cisco.



Cisco Cyber Vision Center VM Installation Guide, Release 4.1.2

First Published: 2021-01-01 **Last Modified:** 2022-08-04

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

© 2019–2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	About this documentation1Document purpose1Warnings and notices1
CHAPTER 2	Information & Characteristics 3
CHAPTER 3	Requirements for installation 7
CHAPTER 4	Install the Virtual Center 9
	Retrieve the installation file 9
	ESXi 10
	Create a Virtual Machine 10
	Boot the Virtual Machine 15
	Hyper-V 17
	Create a Virtual Machine 17
	Configure the disk size 21
	Create the network interfaces 23
	Map the network interfaces 26
	Boot the Virtual Machine 28
CHAPTER 5	Configure the Center 31
	Basic Center configuration 31
	Access the basic Center configuration 32
	Accept the End User License Agreement 32
	Select the language to match your keyboard 33
	Select the Center type 34

	Center 35
	Global Center 37
	Configure the Center's Administration Network Interface 38
	Set interfaces (dual or single) 39
	Configure the Center's DNS 40
	Synchronize the Center and the sensors to NTP servers 40
	Give the Center a name 42
	Set the Center's password 42
	Configure the Center's Collection network interface 43
	Configure the sensors' password 45
	Authorize networks 45
	Complete the basic Center configuration 46
	Cisco Cyber Vision configuration 47
	Install the certificate in your browser 48
	Install Cisco Cyber Vision 55
	Configure the user interface security 58
	Upload a p12 59
	Generate a CSR 61
	Configure Center data synchronization 63
CHAPTER 6	Configure a Center DPI 69
CHAPTER 7	Global Center Configuration 73
	Center enrollment 73
	Center unenrollment 76
	Force the unenrollement of a Center 77
CHAPTER 8	Upgrade procedures 79
	Architecture with a Global Center 79
	Check the Global Center and Centers' health 79
	Update the Global Center 80
	Update the sensors 80
	Update hardware sensors 80
	Update IOx sensors 81

I

I

Architecture with a single Center 82

Update the Center 82

Update the sensors 82

Update hardware sensors 82

Update IOx sensors 83

Contents



About this documentation

- Document purpose, on page 1
- Warnings and notices, on page 1

Document purpose

This installation guide shows how to connect, configure and install Cisco Cyber Vision as a virtual machine running on VMware ESXi and on HyperV.

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

This documentation is applicable to system version 4.1.2.

Warnings and notices

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

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



Warning

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



Important In

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.



Information & Characteristics

• Information & Characteristics, on page 3

Information & 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.

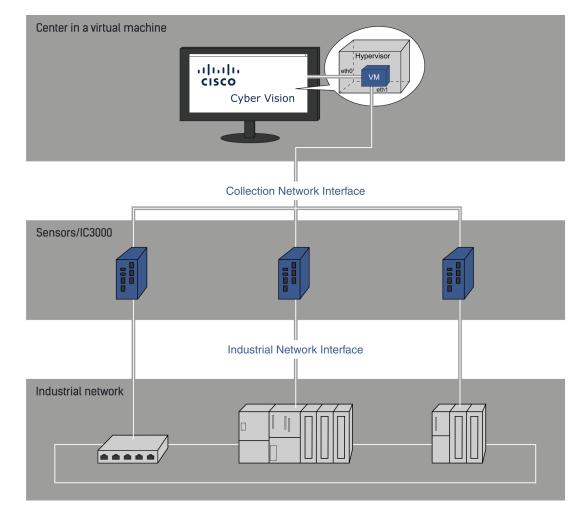
During the installation of the Center, you will have the opportunity to set up Center data synchronization to a Global Center. However, if you choose to set up a global infrastructure, you must install the Global Center first, then the Centers, and finally, the sensors.

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):

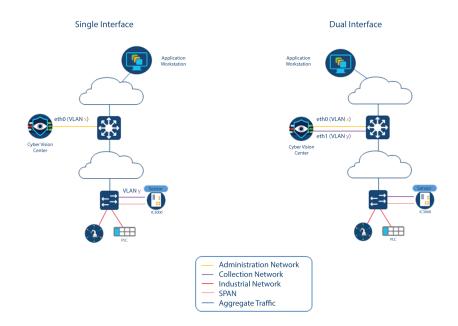


Configuring single or dual interface (not applicable to a Global Center)

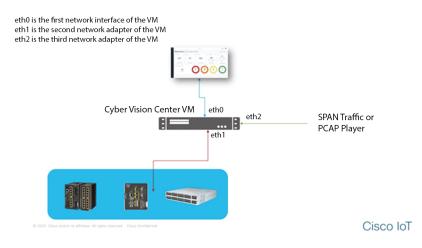
For security reasons, it is recommended to use the Center on **two separate networks**, respectively connected to the following interfaces:

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

L



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



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.



Requirements for installation

• Requirements for installation, on page 7

Requirements for installation

Make sure the conditions listed below are met before installing Cisco Cyber Vision as a virtual machine.

Required configuration for a VM:

Hypervisor:

• VMware vSphere 6.x or later.

OR

• Microsoft Hyper-V Server 2016 or later.

Make sure the hypervisor used is set with the rights necessary for a new VM instantiation.

VM sizing

Minimum – up to 500 components:

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

VM sizing

Recommended:

For 10,000 components w/o Center DPI:

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

For more than 10,000 components or Center DPI:

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

Required resources:

• One or two IP addresses, depending on a Center installed with single or dual interface. Dual interface: one interface receives protocol data from the sensors (Collection network interface), the other is used to access the web interface and for SSH remote administration (Administration network interface) (n/a to a Global Center or a Center configured with single interface).

An additional interface dedicated to DPI is required to deploy a Center with sensor function on EXSi.

- An IP address for each sensor to connect (preferably on a dedicated LAN or VLAN for connections between the sensors and the Center i.e. the Industrial network interface) (n/a to a Global Center).
- A NTP server accessible from the Center (time is generally retrieved on a router).
- A machine name which has to be unique (either configured on the DNS, or to be configured on each client). This is essential for the security exchanges setup between a client (humans or API) and the Center.



Install the Virtual Center

You need to complete several steps to install the Virtual Center:

- 1. Retrieve the Cisco Cyber Vision installation file.
- 2. Create a Virtual Machine on ESXi and deploy Cisco Cyber Vision ova file on the VM. OR

Create a Virtual Machine on Hyper-V, set the disk size, create and map the network interfaces.

The only configurations that may be required during deployment are memory and disks size customization.

- 3. Configure the Cisco Cyber Vision Center.
 - Retrieve the installation file, on page 9
 - ESXi, on page 10
 - Hyper-V, on page 17

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 ova file required for Hyper-V or ESXi from the last version released. 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 5Open 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



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

Software Download

ownloads Home / Security / Network Visib	oility a			
		Details		\times
Q Search		Description :	VMware OVA (Center) - CiscoCyberVision-Center- 3.2.3.ova	
		Release :	3.2.3	
Expand All Collapse All		Release Date :	30-Apr-2021	
		FileName :	CiscoCyberVision-center-3.2.3.ova	
Latest Release	\sim	Size :	382.92 MB (401520640 bytes)	
		MD5 Checksum :	ad553391b4f43128ef922e1a98e7e58c 📋	
3.2.3		SHA512 Checksum :	1338bfb1a17110af80d751ae7b450f2b 📋	
All Release	~	Release Notes for 3.3	2.3 Advisories 📑	
3	>	VMware OVA (C CiscoCyberVI) on Advisories	enter) - CiscoCyberVision-Center-3.2.3. center-3.2.3.ova	ova

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 EXSi.

