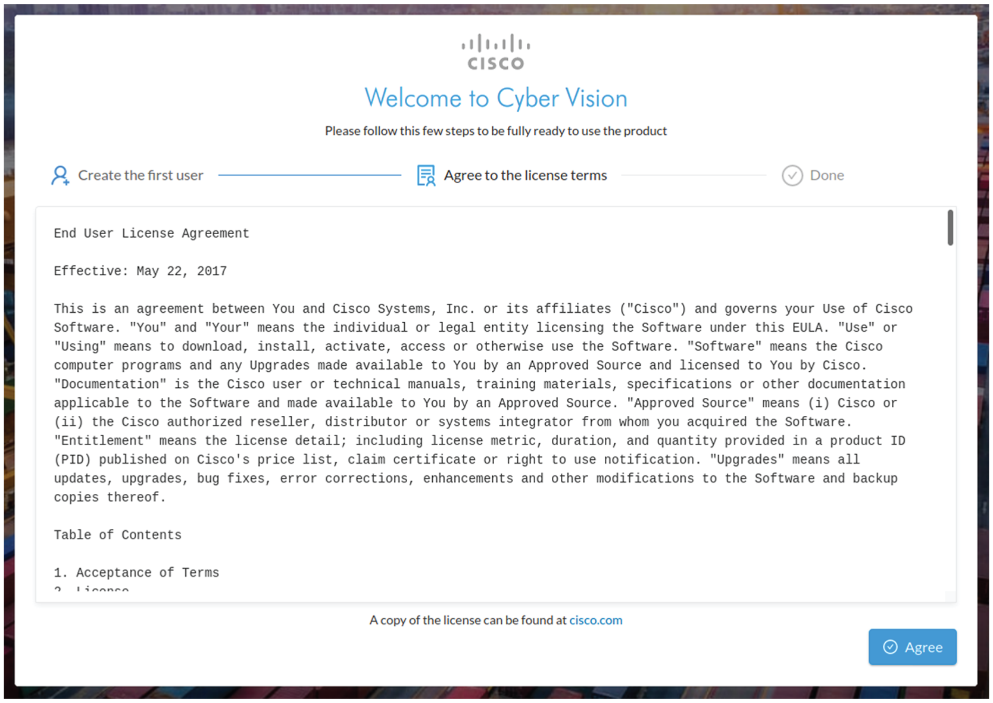
- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

Passwords should be changed regularly to ensure the integrity of the platform and the industrial network security.

Note
You can reset users using the following command in the Center's CLI:

```
sbs-db reset-users
```

Step 6 **Accept the software license agreement:**



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

```
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 detail; including license metric, duration, and quantity provided in a product ID
(PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all
updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup
copies thereof.

Table of Contents

1. Acceptance of Terms
```

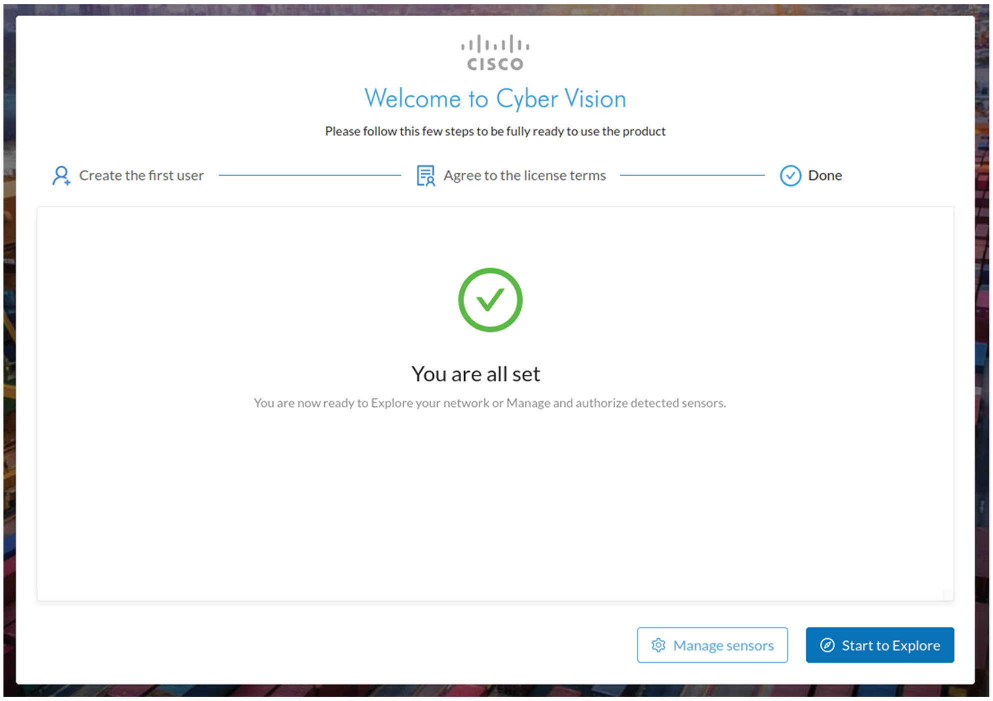
A copy of the license can be found at cisco.com

Step 7

Step 8 **Finish the installation:**

The Center is now correctly installed and Cisco Cyber Vision is ready to operate.

Step 9 Click Start to Explore.



Welcome to Cyber Vision

Please follow this few steps to be fully ready to use the product

You are all set

You are now ready to Explore your network or Manage and authorize detected sensors.

Cisco Cyber Vision installation is now complete.

What to do next

If you aim to use an enterprise certificate, proceed with Configure the user interface security, on page 54.

If you already installed a self-signed certificate, and if you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 59.

If you already installed a self-signed certificate, and if you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Cisco Cyber Vision Sensor Installation Guides.

Configure the user interface security

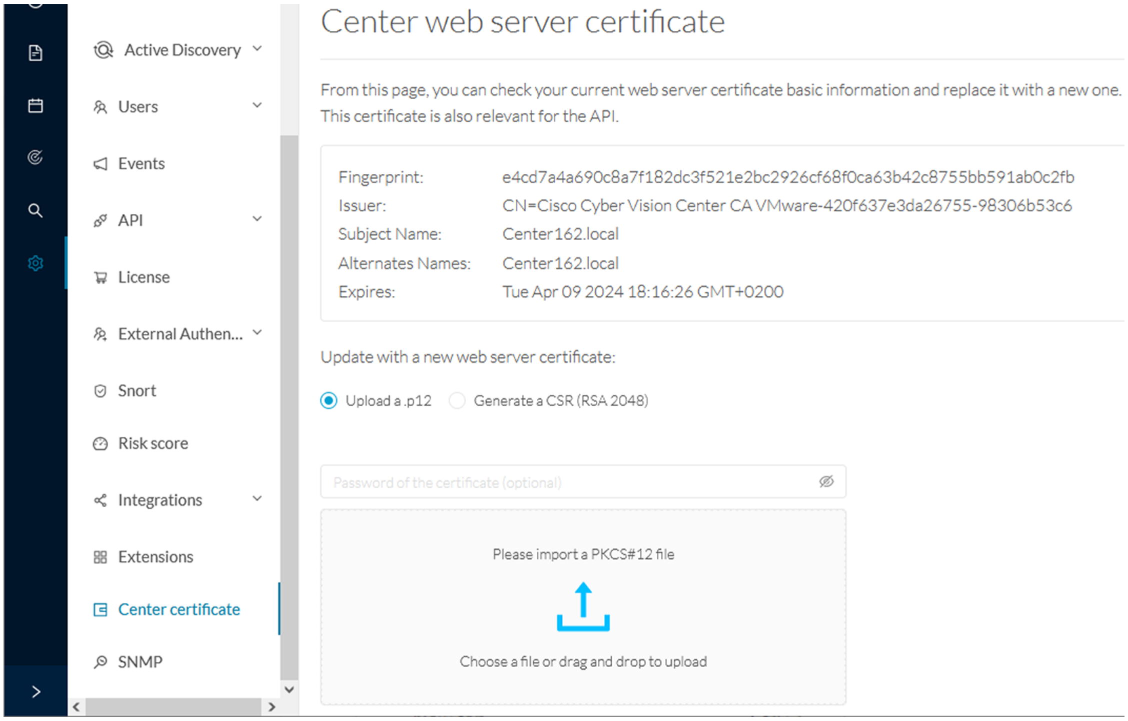
This section explains how to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

Before you begin

Perform this task if you're planning to use an enterprise certificate. You must install Cisco Cyber Vision beforehand.

Procedure

Step 1 To use an enterprise certificate, navigate to Admin > Center certificate.


Active Discovery
Users
Events
API
License
External Authen...
Snort
Risk score
Integrations
Extensions
Center certificate
SNMP
Upload a .p12
Generate a CSR (RSA 2048)
Password of the certificate (optional)
Please import a PKCS#12 file
Choose a file or drag and drop to upload

Center web server certificate

From this page, you can check your current web server certificate basic information and replace it with a new one. This certificate is also relevant for the API.

Fingerprint: e4cd7a4a690c8a7f182dc3f521e2bc2926cf68f0ca63b42c8755bb591ab0c2fb
Issuer: CN=Cisco Cyber Vision Center CA VMware-420f637e3da26755-98306b53c6
Subject Name: Center162.local
Alternates Names: Center162.local
Expires: Tue Apr 09 2024 18:16:26 GMT+0200

Update with a new web server certificate:

● Upload a .p12 ○ Generate a CSR (RSA 2048)

Step 2 You can upload a .p12 or generate a CSR.

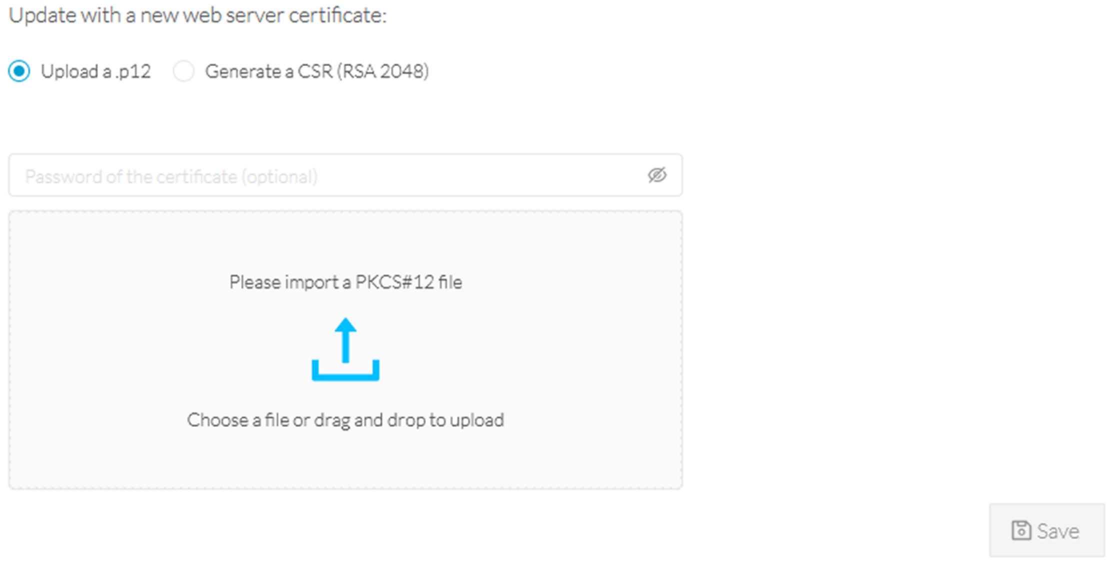
Upload a p12

Before you begin

The p12 (or Microsoft pfx) file must contain a private key, a password, and the field "X509v3 Subject Alternative Name" must contain the Center DNS name.

Procedure

Step 1 Select Upload a .p12.



Update with a new web server certificate:

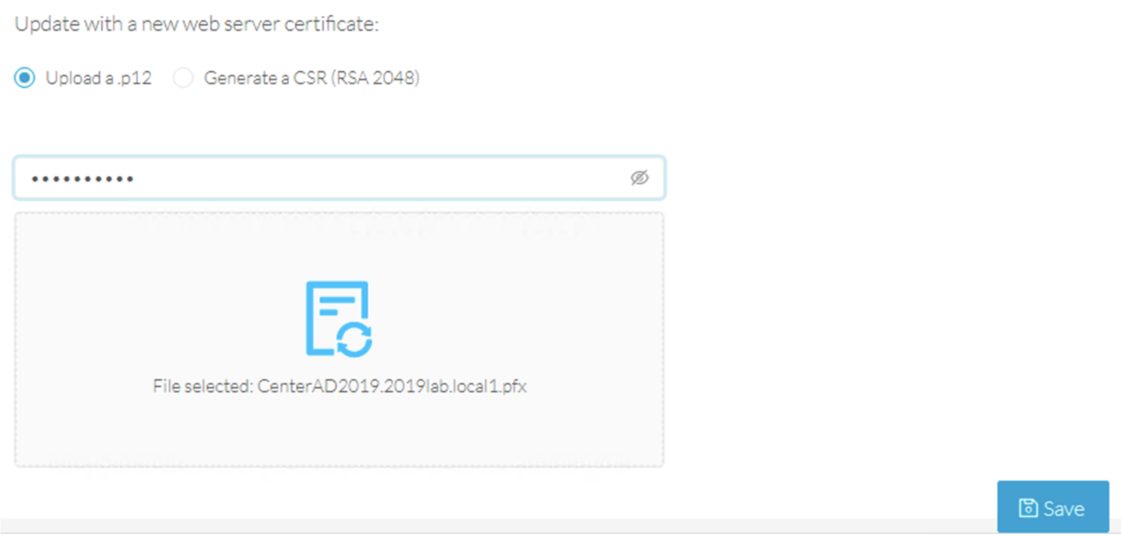
● Upload a .p12 ○ Generate a CSR (RSA 2048)

Password of the certificate (optional)
Please import a PKCS#12 file
Choose a file or drag and drop to upload
Save

Click Please import a PKCS12 file and choose you pfx or p12 file generated from your certification server.