Step 2	Click Create/Register	VM.
--------	-----------------------	-----

VMWare' ESXi"				Help - Q Search -
Navigator	esx			
Image Manage Monitor Image Image	esx Version: 6.7 State: No	VRegister VM in Shut down in Reboot in Oupdate 2 (Build 13981272) mal (not connected to any vCenter Server) 98 days	C Refresh 🏠 Actions	CPU PREE 27 GHE 2% USED: 526 MHE CAPACITY: 27.5 GHE MENORY PREE 68.03 GB 2.4% USED: 30.53 GB CAPACITY: 127.46 GB STORAGE PREE 6.5 TS 0% USED: 475.71 GB CAPACITY: 7.27 TB
	▼ Hardware		✓ Configuration	
	Manufacturer	Dell Inc.	Image profile	(Updated) ESXi-6.7.0-20190402001-stan dard (VMware, Inc.)
	Model	PowerEdge R440	vSphere HA state	Not configured
	▶ ☐ CPU	12 CPUs x Intel(R) Xeon(R) Gold 5118 C PU @ 2.30GHz	▶ vMotion	Not supported
	Memory	127.46 GB	✓ System Information	
	Persistent Memory	0 B	Date/time on host	Tuesday, January 07, 2020, 12:30:03 UT
	Virtual flash	0 B used, 0 B capacity		С
	✓ Q Networking		Install date	Tuesday, August 06, 2019, 15:59:07 UTC
	Hostname	esx	Asset tag	
	IP addresses	1. umi0: 10.2.3.16	Serial number	H4Y9JY2
		2 unit 60 440 0757516	BIOS version	2.2.11
	DNS servers	1.10.2.3.254	BIOS release date	Friday, June 14, 2019, 02:00:00 +0200
	😨 Recent tasks			

The wizard to create a new virtual machine opens.

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

vm ware [,] ESXi	• A.	1 + 1 F	Help 🗸 🔍 Search 🔹
Navigator	esx		
🔻 🛿 Host	🔁 New virtual machine		FREE: 27 GHz
Manage Monitor ▷ ① Virtual Machines ▷ 클 Storage ▷ ᡚ Networking	 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 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	2% CAPACITY: 27.5 GHz FREE: 08.03 GB 24% GAPACITY: 127.46 GB FREE: 88.75 CAPACITY: 127.46 GB FREE: 88.75 CAPACITY: 7.27 TB 0190402001-stan
	vmware Bio anti-		Cancel

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	
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy
 4 Deployment options 5 Ready to complete 	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
vm ware [®]	
	Back Next Finish Cancel

New virtual machine - CCV_Cent	
1 Select creation type 2 Select OVF and VMDK files	Select OVF and VMDK files
3 Select storage	Select the OVF and VMDK files or OVA for the VM you would like to deploy
4 Deployment options	Enter a name for the virtual machine.
5 Ready to complete	CCV_Center_dpi
	Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
vm ware [*]	× 🖬 CiscoCyberVision-center-dpi-3.2.0.ova
VIIIvare	
	Back Next Finish Cancel

Step 5 Select a disk with sufficient storage. Refer to Requirements for installation, on page 7.

L

vmware [,] ESXi	•						Help	↓ Q Search ·
°≝ Navigator	🗆 📋 esx							
🕆 🖥 Host	🔁 New virtual machine - Cisco Cyber	Vision VM						FREE: 27 GHz
Manage Monitor P 🗗 Virtual Machines P 📑 Storage P 💁 Networking	 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 file	es and all of its'	virtual disks.			CAPACITY: 27.5 GHE CAPACITY: 27.5 GHE 24% CAPACITY: 12.46 GB FREE: 69.53 CB CAPACITY: 7.27 TB
	vm ware [,]	Name ~	Capacity ~ 7.27 TB	Free ~ 6.8 TB	Type ~ VMFS6	Thin pro ~ Supported	Access ~ Single 1 items	0190402001-stan 020, 12:30:03 UT 19, 15:59:07 UTC
	Recent tasks	1, 102,3234		E DICCT	Back	lext Fi	inish Can	cel

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

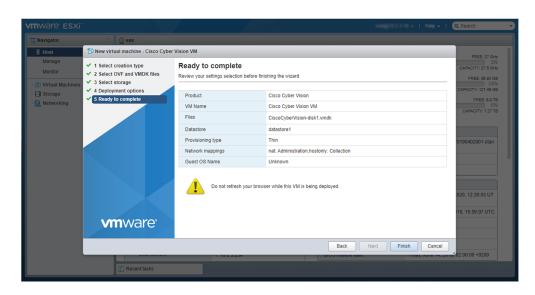
Medium: Intel Xeon, 10 cores, 32GB RAM

Large: Intel Xeon, 16 cores, 64GB RAM

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

🔁 New virtual machine - CCV_Cent	er		
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Deployment options Select deployment options		
4 Deployment options 5 Ready to complete	Network mappings	nat Administration	
	Deployment type		 ✓ ✓ And 2 vC
;	Disk provisioning	PUs and 8GB Memory for the vApp.	
	Power on automatically		
vm ware [®]		Back Next Finish	Cance
		Back Next Finish	Canc
	er	Back Next Finish	Canc
 New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 	er Deployment options Select deployment options	Back Next Finish	Canc
 New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Deployment options	Back Next Finish	Canc
New virtual machine - CCV_Cent Select creation type Select OVF and VMDK files Select Storage 4 Deployment options	Deployment options Select deployment options	1 nat Administration ~ hostonly Collection ~	Canc
P New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 Deployment options	Deployment options Select deployment options	1 nat Administration v hostonly Collection v dpi DPi v	Canc
P New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 Deployment options	Deployment options Select deployment options Network mappings Disk provisioning	1 nat Administration ~ hostonly Collection dpi DPI ~ O Thin ® Thick	Cance
New virtual machine - CCV_Cent Select creation type Select OVF and VMDK files Select Storage 4 Deployment options	Deployment options Select deployment options	1 nat Administration v hostonly Collection v dpi DPi v	Cance
New virtual machine - CCV_Cent Select creation type Select OVF and VMDK files Select Storage 4 Deployment options	Deployment options Select deployment options Network mappings Disk provisioning	1 nat Administration ~ hostonly Collection dpi DPI ~ O Thin ® Thick	Cance
 New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 Deployment options 	Deployment options Select deployment options Network mappings Disk provisioning	1 nat Administration ~ hostonly Collection dpi DPI ~ O Thin ® Thick	Cance
 New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 Deployment options 	Deployment options Select deployment options Network mappings Disk provisioning	1 nat Administration ~ hostonly Collection dpi DPI ~ O Thin ® Thick	Cance
 New virtual machine - CCV_Cent 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 Deployment options 	Deployment options Select deployment options Network mappings Disk provisioning	1 nat Administration ~ hostonly Collection dpi DPI ~ O Thin ® Thick	Canc

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



Your new VM is displayed in the virtual machine list.

🕶 📋 Host							
Manage	😭 Create / Register VM 🛛 📑 Console	🕨 Power on 🔛 F	Power off 🔢 Su	ispend 🧲 Refresh 🧔	Actions	Q Search	
Monitor	. Virtual machine	✓ Status ✓	Used space	~ Guest OS ~	Host name	✓ Host CPU ✓	Host mem
🖆 Virtual Machines 🛛 🛛 🚺	0	•	4.3-08	Other (54-54)	Uningum	0.58%	0.10
Storage	E. Data and a second	•	4.09-08	Other (54-55)	Uningun	0.0010	0.10
🛛 🔮 Networking 👘 👘 📲	C. 🕒 vitil Server	O 74.	12.40.08	Other (54-66)	Uningun	12 984	4.03.08
	E. 🐞 vite Carter		14.45.08	Other (54-66)	University	23.98%	8.05.08
	🗐 🍙 Smart site	• **·	87.81.08	Detran DNULmur 1.	Uningun	0.58%	110
	0. 🐞 000, x0, x0		19-01-08	Other (54-55)	Unineum	211 10010	8.05.08
	🗐 👩 Fal-carlar	• **·	5.41.08	Other (54-66)	Unineum	0.58%	110
	0. 🙆 000,00,000		8 15 08	Other (54-56)	Uningun	17 1894	4.03-08
	C. BRR Cause Fag Dealter	• **·	5.84.08	Ubattle Litera (54-95)	Uningun	0.58%	110
	0. Buantan		12.71.08	Other (54-55)	Uningun	21.0840	2.21.08
	🗐 🐞 Analian	O 74.	10.00.00	Detran DNULmur 1.	Uningun	5.58%	1.89-08
	E	• ***.	200.148	Other (54-60)	Uningun	0.58%	0.108
	🗐 🚰 Cisco Cyber Vision VM	📀 No	200 MB	Other (64-bit)	Unknown	0 MHz	0 MB
	. B Cisco Cyber Vision VM	0.11	200.448	(the (64-66)	Uninput	0.58%	

Boot the Virtual Machine

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

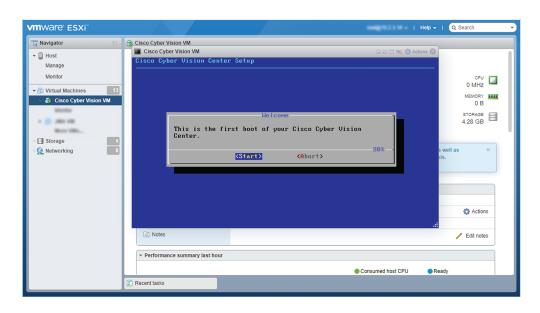
1. Click the VM in the list.