Step 2 Type the certificate password.

Step 3 Click the Import a PKCS#12 file button or drag and drop the file to import it.



Update with a new web server certificate:

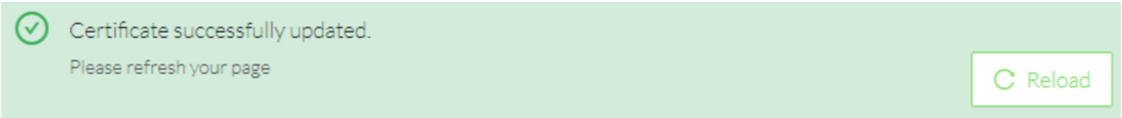
● Upload a .p12 ○ Generate a CSR (RSA 2048)

•••••••••••

File selected: CenterAD2019.2019lab.local1.pfx

Step 4 Click Save.

The following message appears:



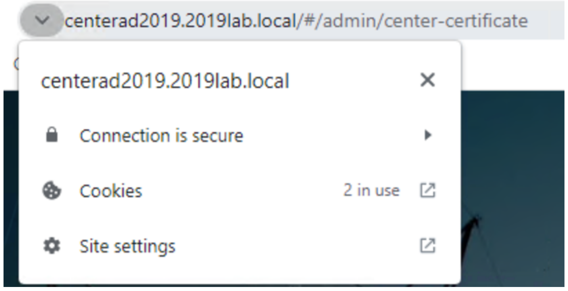
Certificate successfully updated.

Please refresh your page

Step 5 Click Reload.

Step 6 In your browser, use the DNS name to connect to your Cisco Cyber Vision instance.

The error message does not appear and the connection is secure.



centerad2019.2019lab.local/#/admin/center-certificate

centerad2019.2019lab.local

Connection is secure

What to do next

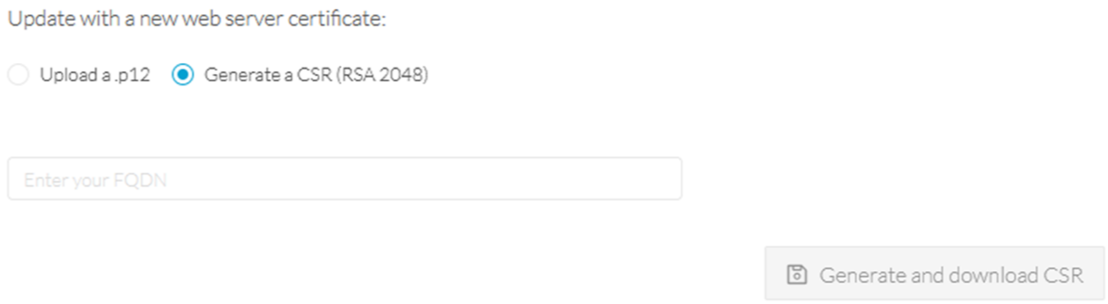
If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 59.

If you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Cisco Cyber Vision Sensor Installation Guides.

Generate a CSR

Procedure

Step 1 Select Generate a CSR.



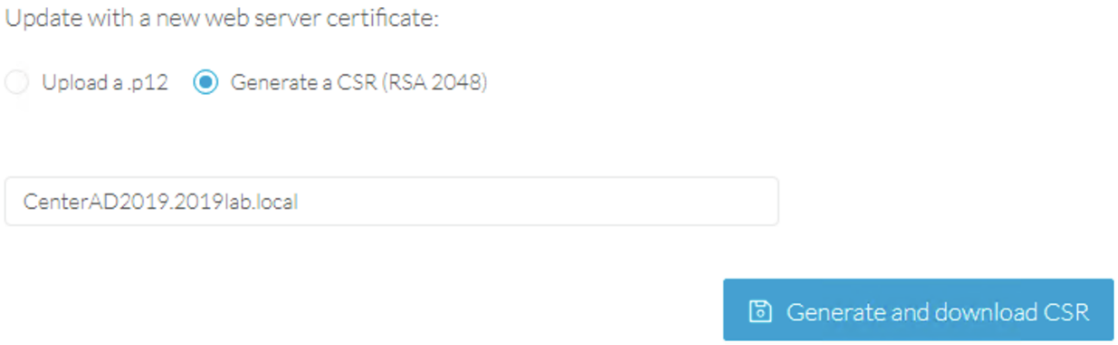
Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

Enter your FQDN

Step 2 Enter the Center FQDN as registered on your DNS server.

Step 3 Click the Generate and download CSR button.



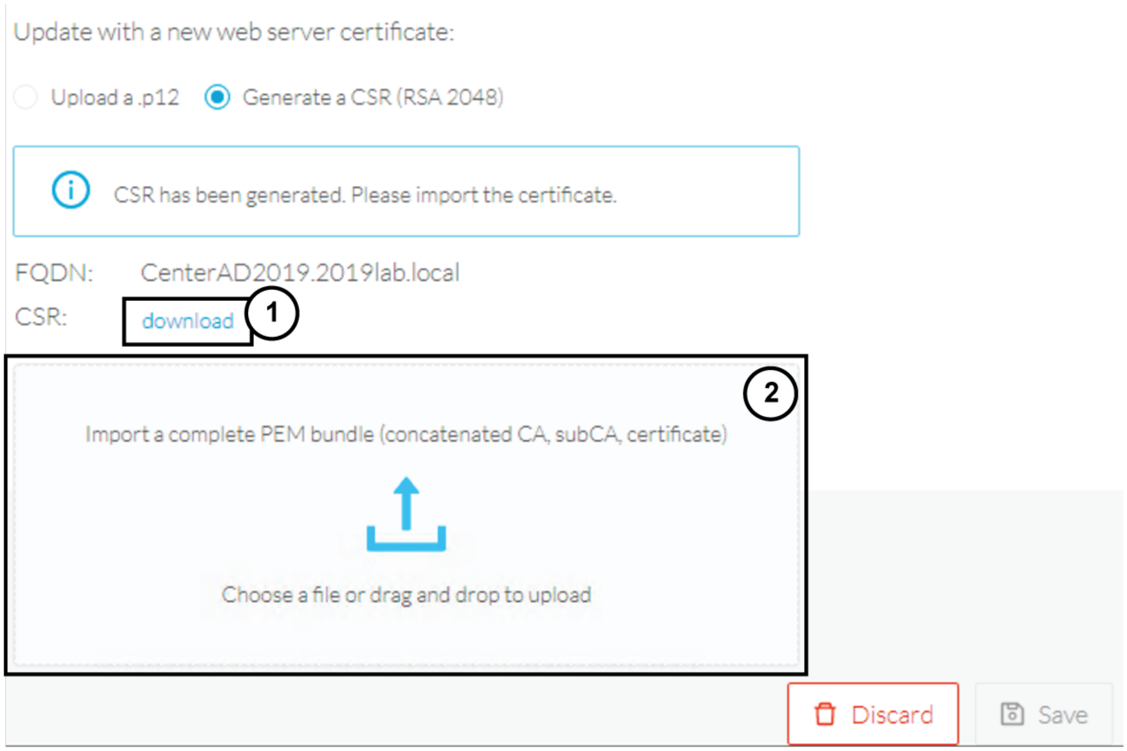
Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

CenterAD2019.2019lab.local

A message indicating that the CSR has been generated is displayed.

Step 4 Click the download button **(1)**.



Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

CSR has been generated. Please import the certificate.

FQDN: CenterAD2019.2019lab.local

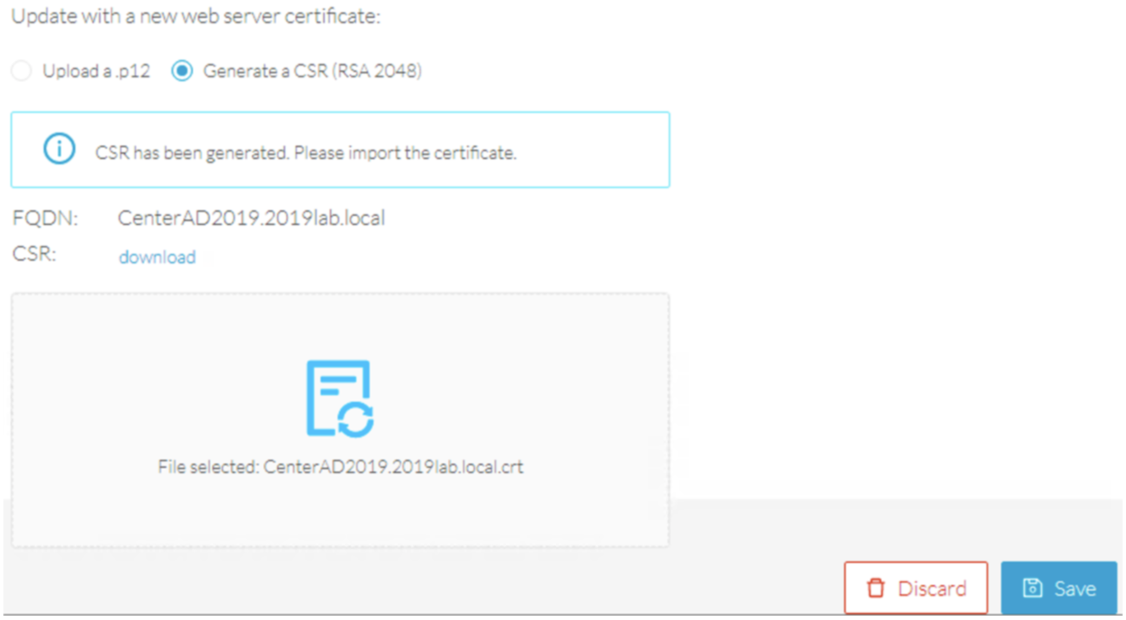
CSR: download

1
2
Import a complete PEM bundle (concatenated CA, subCA, certificate)
Choose a file or drag and drop to upload
Discard
Save

A <FQDN>.csr file is downloaded.

Step 5 Use the <FQDN>.csr file to generate a pem certificate from your enterprise Certification Authority.

Step 6 Once the pem certificate is generated, return to Cisco Cyber Vision and click the Import a complete PEM bundle button **(2)** or drag and drop it to import it.



Update with a new web server certificate:

○ Upload a .p12 ● Generate a CSR (RSA 2048)

CSR has been generated. Please import the certificate.

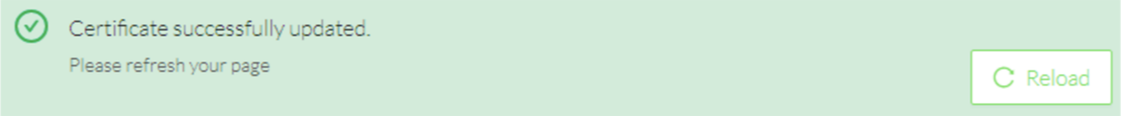
FQDN: CenterAD2019.2019lab.local

CSR: download

File selected: CenterAD2019.2019lab.local.crt

Step 7 Click Save.

The following message appears:



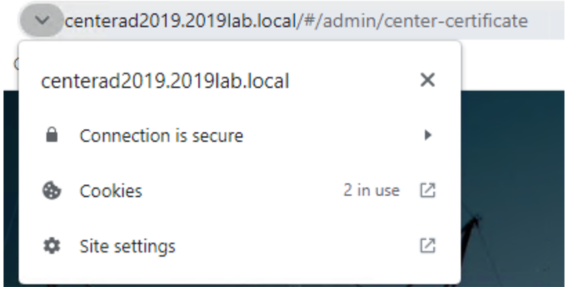
Certificate successfully updated.

Please refresh your page

Step 8 Click Reload.

Step 9 In your browser, use the DNS name to connect to your Cisco Cyber Vision instance.

The error message does not appear and the connection is secure.



centerad2019.2019lab.local/#/admin/center-certificate

centerad2019.2019lab.local

Connection is secure

What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 59.

If you are installing a standalone Center, you can start installing the sensors. To do so, refer to the corresponding Cisco Cyber Vision Sensor Installation Guides.

Configure Center data synchronization

This step is applicable to the Global Center and its synchronized Centers.