Monitor	Create / Register VM Por Console Por	wer on 🔳	Power off 🔢 Susper	nd 🛛 🤁 Refresh 🔹 🎂	Actions	Q Search	
	Virtual machine					Q Search	
5 Michael Machines		Status ~	Used space 🗸 🗸	Guest OS ~	Host name ~	Host CPU V	Host mem
	0	•	4.3.08	Other (64-66)	Unimpun	0.58%	0.10
	🗉 👩 per jarrier	•	4.00-08	(Ther (54-55)	Unineum	0.0010	1.10
9 Networking	🗆 . 🐞 vitil Server		10.40.08	(Ther (54-55)	Uninput	12 181	4.03-08
	🗆 🐞 vitil Carter	•	14.45.08	(thur (54-66)	Unineum	23.98%	8.05.08
	🗆. 👩 teast stat		87.81.08	Detran DNULmus 1	Unknown	0.58%	110
	🗆 🍈 608. ya jen	•	19.01.08	(Ther (54-55)	Unineum	211 684	8.05.08
	🗖 👩 Fritantin		5.41.08	(thur (54-54)	Unineum	0.001	110
	🗆 🐞 604. yr. (40	•	8.15.08	(ther (54-55)	Unineum	17.984	4.03-08
	🗆., 🍙 MFR Cause Pag Deactor		5.04.08	Ubuffs Liture (54-bit)	Unknown	0.58%	110
	🗆 🐞 11.4., 19., 191	•	12.71.68	(Ther (54-55)	Unineum	21.989	2.21.08
	🗆 🌗 *****		10.00.00	Detran DNULmus 1	Unknown	5.68%	1.85-08
	E		200.448	Other (54-56)	Unknown	0.58%	0.108
	🗐 🚰 Cisco Cyber Vision VM	🕑 No	200 MB	Other (64-bit)	Unknown	0 MHz	0 MB
	Quick filters v						13 items

2. Power on the VM.

vm	ware" esxi"		i Help 🗸 i 🔍 Search 🗸
	🔁 Cisco Cyber Vision VM		
	📝 Console 🛛 Monitor 📔 🕨 Power of	🛛 🔲 Power off 🔢 Suspend 🧐 Restart 🥜 Edit 🤁 Refresh 🧔	Actions
😰 🛐 💷 🦹 "E" Navigator		Cisco Cyber Vision VM Guest 0 S Other (64-bit) Compatibility ESX 60 virtual machine VMvare Tools No CPU 2 Memory 4 GB	O MHz
	the guest 03, e.g. gracerar shutta		
	✓ General Information		
	Metworking	Io network information	
	VMware Tools	/Mware Tools is not installed.	🏠 Actions
	▶ 🗐 Storage	disk	
	Notes		🥒 Edit notes
	✓ Hardware Configuration		
	Precent tasks		

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



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.

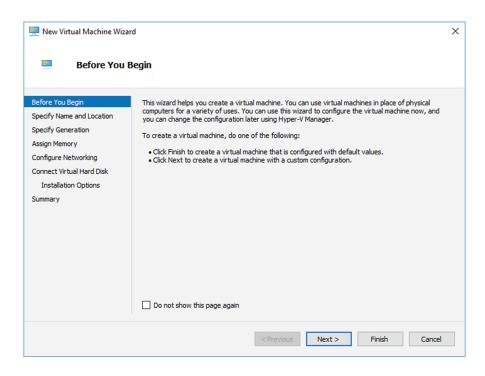
 The following home screen appears:

Hyper-V Manager							- 🗆 X
File Action View Help							
🗢 🏟 🖄 📰 🔝 🖬							
Hyper-V Manager WIN-ENHJR2D8JNR	Virtual Machines						Actions
	Name	State	CPU Usage	Assigned Memory	Uptime	Status	WIN-ENHJR2D8JNR
	CCV_V300_01	Off					New
							🕼 Import Virtual Machine
							Hyper-V Settings
							Virtual Switch Manager
							🛃 Virtual SAN Manager
							🚅 Edit Disk
							Inspect Disk
	<						> Stop Service
	Checkpoints						Remove Server
							🖏 Refresh
			The selected virtua				
							View +
							I Help
							CCV_V300_01
							- Connect
							Settings
							3 Start
	CCV_V300_01						🔂 Checkpoint
	CC+_+550_01						A Move

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

Hy	per-V Manager				
File	Action View Help				
(=	New	>	Virtual Macl	hine	
H	Import Virtual Machine		Hard Disk		
	Hyper-V Settings		Floppy Disk		
	Virtual Switch Manager			State	CPU
	Virtual SAN Manager		_V300_01	Off	
	Edit Disk Inspect Disk				

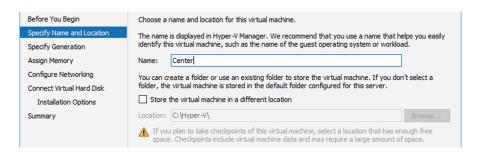
The New Virtual Machine Wizard is displayed.



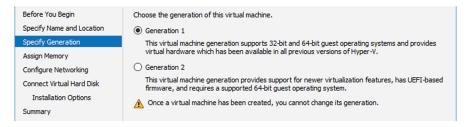
Step 3 Click Next to start.

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).



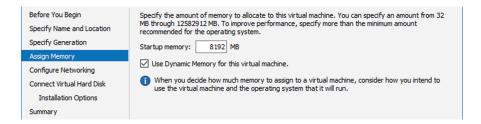
Step 6 Set the VM as Generation 1.



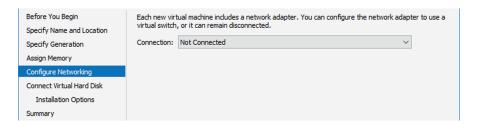


Cisco Cyber Vision Center VM Installation Guide, Release 4.1.2

Note The minimum configuration required is 8192 MB.



Step 8 Leave the network connection disconnected.



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

Before You Begin Specify Name and Location Specify Generation Assign Memory	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.
Configure Networking	Name: Center.vhdx
Connect Virtual Hard Disk	Location: C:\Hyper-V\Virtual hard Disks\ Browse
Summary	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.

Before You Begin Specify Name and Location Specify Generation	You have succo following virtua Description:	essfully completed the New Virtual Machine Wizard. You are about to create the I machine.	
Assign Memory Configure Networking Connect Virtual Hard Disk	Name: Generation: Memory: Network:	Center Generation 1 8192 MB Not Connected	
Summary	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:

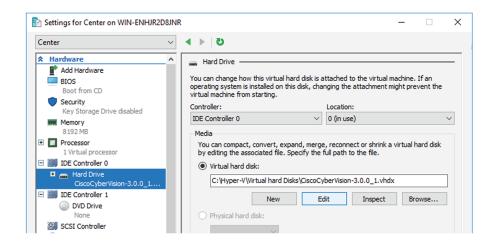
Procedure

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

Step 2 Click Action > Settings.

E H	yper-V Ma	anager		
File	Action	View	Help	
🦛 🖷	Cor	nnect		
H	Sett	tings		tual Machines
	Star	rt		me
	Che	eckpoint		CCV_V300_01
	Mo	ve		Center
	Exp	ort		

Step 3 Click Hard Drive, then Edit.



The Edit Virtual Hard Disk Wizard displays.