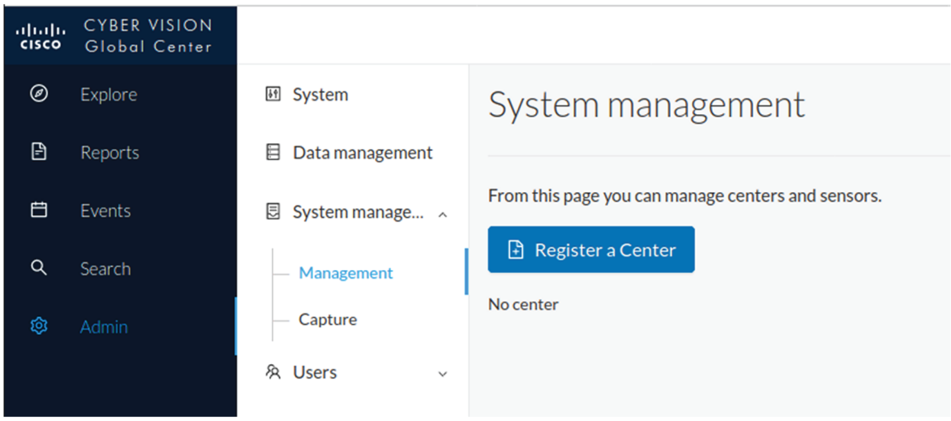
Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists of registering the Center in the Global Center and enrolling the Center to the Global Center. To do so, you need to open each's Cisco Cyber Vision's GUI.

Note To differentiate each user interface, check the top left corner of Cisco Cyber Vision's "Global Center" or "Center".

Procedure

Step 1 In the Global Center's Cisco Cyber Vision GUI, navigate to Admin > System Management > Management.

Step 2 Click the **Register a Center** button.



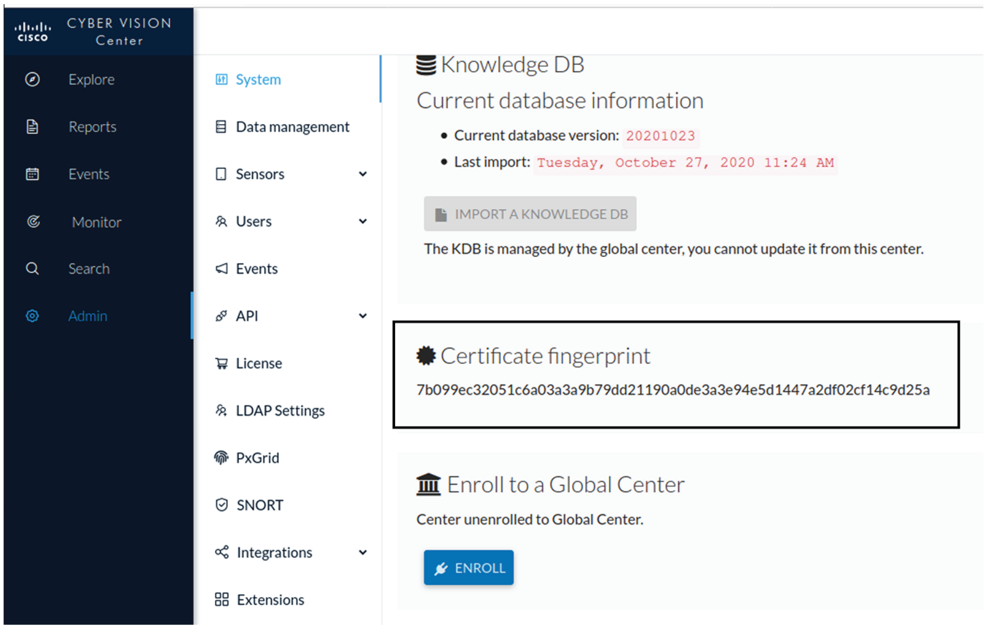
From this page you can manage centers and sensors.

No center

The window "Register a Center" pops up, ready to be filled. Now you must access the Center's GUI to retrieve its fingerprint.

Step 3 In the Center's Cisco Cyber Vision GUI, navigate to Admin > System.

Step 4 Scroll down to Certificate fingerprint and copy it.



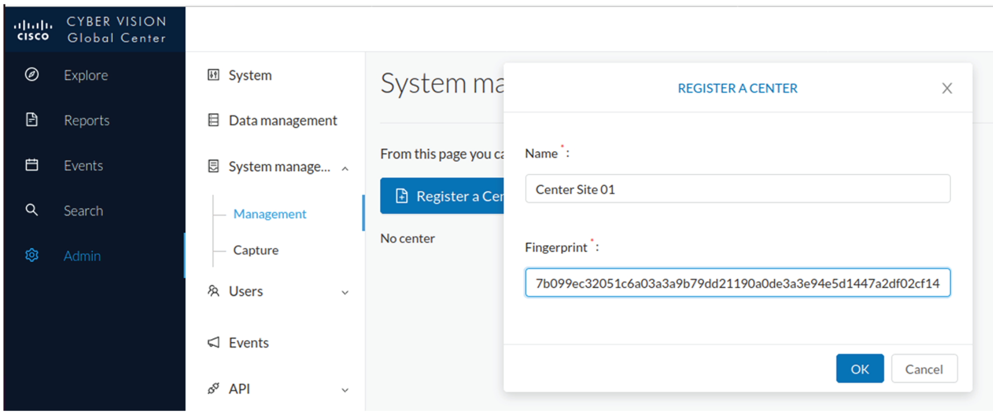
- Current database version: 20201023
- Last import: Tuesday, October 27, 2020 11:24 AM

The KDB is managed by the global center, you cannot update it from this center.

7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14c9d25a

Center unenrolled to Global Center.

Step 5 In the Global Center's GUI, give a name to the Center, and paste the Center's fingerprint into the corresponding field



From this page you ca

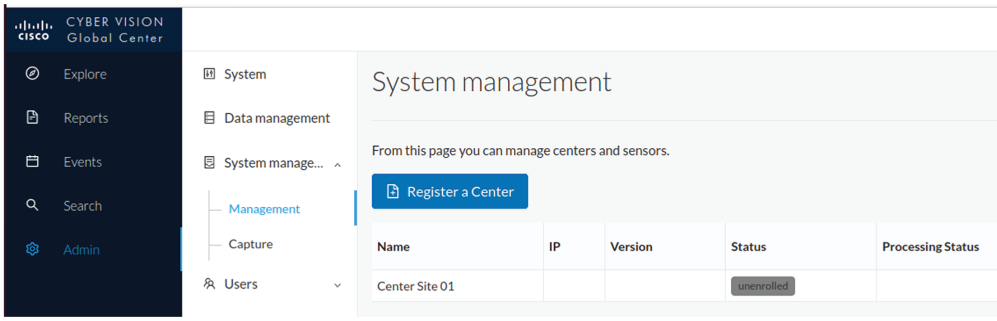
No center

Name * : Center Site 01

Fingerprint * : 7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14

Step 6 Click **OK**.

The Center appears in the list as unenrolled.



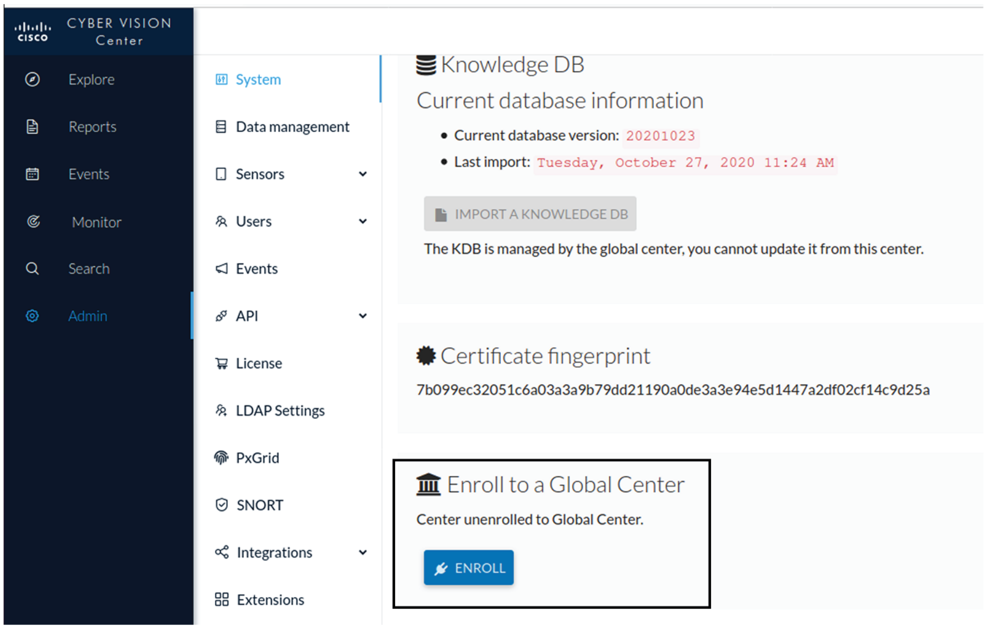
System management

From this page you can manage centers and sensors.

Name	IP	Version	Status	Processing Status
Center Site 01			unenrolled	

At this point you must switch to the Center's GUI and enroll it to the Global Center.

Step 7 In the Center's GUI, scroll down to Enroll a Global Center and click the **Enroll** button.



Knowledge DB

Current database information

- Current database version: 20201023
- Last import: Tuesday, October 27, 2020 11:24 AM

The KDB is managed by the global center, you cannot update it from this center.

Certificate fingerprint

7b099ec32051c6a03a3a9b79dd21190a0de3a3e94e5d1447a2df02cf14c9d25a

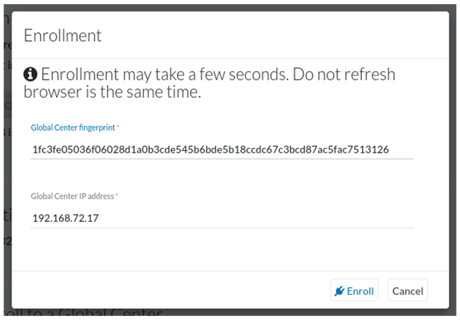
Enroll to a Global Center

Center unenrolled to Global Center.

The Enrollment window pops up.

Step 8 Copy the Global Center's fingerprint from its GUI's System administration page (same location as the Center's).

Step 9 Enter the Global Center's IP address and click **Enroll**.



Enrollment

Enrollment may take a few seconds. Do not refresh browser is the same time.

Global Center fingerprint *
1fc3fe05036f06028d1a0b3cde545b6bde5b18ccdc67c3bcd87ac5fac7513126

Global Center IP address *
192.168.72.17

Once the synchronization is complete, it is indicated that the Center is enrolled to the Global Center.

CHAPTER 6

Configure a Center DPI

Center DPI

Cyber Vision Center Deep Packet Inspection (DPI) is a virtual sensor that

- operates within the center environment,
- analyzes industrial network traffic at a granular level by inspecting application flows locally, and
- adds metadata to the Cyber Vision Center for centralized storage, analytics, and visualization.

Configure Center DPI

Enable Center DPI to function as a virtual sensor in Center for monitoring and analyzing network traffic.

Before you begin

Ensure you have an available Ethernet interface for Center DPI traffic:

- SPAN:
  - Single interface: eth1
  - Dual interfaces: eth2
- ERSPAN:
  - Single interface: eth0
  - Dual interfaces: eth0 and eth1
  - For optimal performance, use a dedicated interface if possible.

Procedure

Step 1 Open the Center shell prompt and run the `sbs-netconf` command.

Step 2 Select the interface to configure, based on your SPAN or ERSPAN setup.

Step 3 Select the configuration type as **DPI+Snort port**.

Step 4 Select an encapsulation type.

- **None** for SPAN configurations.
- **erspan2** for ERSPAN type 2 remote SPAN.
- **erspan3** for ERSPAN type 3 remote SPAN.

Step 5 If you select **erspan2** or **erspan3** as the encapsulation type, enter an IPv4 address to receive traffic.

A new sensor is created and appears in **Admin** > **Sensors** > **Sensor Explorer**, ready to monitor network traffic based on the chosen configuration.

What to do next

- To view traffic statistics from the new sensor, navigate in the Center interface to **Explorer** > **All Data** > **Device list** and select the device for more details.
- To disable Snort on the Center DPI interface, follow these steps.
  1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
  2. Select the sensor and click **Disable IDS**.

CHAPTER 7

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.