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

对 Edit Virtual Hard	Disk Wizard	×	
Loca	te Virtual Hard Disk		
Before You Begin Locate Disk Choose Action Summary	Location: C:\Hype		×
	Before You Begin Locate Disk Choose Action Configure Disk Summary	 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 remains the same. Convert This option converts a virtual hard disk by copying the contents to a new virtual virtual hard disk can use a different type and format than the original virtual hard wirtual hard disk can use a different type and format than the original virtual hard wirtual hard disk. Expand This option expands the capacity of the virtual hard disk. 	al hard disk. The new
		< Previous Next > Finish	Cancel

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

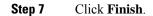
Step 6 Configure a new size for the virtual hard disk.

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.

🚄 Edit Virtual Hard	Disk Wizard	×	
Kata Expa	nd Virtual Hard Disk		
Before You Begin Locate Disk Choose Action Configure Disk Summary	Current size is betw New size: 250	GB (Maximum: 64 TB)	×
	Before You Begin Locate Disk Choose Action Configure Disk Summary	You have successfully completed the Edit Virtual Hard Disk Wizard. You are about to 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 dose the wizard, click Finish. < Previous	Cancel



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.

r								
Hyper-V Manager								
File Action View Help								
🗢 🄿 🞽 🖬 🚺								
Hyper-V Manager	Virtual Machines							Actions
WIN-ENHJR2D8JNR		State	CDUUIssas	Assisted Memory	Unting	Status		WIN-ENHJR2D8JNR
	Name	Off	CPU Usage	Assigned Memory	Uptime	Status		New
	Center	Off						🚯 Import Virtual Machine
								Hyper-V Settings
								Virtual Switch Manager
								🔒 Virtual SAN Manager
								🚄 Edit Disk
								🚔 Inspect Disk
	<						>	Stop Service
	Checkpoints						۲	🗙 Remove Server
			The selected virtua	I machine has no checkp	oints.			🖏 Refresh
								View
								🕐 Help
								Center
								📲 Connect
								Settings
								💿 Start
								🔂 Checkpoint
	Center						1	Move

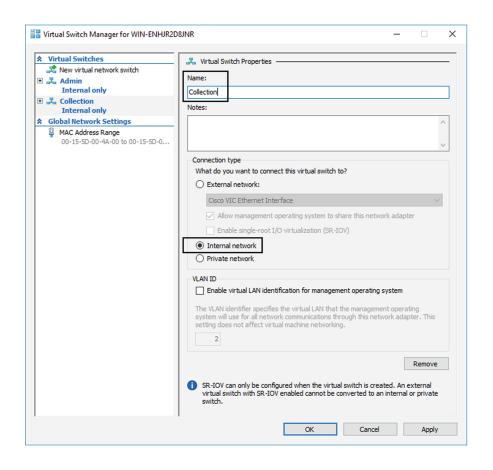
The Virtual switch manager opens.

🕌 Virtual Switch Manager for WIN-ENHJR2D	ISJNR — 🗆 🗙
 Virtual Switches New virtual network switch Global Network Settings MAC Address Range 00-15-5D-00-4A-00 to 00-15-5D-0 	Create virtual switch What type of virtual switch do you want to create? External Internal Private Create 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-ENHJR2D8	
 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 [™] 	Ivitual 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
	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.

- **Step 7** Create a second virtual switch and name it 'Collection'.
- **Step 8** Select 'Internal network'.



Map the network interfaces

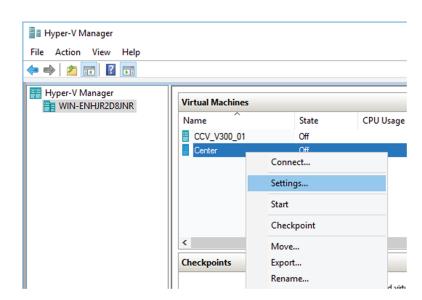
To add a network card:

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'.

L



The settings window for the Virtual Center is displayed.

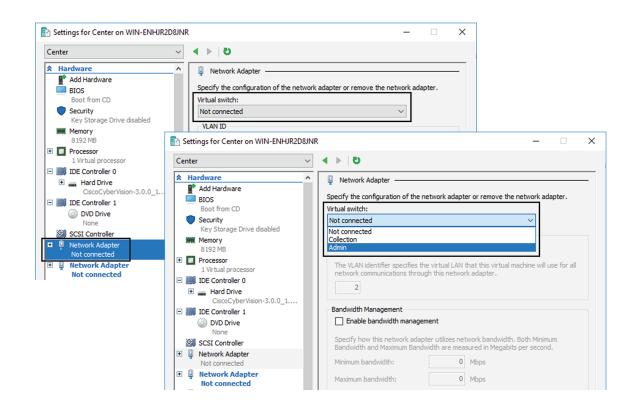
- Step 2 Click 'Add Hardware'.
- Step 3 Select 'Network Adapter'.
- Step 4 Click 'Add'.

enter	\sim	3 4 ►		
Hardware Add Hardware	^	Add Hardware		
BIOS		You can use this setting to add devices to your virtual machine.		
Boot from CD		Select the devices you want to add and click the Add button.		
Security Key Storage Drive dis	abled	SCSI Controller		
, 2	abied	Network Adapter		
8192 MB		RemoteFX 3D Video Adapter		
		Legacy Network Adapter		
Processor 1 Virtual processor		Fibre Channel Adapter		
IDE Controller 0				Add
🗉 👝 Hard Drive				
CiscoCyberVision-	3.0.0_1	Virtual machines are created with one network adapter. You can add	addition	nal networ
IDE Controller 1		adapters as needed.		

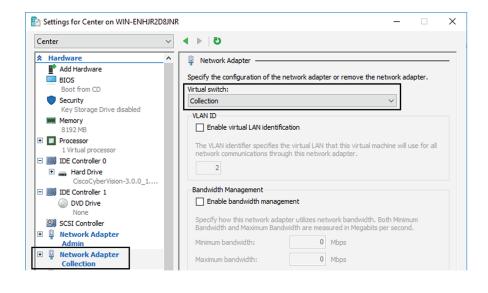
The second network adapter needed is created. Now you need to map each network adapter to a Virtual Switch.

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).



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



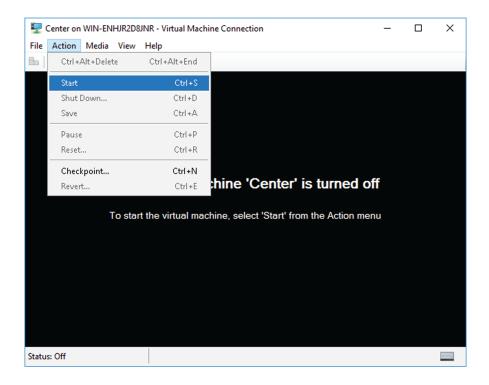
Boot the Virtual Machine

You can now proceed to the Virtual Center first boot.

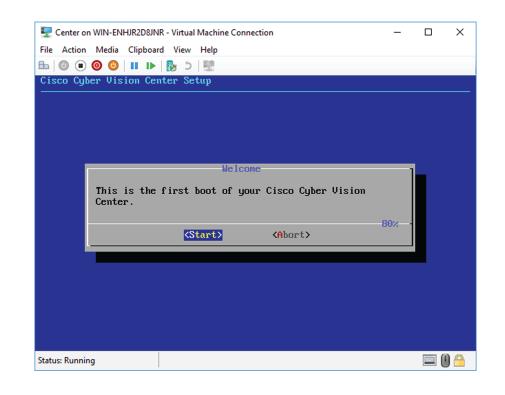
1. Click Center on Hyper-V Manager and click 'Connect'.

Hyper-V Manager			
File Action View Help			
🗢 🔿 🔁 📰 🖬			
📅 Hyper-V Manager			
WIN-ENHJR2D8JNR	Virtual Machines		
	Name CCV_V300_01 Center	State	CPU Usage
		Off	
		<u>^"</u>	
		Connect	
		Settings	
		Start	
		Checkpoint	

2. Start the Virtual Center.



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





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.



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, on page 31
 - Cisco Cyber Vision configuration, on page 47

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).

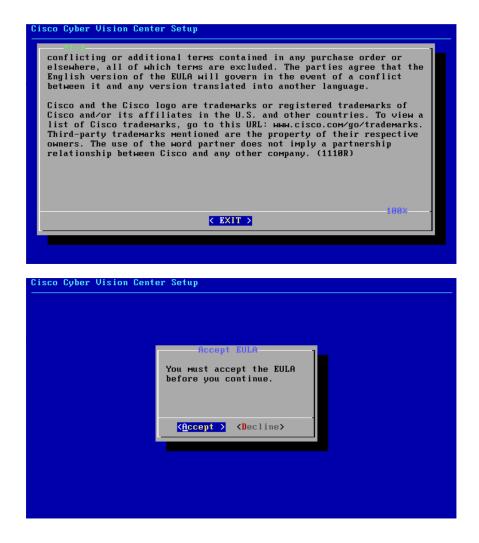
Access the basic Center configuration

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

isco Cyl	per Vision Center Setup
	Internet
	Helcome This is the first boot of your Cisco Cyber Vision Center.

Accept the End User License Agreement

End User License f	greement
ffective: May 22,	2017
Affiliates ("Cisco and "Your" means f under this EULA. ' Lisco computer pro- pproved Source ar Jisco user or tech ther documentatic You by an Approved. he Cisco authoriz	nt between You and Cisco Systems, Inc. or its ") and governs your Use of Cisco Software. "You" he individual or legal entity licensing the Software Use" or "Using" means to download, install, r otherwise use the Software. "Software" means the grams and any Upgrades made available to You by an d licensed to You by Cisco. "Documentation" is the nical manuals, training materials, specifications or n applicable to the Software and made available to . Source. "Approved Source" means (i) Cisco or (ii) red reseller, distributor or systems integrator from the Software. "Entitlement" means the license
	< EXIT >



Select the language to match your keyboard

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

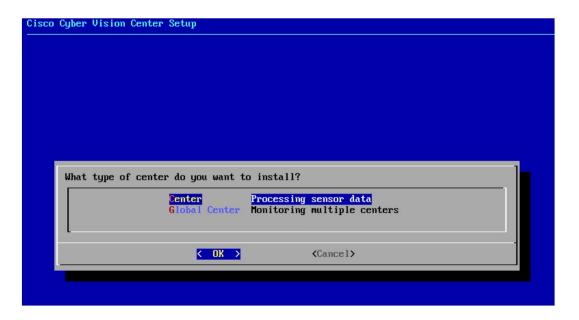
isco Cyber V	ision Center Setup
	Choose your keyboard Mapping. IS American fr French de German it Italian es Spanish
	< OX <cancel></cancel>

Select the Center type

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

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

Select the type of Center you want to install.



Center

If installing a Center, select the first option.

CISCO	Cyber	Vision Center Setup	
	What	type of center do you want to install?	
	What	: type of center do you want to install? Center Global Center Monitoring multiple centers	
	What	Center Processing sensor data	
	What	Center Processing sensor data	
	What	Center Global Center Monitoring multiple centers	

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

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



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



Use the following command from the Global Center's CLI to get a list of all Center's id: sbs-db exec "select name, id from center"

Type the id into the basic Center configuration UUID field.

Cisco Cyber Vision Center Setup
This UUID is used to uniquely identify the center You can override the following with an identifier that respects the UUID format.
<u>5</u> 64d1886-db38-bf9d-4235-f3c412f196d1
< OK > <cancel></cancel>

Click OK. You will be direct 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	
Center Processing sensor data	
Center Colobal Center Honitoring multiple centers	

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



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.

interface				
L*	IHCP Automat	ion type for th <mark>ic (DHCPv4)</mark> IP and gateнay	e ACCESS	
	<u>< 0x ></u>	<cancel></cancel>		

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

• Manually:

o Cyber Vision	
	se select configuration type for the ACCESS rface DHCP Automatic (DHCPv4) Manual Static IP and gateмay
	<mark>< <u>0</u>K → <cancel></cancel></mark>
o Cyber Vision	Center Setup
	Setup Access Network Interface IP Address 10.2.3.102 Netmask 24 Gateway 10.2.3.254
	< OK > <cancel></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. Select No.

Concerning a Center, it is possible to:

- Set the Administration and Collection Network Interfaces on two distinct interfaces (recommended for security). In this case, select Yes.
- Use a single interface. In this case, select No.



If you choose to set a dual interfaces, you will be directed to the following screens in the Configure the Center's Collection network interface, on page 43 subsection.

Configure the Center's DNS

Type a DNS server address and optional fallbacks.

Cisco Cyber Visio	n Center Setup
	Setup DNS configuration Up to three maximum, leave blank unnecessary fields
	Preferred 208.67.222.222 Alt 1 208.67.220.220 Alt 2

Synchronize the Center and the sensors to NTP servers

Enter IP addresses of local or remote NTP servers (gateway configuration needed) to synchronize the Center and the sensors with a clock reference. Each address must be separated by a space.

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
<pre> Cancel> </pre>

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

Cisco Cyb	per Vision Center Setup
	Please enter some NTP time servers: They will be used to synchronize the Center's clock, which is required to generate correct certificates. The servers must be separated by whitespace. A server is composed by its address and optionally by a key ID and an AES 128 CMAC key value (32 hex character) separated by semicolon. Format: server_address[;key_id;key_value] Leave this field empty to use local time only. [18.0.6.10;1;9f8f32554ad5a369370f08d536fa8fc9
	Cancel>

The synchronization takes a few seconds.

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



Note The time is set in the UTC standard.

Time is now: Tue Oct :	29 16:37:43 2019 UTC
If this is incorrect, below (MMDDhhmm[[CC]Y	please specify current UTC time Y][.ss])
Leave empty or cancel	to skip.
_	
< 0K	> <cancel></cancel>

Give the Center a name

<u> </u>	
te This na	me 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) <u>C</u> enter
	Cancel>

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

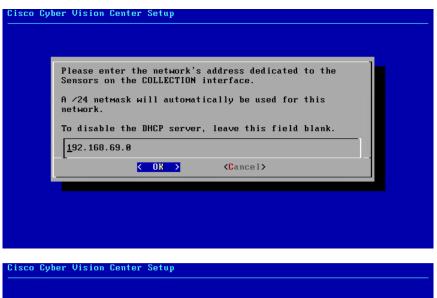


Confirm the password.

Cisco Cyber Vision Cente	r Setup
	Please confirm the cu-admin password
	-
	·
	Cancel>

Configure the Center's Collection network interface

Erase the network address suggested into the field to disable the DHCP server and enter OK to proceed to the next step.



A $/24$ netmask will automatically be used for this	
network.	
To disable the DHCP server, leave this field blan	k
< OK > <cancel></cancel>	

Type the IP address of the Industrial network interface:

Cisco Cyber Vision Center Setup	
Please specify the IP address t acquisition interface, includin 192.168.1.1/24):	
192.168.69.1/24	
<u>< 0k ></u> <	Cancel>

L

Configure the sensors' password

As this step does not apply when installing a Global Center, the following screens won't be displayed. Instead, you'll be directed to Authorize networks.

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

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



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

Confirm the password.

ision Center Setup
Please confirm the sensor's root password
Cancel>

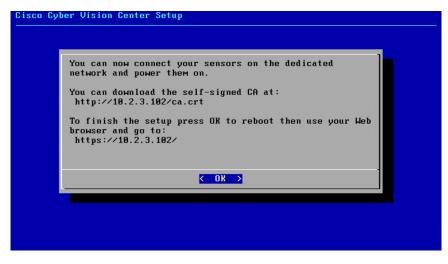
Authorize networks

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

on the ad	ovide networks au Ministration inte prized. Local net	erface. By defau	lt all networks
	networks must be		
<u>0</u> .0.0.0/	0		
	< 0K >	<cancel></cancel>	

Complete the basic Center configuration

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



Enter OK to finish the basic Center configuration.

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. BS 4.1.0 center tty1 enter login: _



Note A major change regarding the Center command line (CLI) access through serial console or SSH was made in Cisco Cyber Vision version 4.1.0. The user root is no more usable to establish the connection. A new user called 'cv-admin' must be used. This user has limited rights and many CLI commands will require permission elevation:

- prefix the command with "sudo".
- or open a root shell using "sudo -i" and enter the command.