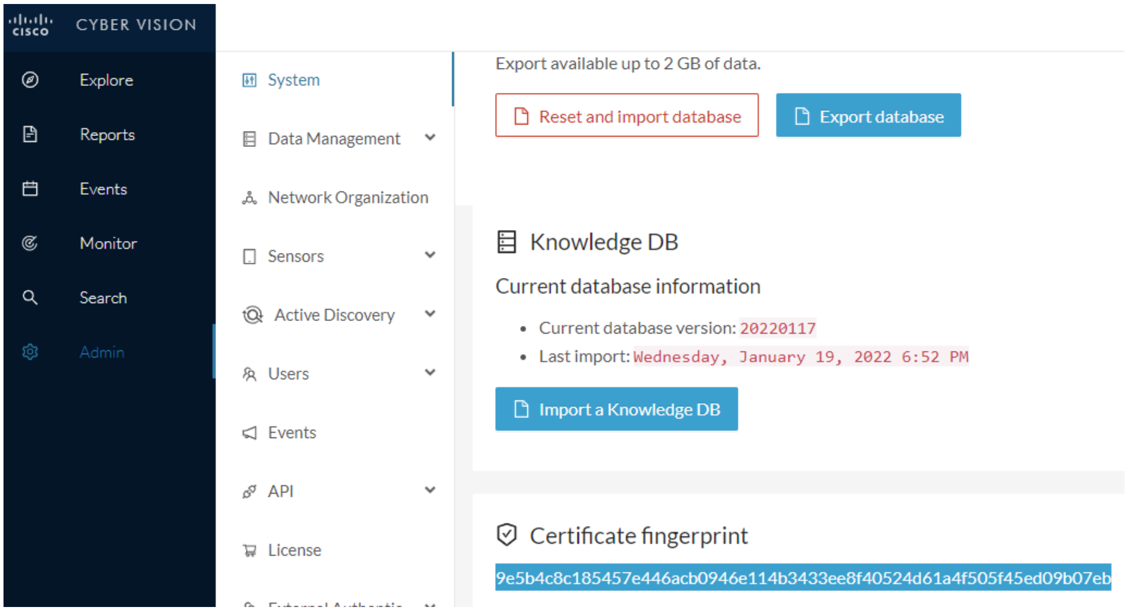
Center enrollment

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

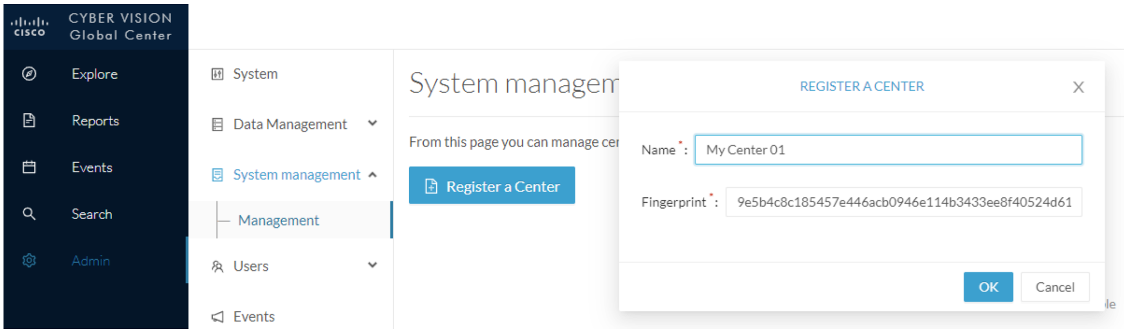
Certificate fingerprint

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



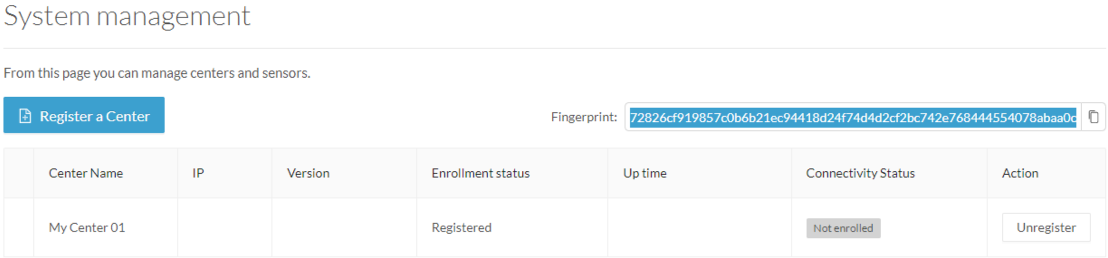
System managem

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

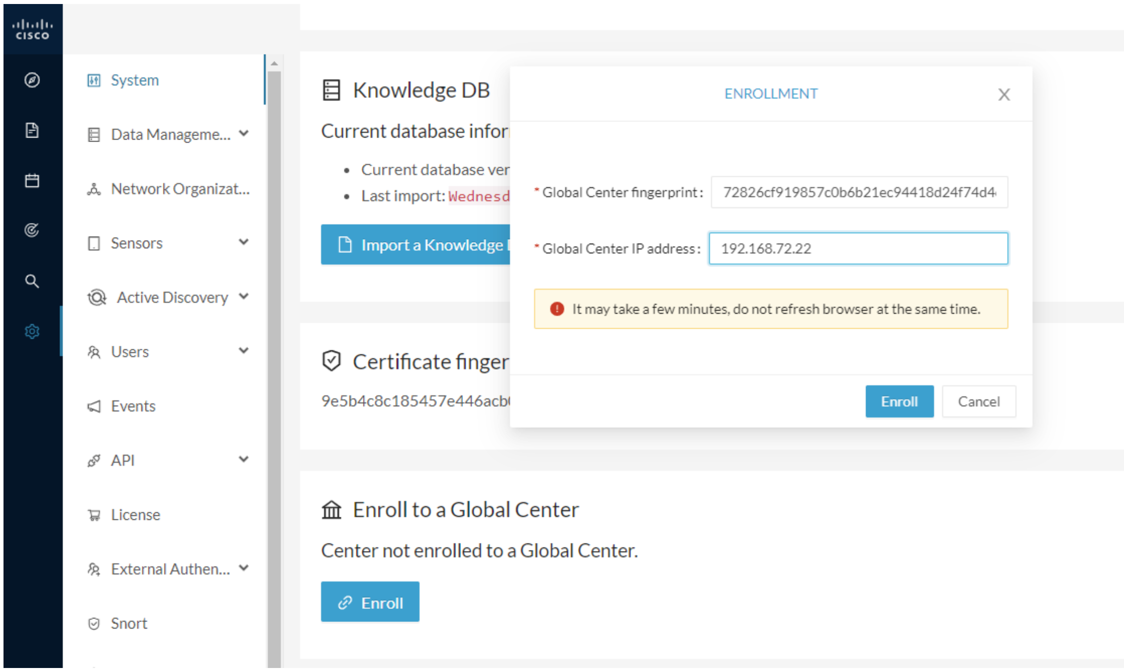
	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
	My Center 01			Registered		Not enrolled	Unregister

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**



- Current database ver
- Last import: Wednesd

9e5b4c8c185457e446acb

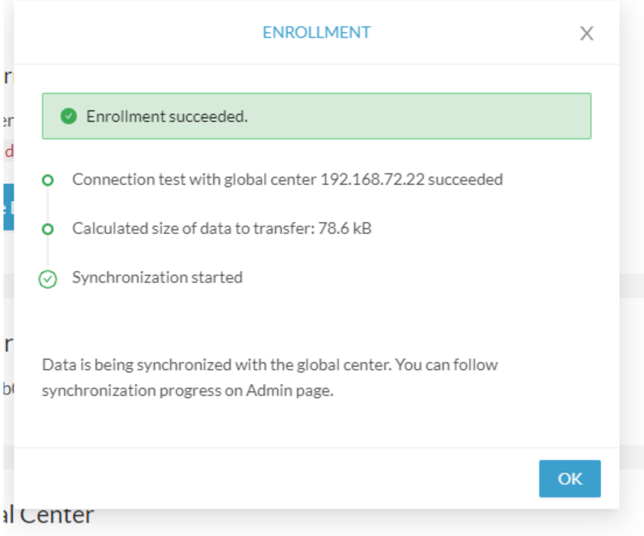
Center not enrolled to a Global Center.

* 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**.



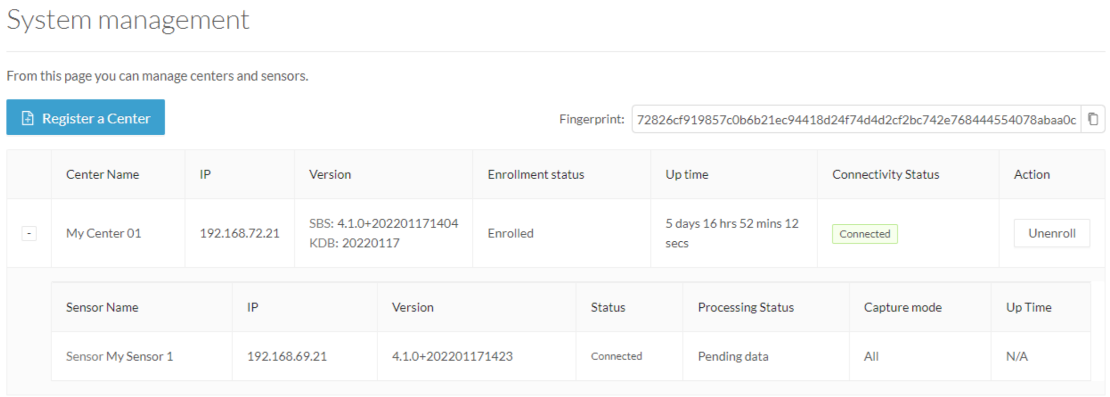
Enrollment succeeded.

- 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

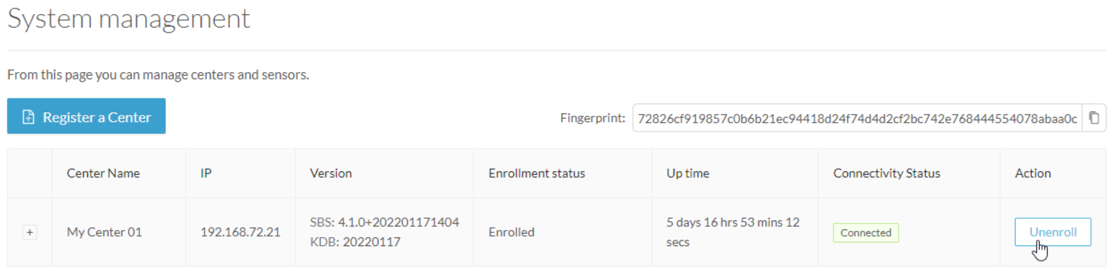
A Center can be unenrolled whenever it is needed, for example as a maintenance operation to replace the Center or the Global Center. This will delete all the Center's data in the Global Center.

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

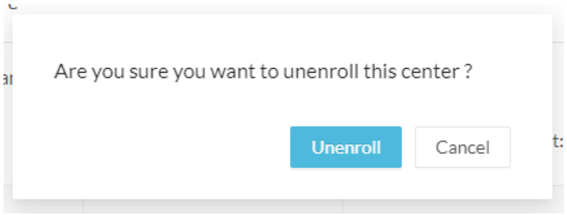
From this page you can manage centers and sensors.

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.

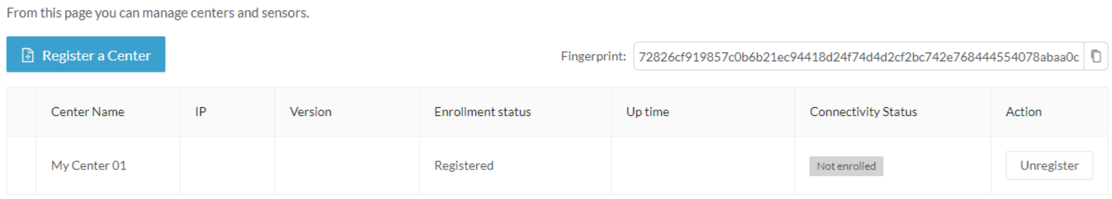
Step 3 A popup asking for confirmation appears. Click **Unenroll** to start the process.



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.

Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c

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

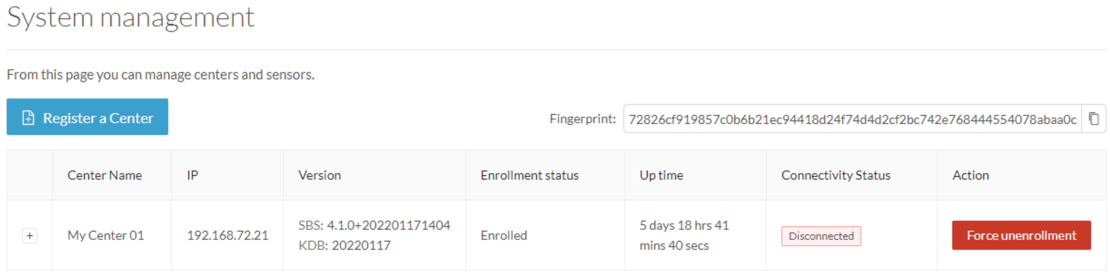
Force the unenrollement of a Center

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.

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 8

Upgrade procedures

Architecture with a Global Center

Check the Global Center and Centers' health

It is highly recommended that you check the health of the Centers connected to the Global Center and of the Global Center itself before proceeding to the update. To do so:

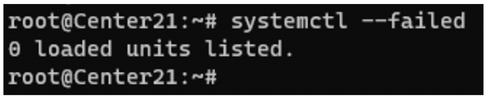
Procedure

Step 1 Connect to the Center in SSH.

Step 2 Type the following command:

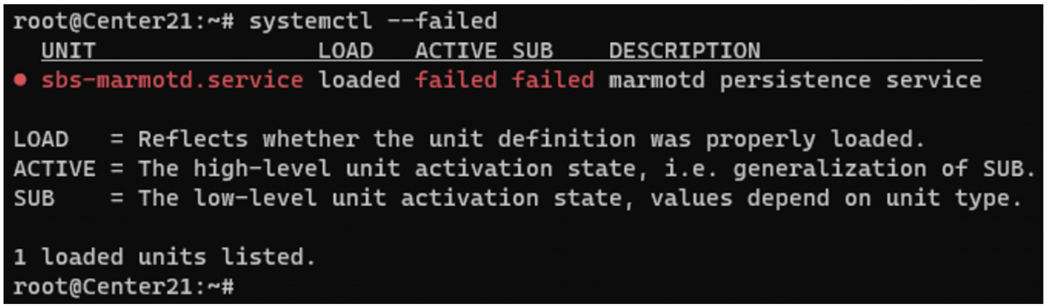
```
systemctl --failed
```

The number of listed sbs-* units should be 0, otherwise the failure must be fixed before proceeding with the update.



```
root@Center21:~# systemctl --failed
0 loaded units listed.
root@Center21:~#
```

If one or several sbs services are in failed state like below, it has to be fixed before proceeding to the update.



```
root@Center21:~# systemctl --failed
  UNIT                LOAD   ACTIVE SUB    DESCRIPTION
● sbs-marmotd.service loaded failed failed marmotd persistence service

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

1 loaded units listed.
root@Center21:~#
```

Usually, a reboot of the Center is enough to solve the issue. If not, contact the product support.