Close the Center configuration window before proceeding with the next steps of Cisco Cyber Vision configuration.

To proceed with the Cisco Cyber Vision configuration, open your browser and go to the URL previously indicated to access the user interface.



Note

Each Cisco Cyber Vision Center includes its own PKI (Public Key Infrastructure), with a CA (Certification Authority), that will be used to establish the TLS connection with the sensors and to clients. The CA must be installed on each client browser (see the following chapters).

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 and then access the Install Cisco Cyber Vision 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 Install Cisco Cyber Vision to configure users and sensors.
- 2. Configure the user interface security 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 55.

Procedure

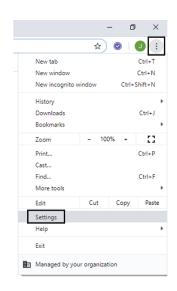
Step 1	Open your	browser.
--------	-----------	----------

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.

Q certificate	8
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 <mark>certificate</mark> s Manage HTTPS/SSL <mark>certificate</mark> s and settings	Z
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.

ersonal	Other People	Intermediate Certification	Authorities Tru	sted Root Certificat	ion 🖣
Issued	То	Issued By	Expiratio	Friendly Name	^
100000		10000003	Expiration	Thendry Hame	
2.5	and the first	Reference Color/Trust	100000000	Design 1 Automa	
100	Les CA	Carbon CA	10000	Carlue	
(and	La Tratadita	Cartue Trusted Nation	Physics and Physic	Carlue Trusted	
Que.	- Real CA 204	Case Reat CA 2048	1400.000	-filmer -	
Que.	a Rost (A.M)	Caro Rost CA/H)	10111-0010	-manaco	
Q.	a Rost (A.H.)	Caro Rost (A.H)	10110-0010	-Clarge -	
- Carlor	a Rost (A.H.)	Caso Rost (A.H)	12112	-Termin	
- CBU	e RIC AL	Caso RIC #2	19,00,000	-Care -	~
erver Au	e intended purp	oses lient Authentication, Secure		ing, Time	/anced
tamping, ser	, Encrypting File	System, IP security tunnel	termination, IP s	Vie	w

A certificate importation wizard opens.

Step 7 Go to the next step.



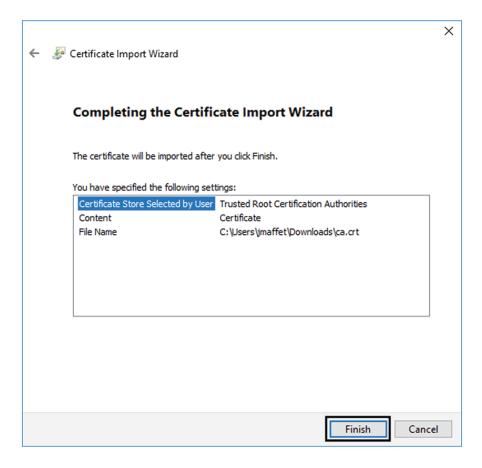
- **Step 8** Search for the certificate you downloaded earlier.
- **Step 9** Go to the next step.

←	🚰 Certificate Import Wizard	×
	File to Import Specify the file you want to import.	
	File name: C:\Users\jmaffet\Downloads\ca.crt Browse	
	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)	
	Next Cancel	

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

ertificate St Certifica	ore te stores are system	areas where certifi	cates are kept.	
Window: the certi	can automatically se ficate.	ect a certificate st	ore, or you can spec	ify a location fo
	itomatically select the	e certificate store b	ased on the type of	certificate
Pl	ace all certificates in t	the following store		
C	ertificate store:			
[Trusted Root Certifica	ation Authorities		Browse

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



What to do next

Install Cisco Cyber Vision, on page 55

Install Cisco Cyber Vision

Access the Cisco Cyber Vision installation wizard:

Procedure

Step 1	With your browser, access https:// <centername>/.</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 Step 3		up wizard used for the first access to Cisco Cyber Vision is displayed: an admin account:		

Welcome to Cyber Vision Please follow this few steps to be fully ready to use the product				
2 Create the first user	$\begin{bmatrix} \blacksquare \\ P \end{bmatrix}$ Agree to the license terms \bigcirc Done			
Firstname :	Lastname*:			
Email :				
Password :	Confirm password *:			
Suggested password: \$kvIH2Qq*odz90fj0E3				
	•	Creat		

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:

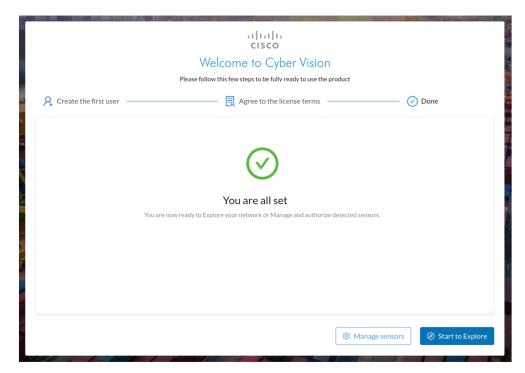
	uluulu cisco	
	Welcome to Cyber Vision	
	Please follow this few steps to be fully ready to use the product	
A Create the first user	Agree to the license terms	⊘ Done
End User License Agreement		
Effective: May 22, 2017		
	s the individual or legal entity licensing the Softwa	
computer programs and any Upgrad "Documentation" is the Cisco use applicable to the Software and m (ii) the Cisco authorized resell "Entitlement" means the license (PID) published on Cisco's price	all, activate, access or otherwise use the Software. des made available to You by an Approved Source and J er or technical manuals, training materials, specific made available to You by an Approved Source. "Approve ler, distributor or systems integrator from whom you detail; including license metric, duration, and quar e list, claim certificate or right to use notification rror corrections, enhancements and other modification	"Software" means the Cisco licensed to You by Cisco. cations or other documentation ed Source" means (i) Cisco or acquired the Software. ntity provided in a product ID on. "Upgrades" means all
computer programs and any Upgrac "Documentation" is the Cisco use applicable to the Software and m (ii) the Cisco authorized resell "Entitlement" means the license (PID) published on Cisco's price updates, upgrades, bug fixes, er copies thereof.	all, activate, access or otherwise use the Software. Jes made available to You by an Approved Source and Jer er or technical manuals, training materials, specific made available to You by an Approved Source. "Approved ler, distributor or systems integrator from whom you detail; including license metric, duration, and quare list, claim certificate or right to use notificatic	"Software" means the Cisco licensed to You by Cisco. cations or other documentation ed Source" means (i) Cisco or acquired the Software. ntity provided in a product ID on. "Upgrades" means all
computer programs and any Upgrad "Documentation" is the Cisco use applicable to the Software and m (ii) the Cisco authorized resell "Entitlement" means the license (PID) published on Cisco's price updates, upgrades, bug fixes, er copies thereof. Table of Contents	all, activate, access or otherwise use the Software. Jes made available to You by an Approved Source and Jer er or technical manuals, training materials, specific made available to You by an Approved Source. "Approved ler, distributor or systems integrator from whom you detail; including license metric, duration, and quare list, claim certificate or right to use notificatic	"Software" means the Cisco licensed to You by Cisco. cations or other documentation ed Source" means (i) Cisco or acquired the Software. ntity provided in a product ID on. "Upgrades" means all

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.



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 58.

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 63.

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.

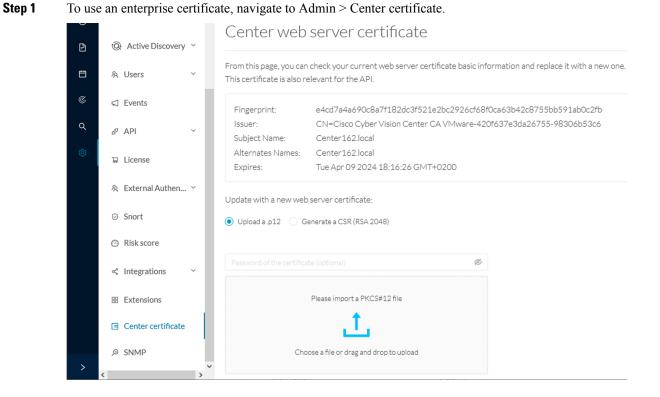
Configure the user interface security

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



Cisco Cyber Vision Center VM Installation Guide, Release 4.1.2

Step 2 You can Upload a p12 orGenerate 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:



	Ø
Please import a PKCS#12 file	
Please Import a PRC5#12 file	
<u>1</u>	
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.