Step 3 Repeat the previous steps for the other Centers and the Global Center.

Update the Global Center

In the case of a distributed architecture, **you must first update the Global Center, then its Centers**.

You can do so through the corresponding Center's Cisco Cyber Vision application or using its Command Line Interface.

To update the Global Center:

- Through the Cisco Cyber Vision application:
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-combined-<VERSION>.dat
  2. Navigate to Admin > System.
  3. Click **System Update**.
  4. Browse to select the update file.
- Through the Command Line Interface (CLI):
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-center-<VERSION>.dat
  2. Launch the update using the following command:

     ```
     sbs-update install /data/tmp/CiscoCyberVision-update-center-<VERSION>.dat
     ```

To update the Centers:

Connect to each Center's Cisco Cyber Vision application or CLI and repeat the same procedure used to update the Global Center.

Update the sensors

The update of the sensors is done from their corresponding Center (not from the Global Center). You must repeat the following procedures from each of your Centers to cover all sensors of your industrial network. Procedures differ between hardware sensors and IOx sensors.

Update hardware sensors

To update hardware sensors:

If you used the combined file to update the Center which owned the sensor, the hardware sensors (IC3000 and Sentryo Sensors) were updated at the same time.

If not, the update needs to be done from the Command Line Interface (CLI):

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-update-sensor-<VERSION>.dat

Step 2 Launch the update using the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-<VERSION>.dat
```

Update IOx sensors

To update IOx sensors:

If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable by the Center.

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-sensor-management-<VERSION>.ext

Step 2 In Cisco Cyber Vision, navigate to Admin > Extensions.

Step 3 In the Actions column, click the **Update** button, and browse to select the update file.

If one or several sensors were not updated by the extension update:

Step 4 Navigate to Admin > Sensors > Sensor Explorer.

Step 5 Click **Manage Cisco devices**, then click **Update Cisco devices**.

A pop up with all remaining IOx sensors connected to the Center appears. Click **Update**.

If you have not installed one or several sensors with the sensor management extension, you can upgrade them with the sensor package from the platform's local manager or from the platform's Command Line Interface. This procedure is detailed in the corresponding sensor installation guide.

- Cisco IE3x00 and Cisco IR1101 file names: CiscoCyberVision-IOx-aarch64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64-<VERSION>.tar
- Catalyst 9300 and Catalyst 9400 file names: CiscoCyberVision-IOx-x86-64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<VERSION>.tar

Architecture with a single Center

Update the Center

You can update the Center through its Cisco Cyber Vision application or using its Command Line Interface.

- Through the Cisco Cyber Vision application:
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-combined-<VERSION>.dat
  2. Navigate to Admin > System.
  3. Click **System Update**.
  4. Browse to select the update file.
- Through the Command Line Interface (CLI):
  1. Go to cisco.com and retrieve the following file:

     File name: CiscoCyberVision-update-center-<VERSION>.dat
  2. Launch the update using the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-<VERSION>.dat
```

Update the sensors

Sensor upgrade is done from the Center. Update procedures differ between hardware sensors and IOx sensors.

Update hardware sensors

To update hardware sensors:

If you used the combined file to update the Center which owned the sensor, the hardware sensors (IC3000 and Sentryo Sensors) were updated at the same time.

If not, the update needs to be done from the Command Line Interface (CLI):

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-update-sensor-<VERSION>.dat

Step 2 Launch the update using the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-<VERSION>.dat
```

Update IOx sensors

To update IOx sensors:

If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable by the Center.

Procedure

Step 1 Go to cisco.com and retrieve the following file:

File name: CiscoCyberVision-sensor-management-<VERSION>.ext

Step 2 In Cisco Cyber Vision, navigate to Admin > Extensions.

Step 3 In the Actions column, click the **Update** button, and browse to select the update file.

If one or several sensors were not updated by the extension update:

Step 4 Navigate to Admin > Sensors > Sensor Explorer.

Step 5 Click **Manage Cisco devices**, then click **Update Cisco devices**.

A pop up with all remaining IOx sensors connected to the Center appears. Click **Update**.

If you have not installed one or several sensors with the sensor management extension, you can upgrade them with the sensor package from the platform's local manager or from the platform's Command Line Interface. This procedure is detailed in the corresponding sensor installation guide.

- Cisco IE3x00 and Cisco IR1101 file names: CiscoCyberVision-IOx-aarch64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64-<VERSION>.tar
- Catalyst 9300 and Catalyst 9400 file names: CiscoCyberVision-IOx-x86-64-<VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<VERSION>.tar

CHAPTER 9

Certificate renewal

The certificates generated by Cisco Cyber Vision have a validity of two years.

Certificates renewal should be automatic. However, manual procedures to renew the Global Center certificate and Centers with sync exist in case automatic ones are not possible.

- Renew the certificate of a Center, on page 77

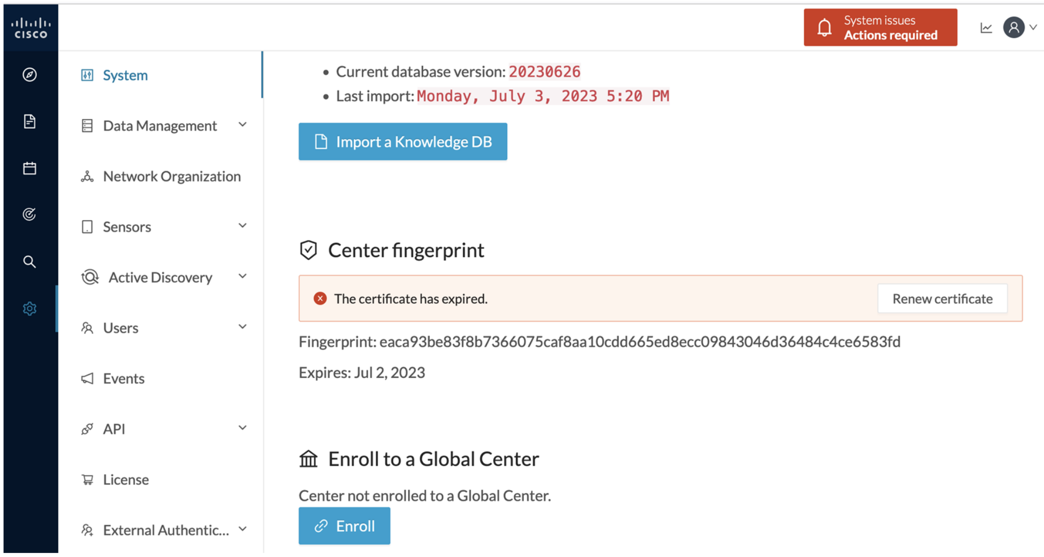
Renew the certificate of a Center

This procedure applies to Centers, Global Centers and Centers with sync. Extra steps are required to update fingerprints in the case of an architecture with a Global Center.

Procedure

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

Step 2 Slide down to Center fingerprint.



- Current database version: 20230626
- Last import: Monday, July 3, 2023 5:20 PM

Center fingerprint

The certificate has expired.

Fingerprint: eaca93be83f8b7366075caf8aa10cdd665ed8ecc09843046d36484c4ce6583fd

Expires: Jul 2, 2023

Enroll to a Global Center

Center not enrolled to a Global Center.

A message indicates that the certificare has expired.

Step 3 Click **Renew certificate**.

A warning page will be displayed at next login.

Step 4 Click **Advanced**, then **Accept the Risk and Continue**.

What to do next

In the case you're performing a certificate renewal within a Global Center architecture, you must follow the procedures below to update fingerprints according to the Center type.

Update the Global Center fingerprint

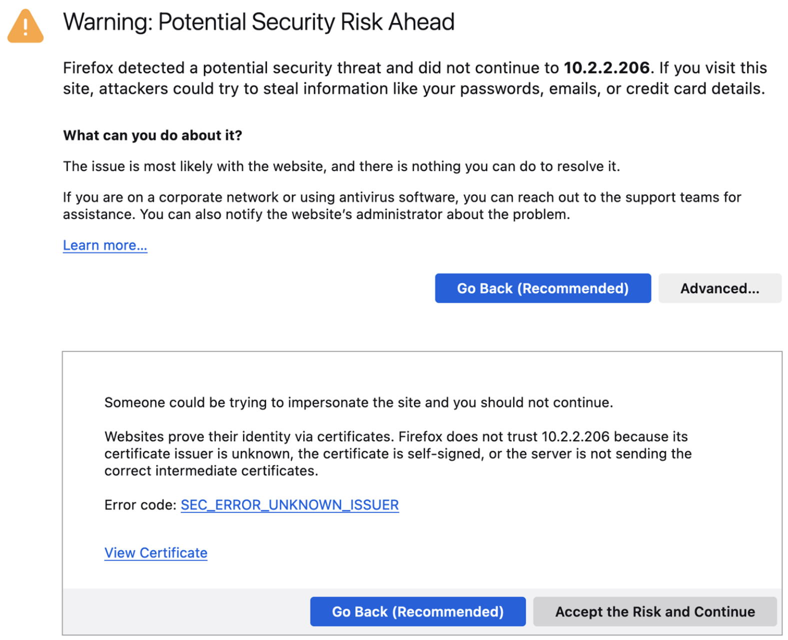
Before you begin

You need access to the Global Center and to all its Centers with sync.

Procedure

Step 1 Access the **Global Center**.

This warning page indicates that the certificate has been renewed.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.2.2.206**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

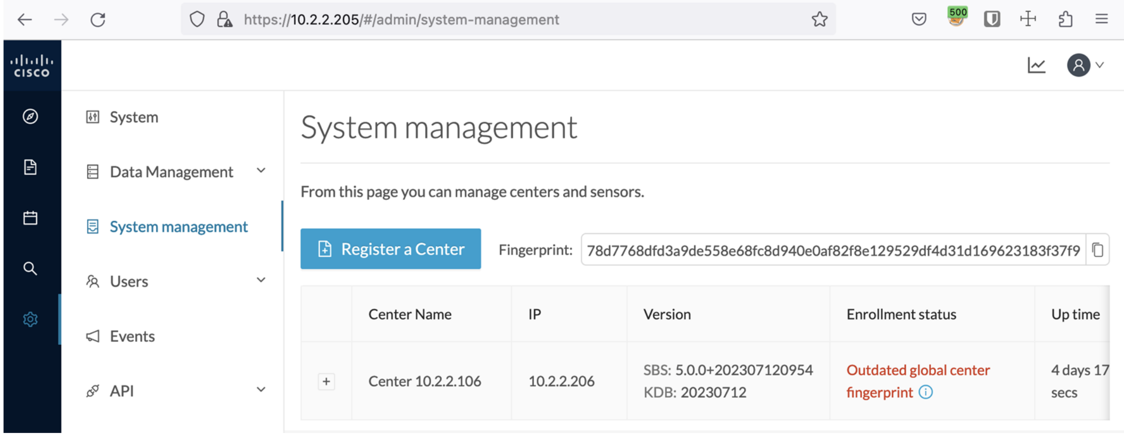
Websites prove their identity via certificates. Firefox does not trust 10.2.2.206 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Step 2 Click **Advanced**, then **Accept the Risk and Continue**.

Step 3 Login to the Global Center.

Step 4 Navigate to the System management page.



System management

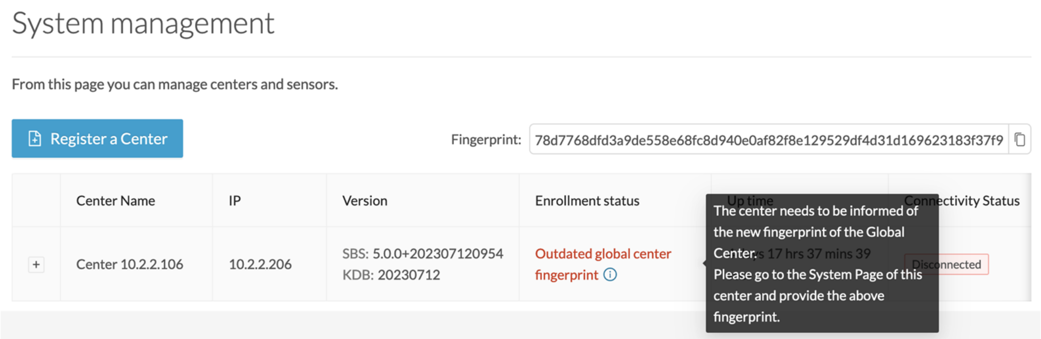
From this page you can manage centers and sensors.

Register a Center Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9

	Center Name	IP	Version	Enrollment status	Up time
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated global center fingerprint ⓘ	4 days 17 secs

In the Center list, you can see the Center with sync which must be updated with the Global Center's fingerprint.

Step 5 Copy the Global Center fingerprint.



System management

From this page you can manage centers and sensors.

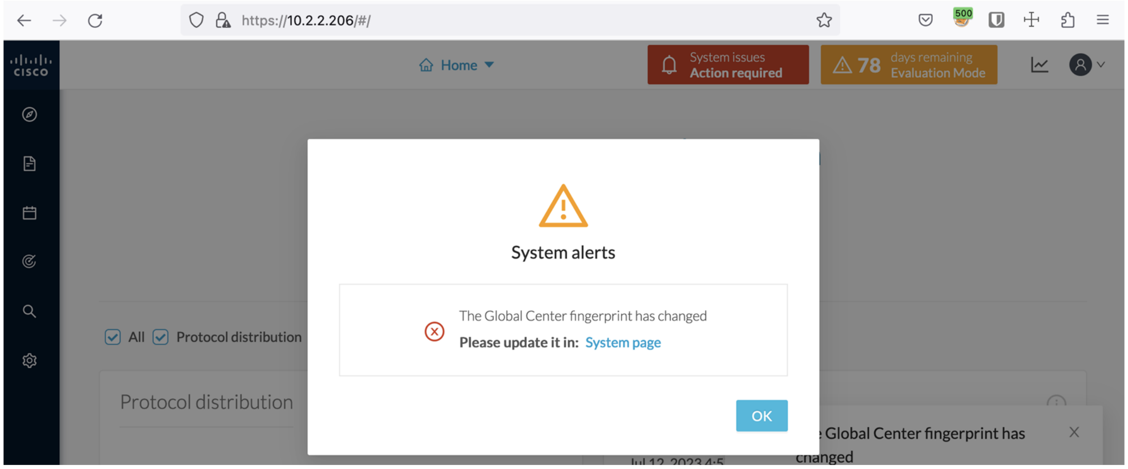
Register a Center Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated global center fingerprint ⓘ	s 17 hrs 37 mins 39	Disconnected

The center needs to be informed of the new fingerprint of the Global Center.
Please go to the System Page of this center and provide the above fingerprint.

Step 6 Login to the **Center with sync**.

The following system alert pops up, indicating that the Global Center fingerprint has changed with a link to the administration system page to update it.



System alerts

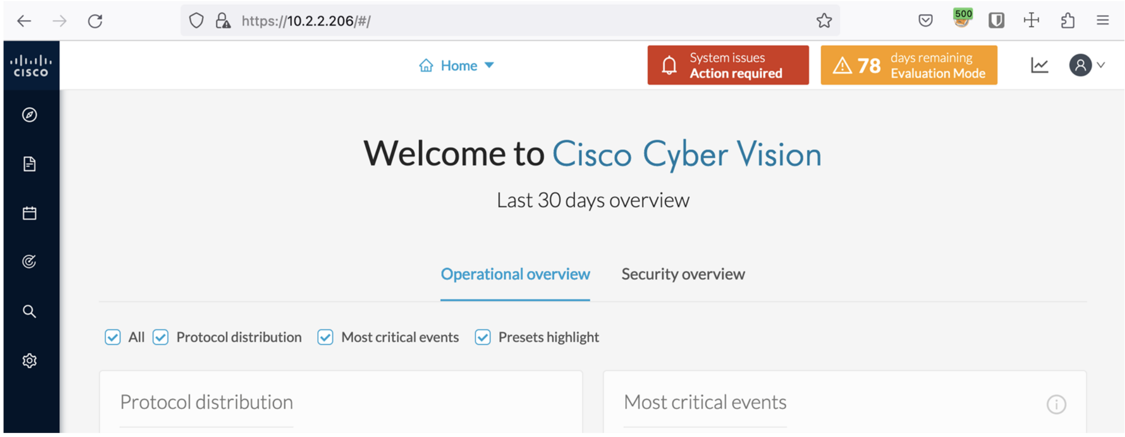
The Global Center fingerprint has changed
Please update it in: System page

OK

Global Center fingerprint has changed

Step 7 Click **OK**.

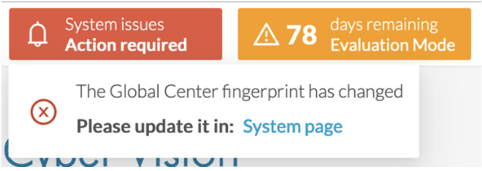
A red banner is displayed at the top of Cisco Cyber Vision's user interface.



Welcome to Cisco Cyber Vision

Last 30 days overview

If you click the red banner, you will see the same message that appeared in the previous popup, with a link to the System page to update the Global Center fingerprint.



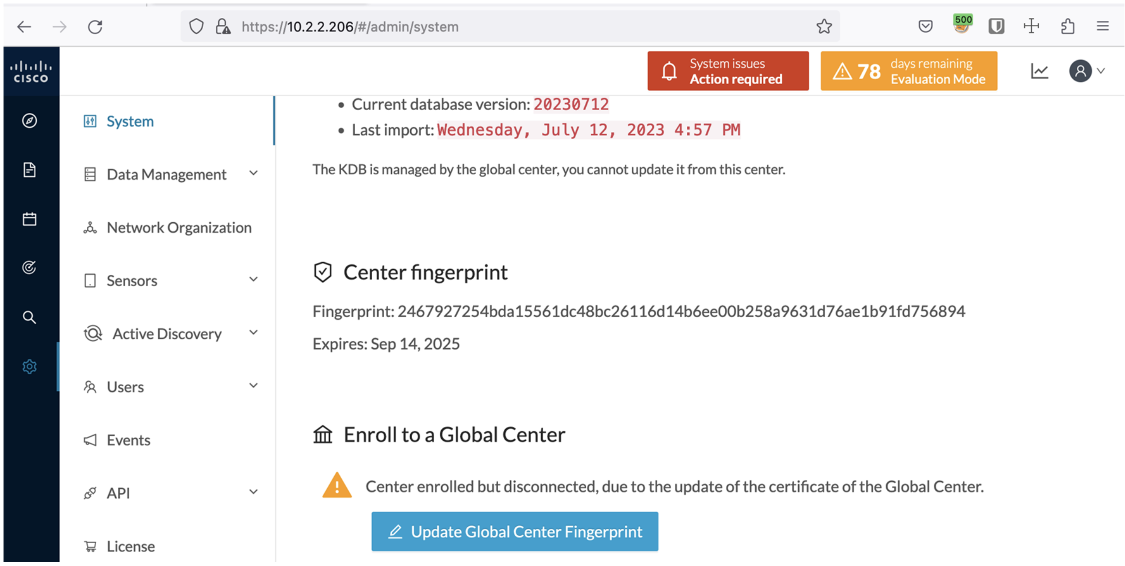
The Global Center fingerprint has changed

Please update it in: System page

Step 8 In the System page, slide down to Enroll to a Global Center.

It is indicated that the Center is enrolled but disconnected.

Step 9 Click **Update Global Center Fingerprint**.



- Current database version: 20230712
- Last import: Wednesday, July 12, 2023 4:57 PM

The KDB is managed by the global center, you cannot update it from this center.

Center fingerprint

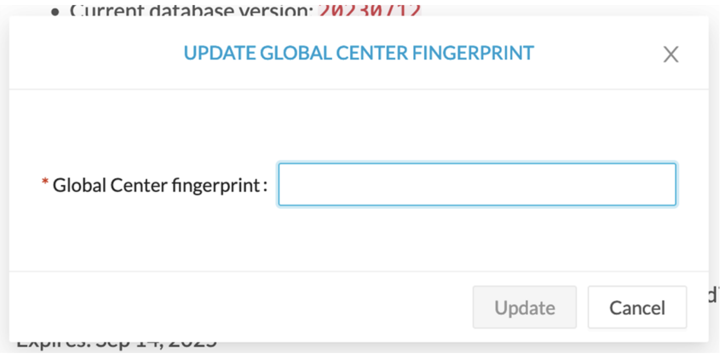
Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894

Expires: Sep 14, 2025

Enroll to a Global Center

Center enrolled but disconnected, due to the update of the certificate of the Global Center.

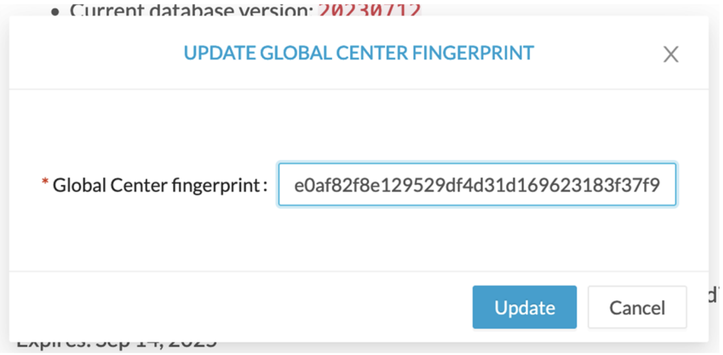
The Update Global Center fingerprint window pops up.



UPDATE GLOBAL CENTER FINGERPRINT

* Global Center fingerprint :

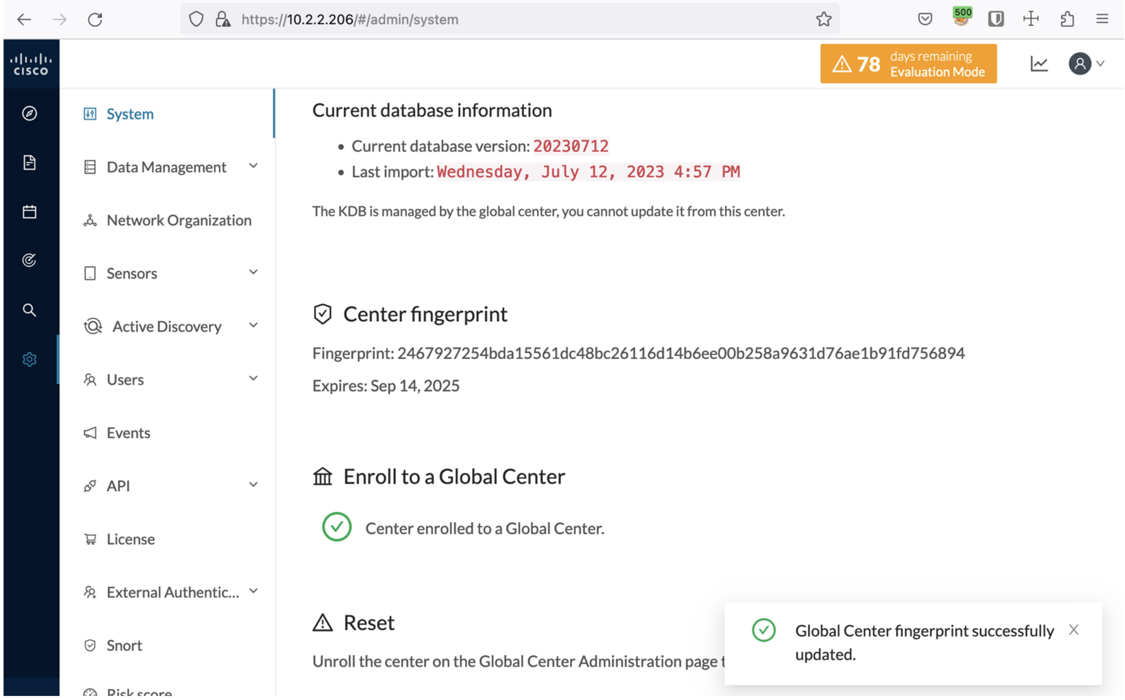
Step 10 Paste the Global Center fingerprint and click **Update**.



UPDATE GLOBAL CENTER FINGERPRINT

* Global Center fingerprint : e0af82f8e129529df4d31d169623183f37f9

A message indicating that the Global Center fingerprint successfully updated appears and the Global Center enrollment status switches to enrolled.



Current database information

- Current database version: 20230712
- Last import: Wednesday, July 12, 2023 4:57 PM