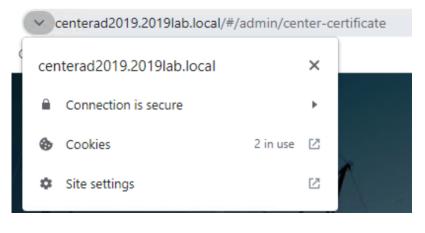
- **Step 2** Type the certificate password.
- **Step 3** Click the Import a PKCS#12 file button or drag and drop the file to import it.

Step 4

Step 5 Step 6

		Ø
_	2019.2019lab.local1.pfx	
lick Save. he following message appears		

The error message does not appear and the 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 63.

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 O Generate a CSR (RSA 2048)	
		Generate and download CSR
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	
		Generate and download CSR
	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		
i CSR has been generated. Please import the certificate.]	
FQDN: CenterAD2019.2019lab.local CSR: download		
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.

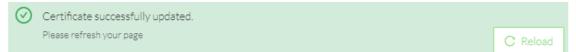
Step 5 Use the <FQDN>.csr file to generate a pem certificate from your enterprise Certification Authority.

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.

	ith a new web server certificate: da.p12 (Generate a CSR (RSA 2048)	
(i)	CSR has been generated. Please import the certificate.	
FQDN: CSR:	CenterAD2019.2019lab.local download	
	File selected: CenterAD2019.2019lab.local.crt	
		🗋 Discard 🚺 Sav



The following message appears:



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.

	~ 0	enterad2019.2019lab.local/#/a	dmin/cer	nter-ce	ertificate
<	cen	terad2019.2019lab.local		×	
l		Connection is secure		Þ	
l	٩	Cookies	2 in use	Z	
	\$	Site settings		Ľ	r

What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 63.

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.

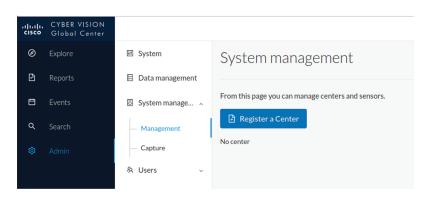
Once the Global Center and its synchronized Centers are installed, proceed to data synchronization, which consists of registering the Center in the Global Center and enrolling the Center to the Global Center. To do so, you need to open each's Cisco Cyber Vision's GUI.



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

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

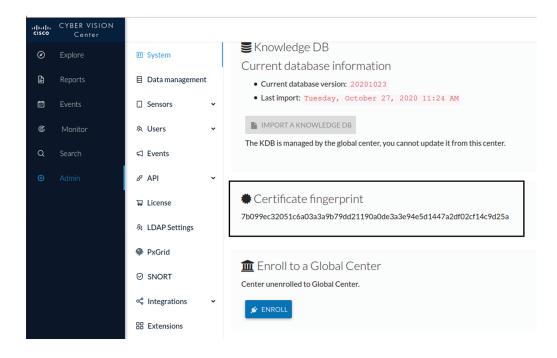
Click the Register a Center button.



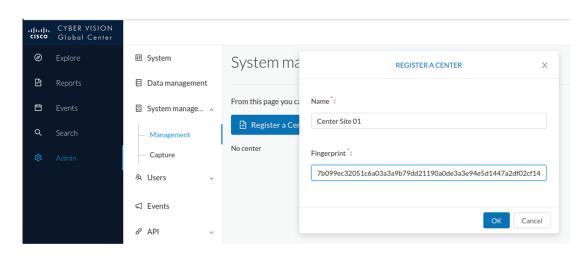
The window "Register a Center" pops up, ready to be filled. Now you must access the Center's GUI to retrieve its fingerprint.

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

Scroll down to Certificate fingerprint and copy it.



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



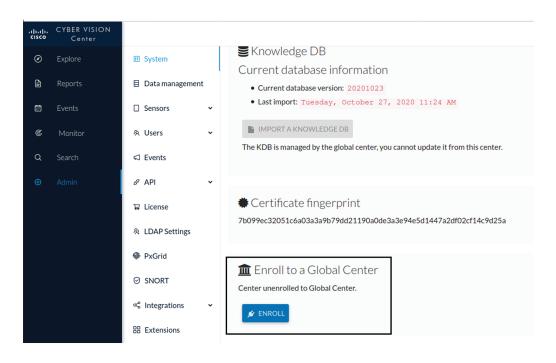


The Center appears in the list as unenrolled.

	CYBER VISION Global Center						
Ø	Explore	া System	System management From this page you can manage centers and sensors.				
Ē	Reports	🗐 Data management					
Ð	Events	System manage ^					
م	Search	— Management					
ø	Admin	— Capture	Name	IP	Version	Status	Processing Status
		冬 Users v	Center Site 01			unenrolled	

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

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



The Enrollment window pops up.

Copy the Global Center's fingerprint from its GUI's System administration page (same location as the Center's). 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	
🖋 Enroll 🛛 Can	cel

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



In the Global Center's GUI, the Center status changes to Connected.

.ı ı.ı ı. cısco	CYBER VISION Global Center									
Ø	Explore	태 System	System ma	anagement						
£	Reports	🗐 Data management								
Ħ	Events	🗟 System manage 🔨	From this page you can manage centers and sensors.							
۹	Search	— Management	Register a Cer	nter						
ø	Admin	— Capture	Name	IP	Version	Status	Processi			
		冬 Users 🗸 🗸	Center Site 01	192.168.72.16	SBS: 3.2.0+202010230959 KDB: 20201023	Connected				
		⊲ Events								

The Global Center and the Center are successfully connected.

Repeat the previous steps as many times as necessary to connect other Centers.

The next step will be to install and enroll the sensors. To do so, refer to the corresponding Cisco Cyber Vision Sensors Installation Guides.

Once a sensor will be connected it will appear in the Global Center's GUI as below:

Name	IP	Version	Status	Processing Status	Capture Mode	UpTime
- Center Site 01	192.168.72.16	SBS: 3.2.0+202010230959 KDB: 20201023	Connected			1 hr 19 mins 42 secs
Sensor IE3400-LAB1	192.168.69.210	3.2.0+202010231006	Connected	Pending data		7 mins 29 secs



Configure a Center DPI

• Configure a Center DPI, on page 69

Configure a Center DPI

This section describes how to configure a Center DPI, that is, a virtual sensor in the Center.

Requirements:

Make sure an ethernet interface is available for the Center DPI traffic, depending on:

- If the server has a dual interface, that is, the Administration interface is on eth0 and the Collection interface is on eth1, then eth2 will be used for the Center DPI.
- If the server has a single interface, that is, the Administration and Collection interfaces are on the same interface, then eth1 will be used for the Center DPI.

In the example below, the server has a single interface.

To configure a Center DPI:

Procedure

Step 1 Access the Cisco Cyber Vision sensors administration page.

-ilialia cisco		<u>⊮</u> ⊗ ∽
Ø	III System	Sensors
	🗄 Data Manage 🗸	From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.
Ē	& Network Organization	
¢	Sensors ^	No sensors found.
Q	- Sensors	Please check the following:
©	 Capture 	Sensor(s) are powered on Sensor(s) are connected to the same network as the Center 'COLLECTION' interface.
	糸 Users 🗸	AMANAGE CREDENTIALS
	⊲ Events	

Step 2 Open the Center shell prompt and type the following command:

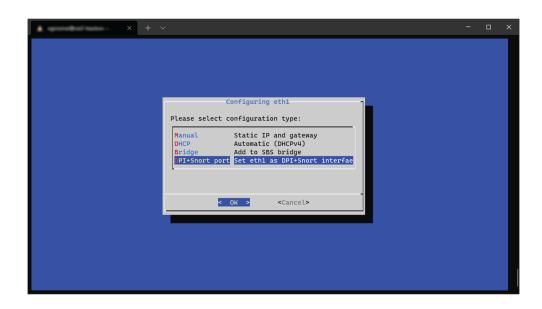
sbs-netconf



Step 3In the case of a single interface, select the eth1 interface.In the case if a dual interface, select eth2.