The KDB is managed by the global center, you cannot update it from this center.

Center fingerprint

Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894

Expires: Sep 14, 2025

Enroll to a Global Center

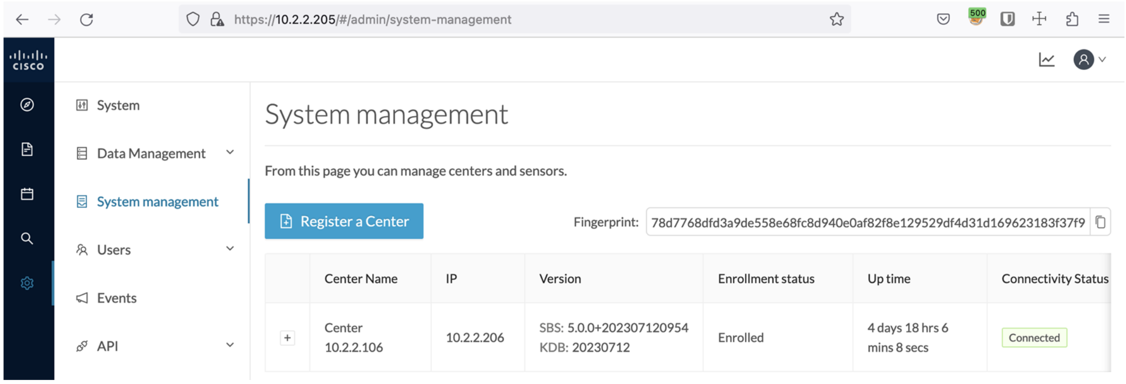
Center enrolled to a Global Center.

Reset

Unroll the center on the Global Center Administration page t

Global Center fingerprint successfully updated.

In the Global Center System management page the Center appears as Connected.



System management

From this page you can manage centers and sensors.

Fingerprint: 78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Enrolled	4 days 18 hrs 6 mins 8 secs	Connected

What to do next

Repeat the previous steps for each Center with sync.

Update a Center with sync fingerprint

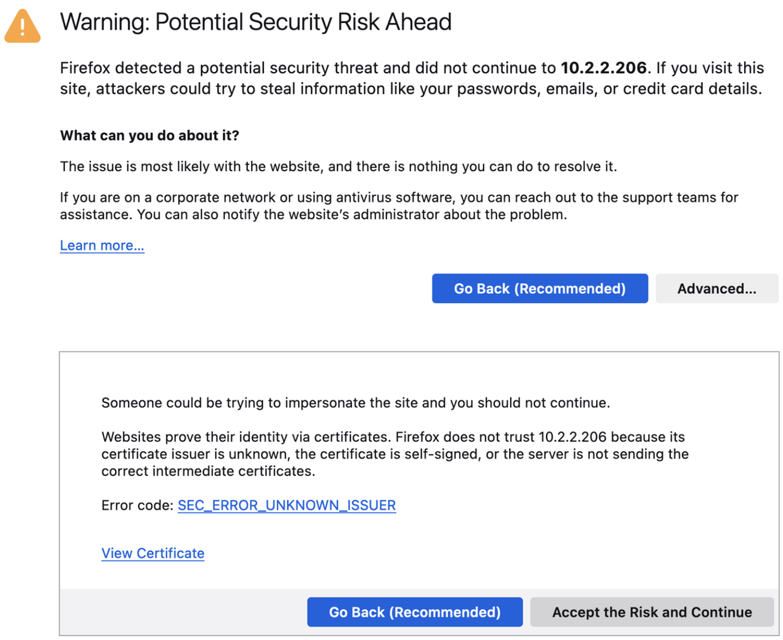
Before you begin

You need access to the Center with sync and its Global Center.

Procedure

Step 1 Access the **Center with sync**.

This warning page indicates that the certificate has been renewed.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.2.2.206**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

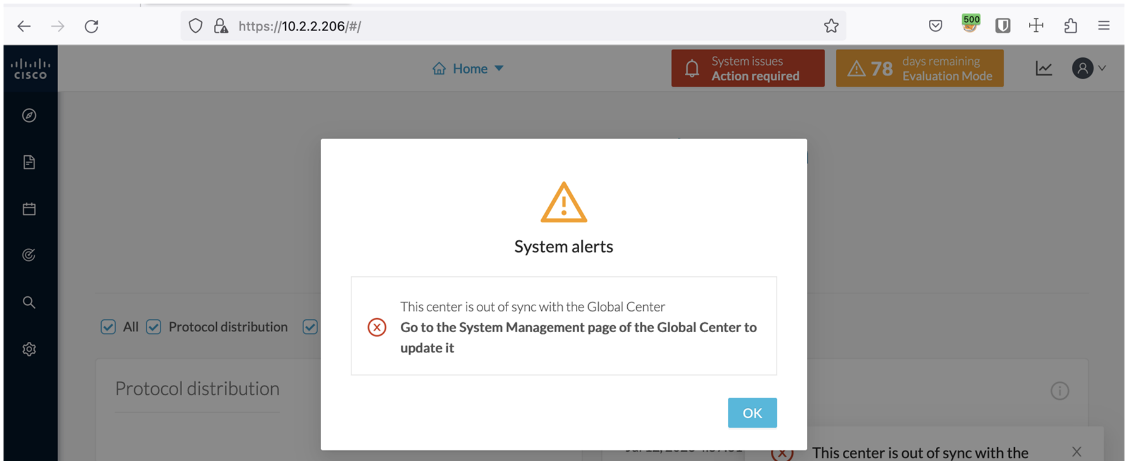
Websites prove their identity via certificates. Firefox does not trust 10.2.2.206 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Step 2 Click **Advanced**, then **Accept the Risk and Continue**.

Step 3 Login to the Center.

An alert appears indicating that the Center is out of sync with the Global Center and the actions to take on the Global Center.



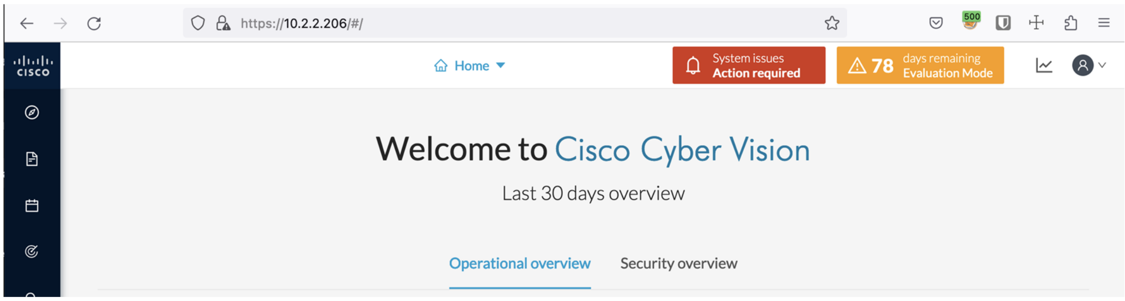
System alerts

This center is out of sync with the Global Center

Go to the System Management page of the Global Center to update it

Step 4 Click **OK**.

A red banner is displayed at the top of Cisco Cyber Vision's user interface.

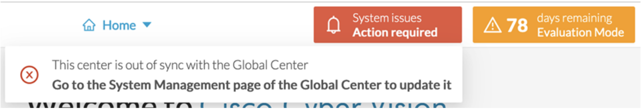


https://10.2.2.206/#/

Welcome to Cisco Cyber Vision

Last 30 days overview

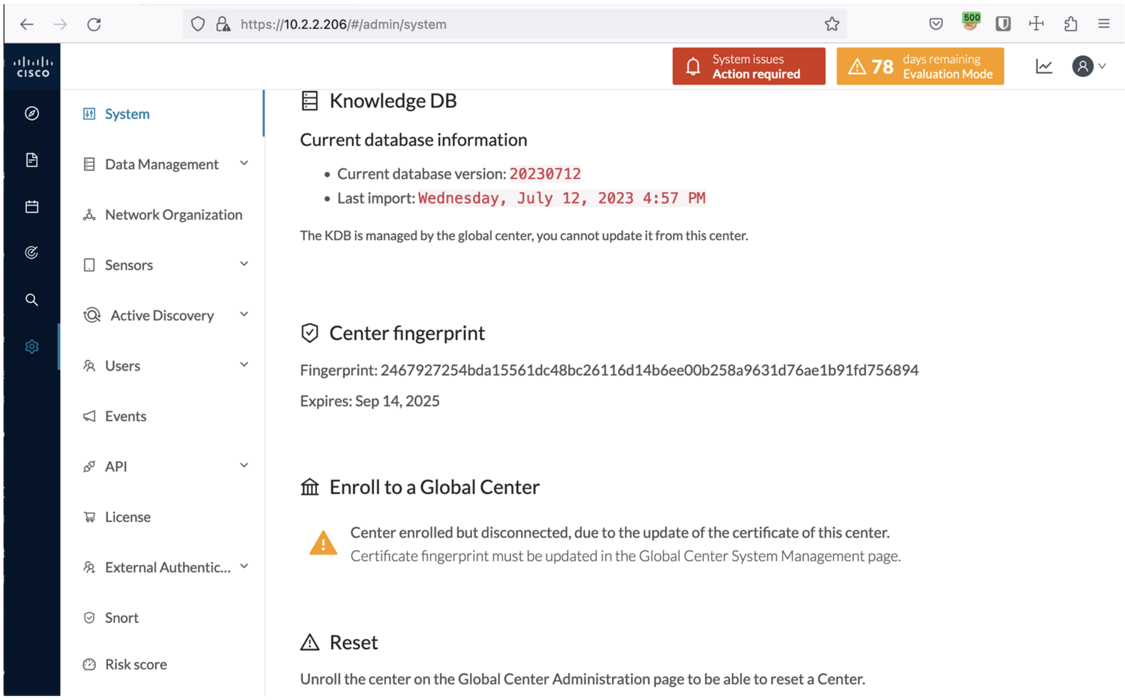
If you click the red banner, you will see the same message that appeared in the previous popup.



This center is out of sync with the Global Center

Go to the System Management page of the Global Center to update it

In the Center's administration system page, the Enroll to a Global Center state indicates that the Center is enrolled but disconnected.



https://10.2.2.206/#/admin/system

Knowledge DB

Current database information

- Current database version: 20230712
- Last import: Wednesday, July 12, 2023 4:57 PM

The KDB is managed by the global center, you cannot update it from this center.

Center fingerprint

Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894

Expires: Sep 14, 2025

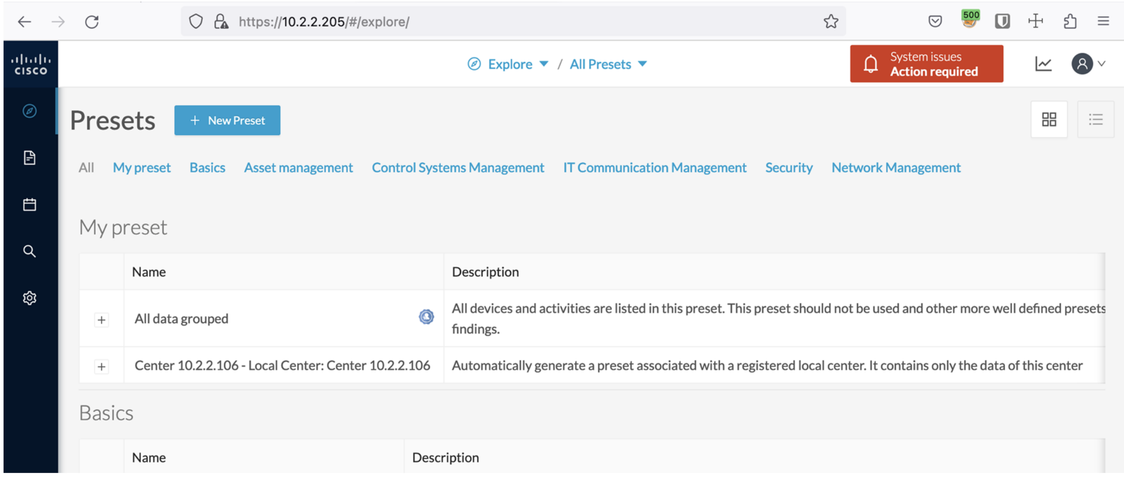
Enroll to a Global Center

Center enrolled but disconnected, due to the update of the certificate of this center.
Certificate fingerprint must be updated in the Global Center System Management page.

Reset

Unroll the center on the Global Center Administration page to be able to reset a Center.

Step 5 Access the **Global Center**.



Presets

+ New Preset

All | My preset | Basics | Asset management | Control Systems Management | IT Communication Management | Security | Network Management

My preset

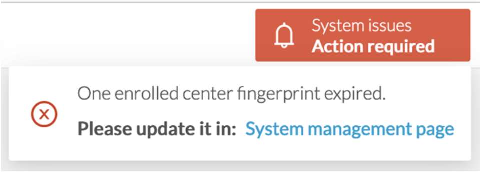
	Name	Description
+	All data grouped	All devices and activities are listed in this preset. This preset should not be used and other more well defined presets findings.
+	Center 10.2.2.106 - Local Center: Center 10.2.2.106	Automatically generate a preset associated with a registered local center. It contains only the data of this center

Basics

	Name	Description

Step 6 Click the red banner.

A message indicating that a Center fingerprint is expired is displayed with a shortlink to access the administration system management page.

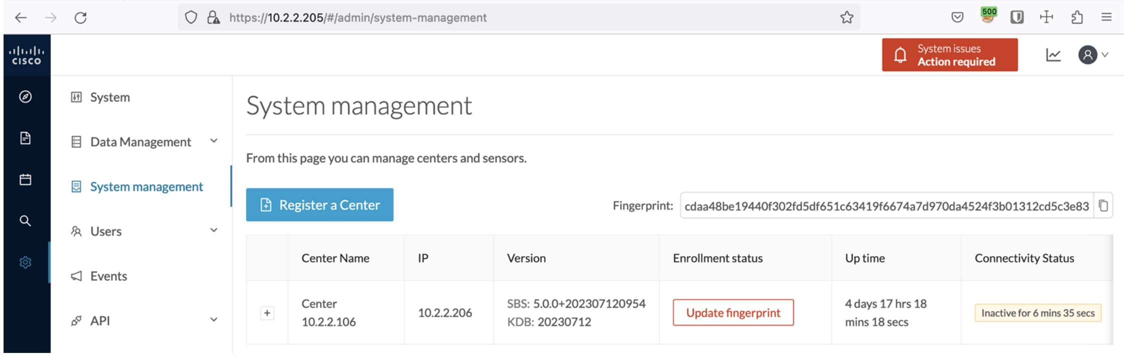


System issues
Action required

One enrolled center fingerprint expired.

Please update it in: System management page

In the System management page you can see the Center with its enrollment status as Update fingerprint and Connectivity status as Inactive.



System management

From this page you can manage centers and sensors.

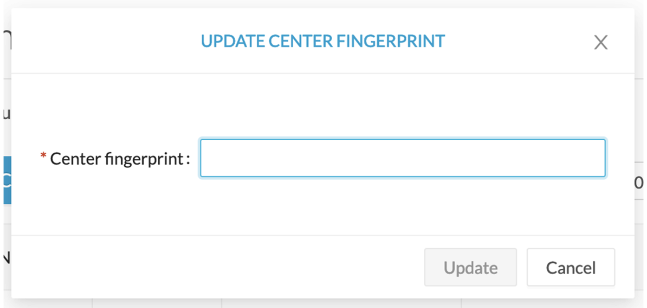
Register a Center

Fingerprint: cdaa48be19440f302fd5df651c63419f6674a7d970da4524f3b01312cd5c3e83

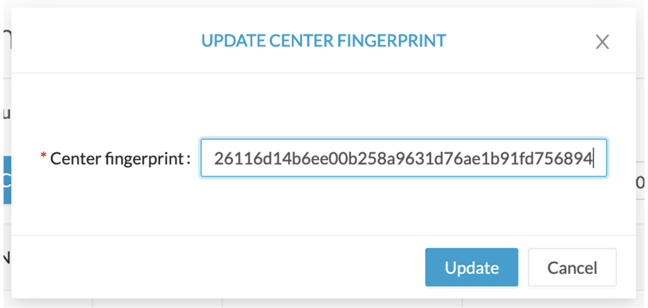
	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Update fingerprint	4 days 17 hrs 18 mins 18 secs	Inactive for 6 mins 35 secs

Step 7 Click the **Update fingerprint** status button.

An Update Center fingerprint window pops up.



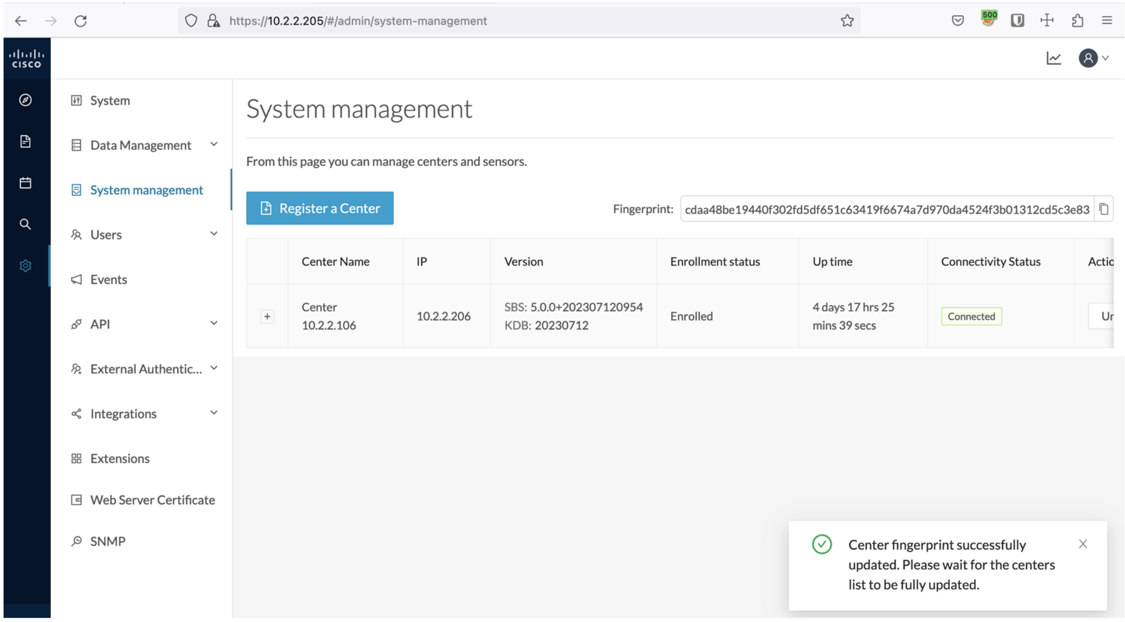
Step 8 Paste the Center fingerprint.



* Center fingerprint : 26116d14b6ee00b258a9631d76ae1b91fd756894

A message indicating that the Center fingerprint successfully updated appears.

Wait a few moments for the Center enrollment status to switch to Enrolled and the connectivity status to Connected.



System management

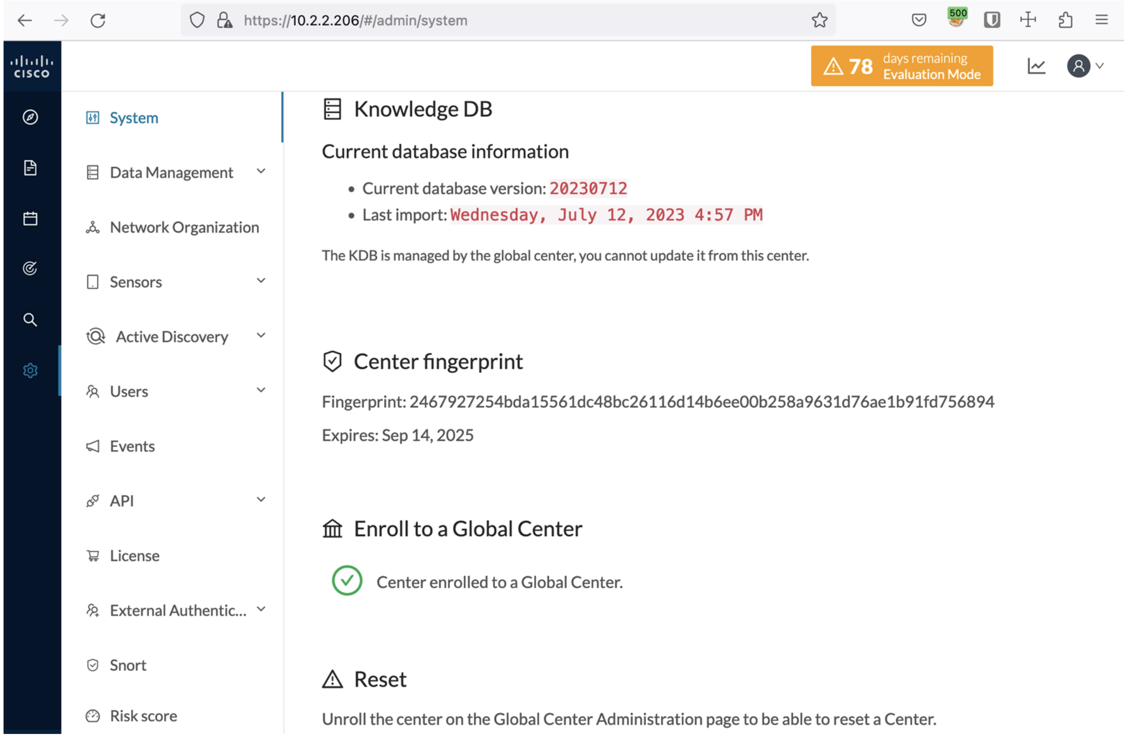
From this page you can manage centers and sensors.

Fingerprint: cdaa48be19440f302fd5df651c63419f6674a7d970da4524f3b01312cd5c3e83

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Actic
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Enrolled	4 days 17 hrs 25 mins 39 secs	Connected	Ur

Center fingerprint successfully updated. Please wait for the centers list to be fully updated.

In the **Global Center**'s administration system page the Center state is indicated as enrolled.



Knowledge DB

Current database information

- Current database version: 20230712
- Last import: Wednesday, July 12, 2023 4:57 PM

The KDB is managed by the global center, you cannot update it from this center.

Center fingerprint

Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b258a9631d76ae1b91fd756894

Expires: Sep 14, 2025

Enroll to a Global Center

Center enrolled to a Global Center.

Reset

Unroll the center on the Global Center Administration page to be able to reset a Center.

CHAPTER 10

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

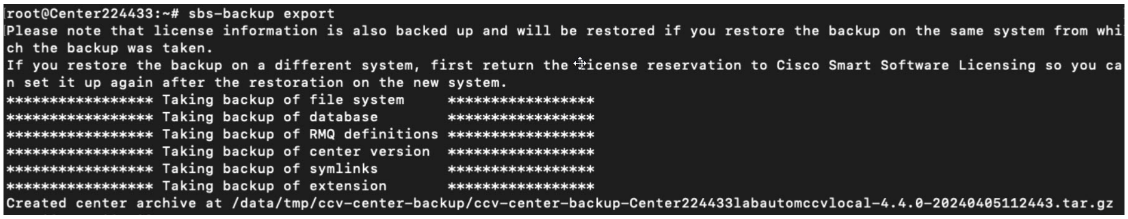
Procedure

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

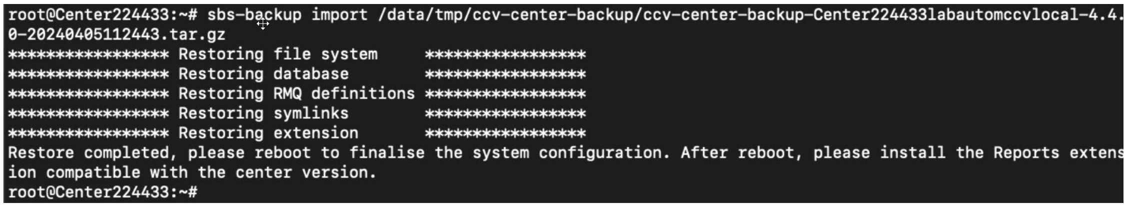
Copy the center backup file to the new center's **/data/tmp/ folder**.

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

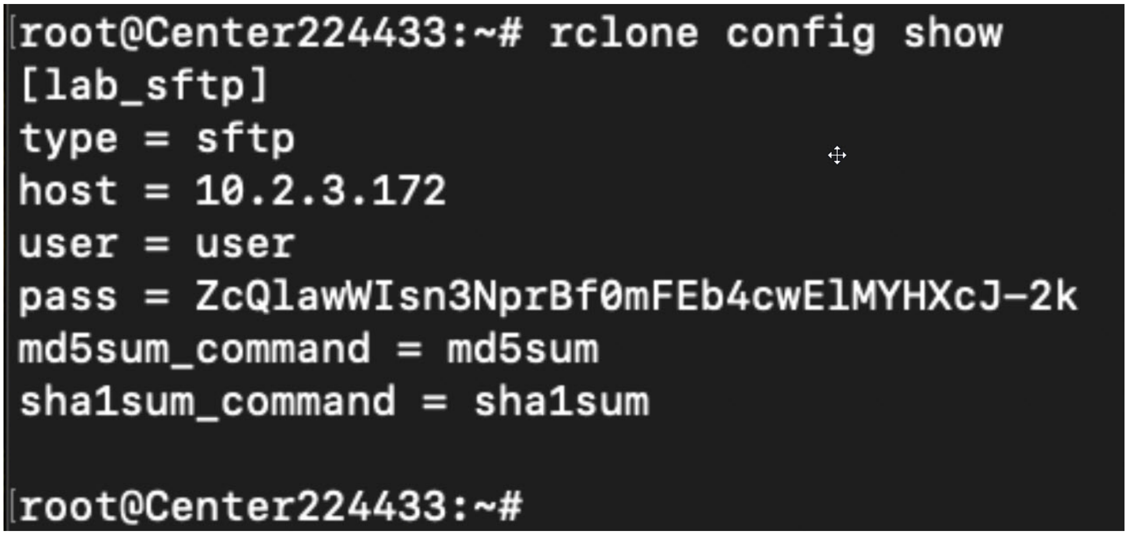
Step 1 To handle the complex authentication of object storage systems, rclone requires configuration due to the information being stored in a config file. The simplest way to create this config is by running rclone with the config option:

```
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'.`

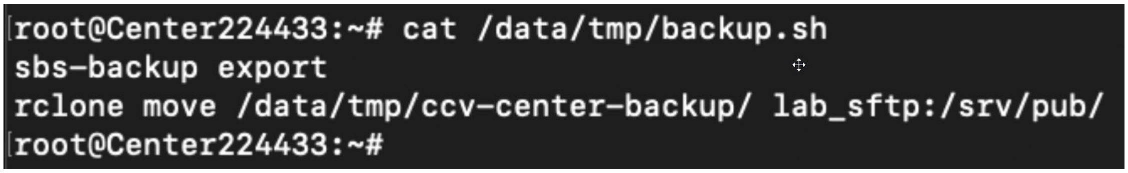
Bash Script

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:

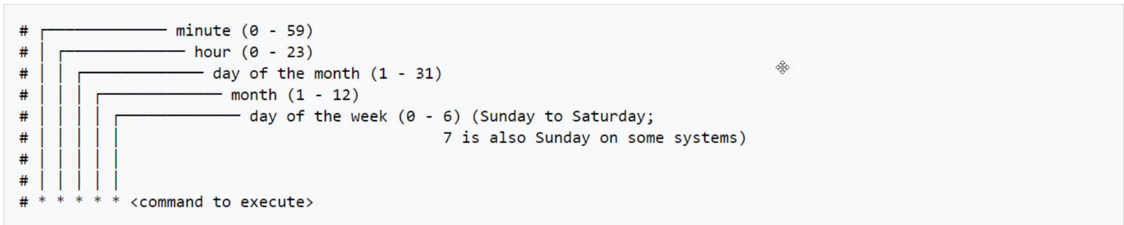
1. Edit crontab launching the command:

    - `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>
```