× -	+ v	-	×
	Network configuration Please select an interface to configure: eth0 3c:57:31:ff:10:de th1 3c:57:31:ff:10:df		
	< OK > <cancel></cancel>		

Step 4 Select the interface as DPI+Snort port.

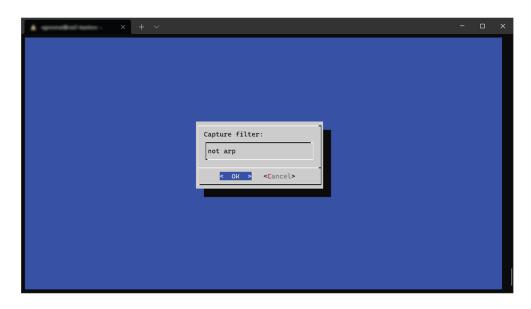


Step 5 Configure a capture filter mode. You can do that later in the Cisco Cyber Vision sensor page clicking the Capture mode button.

For more information on how to configure a capture mode filter, refer to the Cisco Cyber Vision GUI user guide.

× + ×		-	×
	Capture filter:		

For example, you can type "not arp".



In the Cisco Cyber Vision administration sensor page, the new virtual sensor appears and is ready to receive data.

alialia cisco								I	₩ 8.
ø	I System	Sensors							
B	Data Manage					packages to deploy Cisco Cyb nust authorize it so the Center		ensors. Sensors can also	o be remotely
.	🙏 Network Organizat	ion							
C	Sensors	^ Name	IP	Version	Status	Processing status	Active	Capture Mode [©]	Uptime
Q	- Sensors						Discovery status		
۵	 Capture 	▼ CENTER-ETH1	N/A	N/A	Running	Waiting for data	Unavailable	not arp	N/A
	糸 Users	 Name: CENTER 	ETH1 🖋						
	⊲ Events	Status: Running Processing statu	IS: Waiting for data						
	& API	Active discovery Deployment: Au	tomatic via DHCP				Remov	ve Capture Mode	Disable IDS
	₩ License	Capture mode:	not arp						
	条 LDAP Settings				5				
	⊖ Snort					IMANAGE CREDENTIALS	LUPDATE CISCO DEV	/ICES + DEPLOY CIS	CO DEVICE
	Risk score					+15	ISTALL SENSOR MANU	UALLY DIMPORT O	FFLINE FILE



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, on page 73
- Center unenrollment, on page 76
- Force the unenrollement of a Center, on page 77

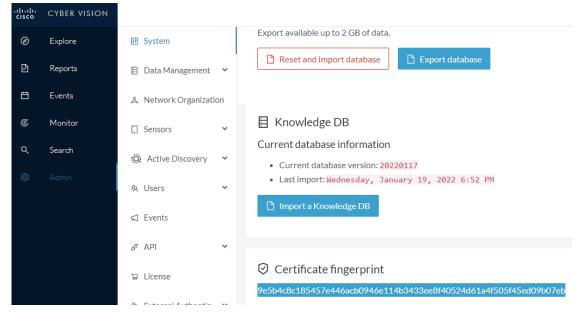
Center enrollment

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.



- **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

uluilu cisco	CYBER VISION Global Center			
Ø	Explore	됀 System	System managem	REGISTER A CENTER X
Ð	Reports	🗐 Data Management 🛛 💙	From this page you can manage cer	Name*: My Center 01
Ë	Events	System management	Register a Center	
م	Search	— Management		Fingerprint : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61
¢		첫 Users 🗸		OK Cancel
		🖾 Events		

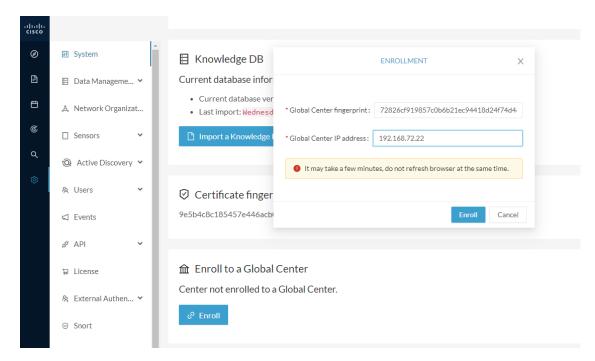
Step 3 Stay in the Global Center, on the same menu (Admin - System management - Management) and copy the Fingerprint of the Global Center.

System management

From	this page you can mana	ge centers and s	ensors.				
Ð	Register a Center			Fingerprin	t: 72826cf919857c0b6b21ec9	94418d24f74d4d2cf2bc742e76844	4554078abaa0c
	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
	My Center 01			Registered		Notenrolled	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



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	Х
r		-	
er d		Enrollment succeeded.	
	0	Connection test with global center 192.168.72.22 succeeded	
	0	Calculated size of data to transfer: 78.6 kB	
	\oslash	Synchronization started	
r			
b(ta is being synchronized with the global center. You can follow achronization progress on Admin page.	
			ОК
al C	en	ter	

What to do next

System management

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.

From th	is page you can manag	e centers	s and senso	rs.								
🖪 R	egister a Center					Fir	gerprint: 7	2826cf	919857c0b6b21ec94418	d24f74d	4d2cf2bc742e7684	44554078abaa0c 🖸
	Center Name	IP		Version		Enrollment state	ıs	Up	time	Conne	ctivity Status	Action
-	My Center 01	Center 01 192.168.72.21 SBS: 4.1.0+202 KDB: 2022011		Enrolled			5 days 16 hrs 52 mins 12 secs		cted	Unenroll		
	Sensor Name		IP		Version		Status		Processing Status	C	Capture mode	Up Time
	Sensor My Sensor 1		192.168	.69.21	4.1.0+2022011	171423	Connected		Pending data	A	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.

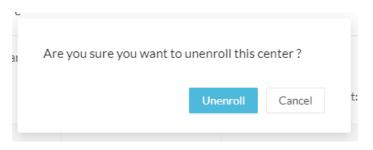
Step 2 Click Unenroll on the Center required.

System management

From th	nis page you can manage	e centers and senso	rs.				
₽ R	legister a Center			Fingerprint: 7	2826cf919857c0b6b21ec9441	8d24f74d4d2cf2bc742e768444	554078abaa0c
	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.



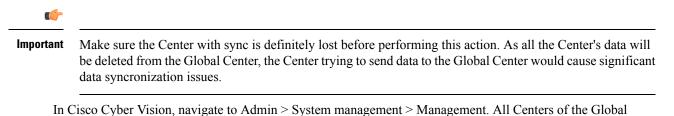
All Center's data are deleted from the Global Center. The Center is then ready to be enrolled again in the Global Center or in another Global Center.

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.

Register	a Center		Fingerpr	rint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0			
Center I	Name IP	Version	Enrollment status	Up time	Connectivity Status	Action	
My Cen	ter 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.



Center are listed.

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

System management

From this page you can manage centers and sensors.

🗄 Register a Center				Fingerprint:	72826cf919857c0b6b2	326cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c		
	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	



Upgrade procedures

- Architecture with a Global Center, on page 79
- Architecture with a single Center, on page 82

Architecture with a Global Center

Check the Global Center and Centers' health

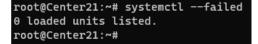
It is highly recommended that you check the health of the Centers connected to the Global Center and of the Global Center itself before proceeding to the update. To do so:

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.



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</version>		
Step 2	Launch the update using the following command: sbs-update install /data/tmp/CiscoCyberVision-update-sensor- <version>.dat</version>		

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:
- 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):
- 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</version>						
Step 2	Launch the update using the following command:						
	sbs-update install /data/tmp/CiscoCyberVision-update-sensor- <version>.dat</version>						

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</version>				
Step 2 Step 3	In Cisco Cyber Vision, navigate to Admin > Extensions. 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 Step 5	Navigate to Admin > Sensors > Sensor Explorer. 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</version>				

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

I