# cisco.



### **Cisco Cyber Vision Center VM Installation Guide, Release 4.4.0**

**First Published:** 2021-01-01 **Last Modified:** 2023-12-13

### **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 © 2019–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	About this documentation 1
	Document purpose 1
	Warnings and notices 1
CHAPTER 2	Information and characteristics 3
	Information and Characteristics <b>3</b>
CHAPTER 3	Requirements for installation 7
	Requirements for installation 7
CHAPTER 4	Install the Virtual Center 9
	Retrieve the installation file <b>9</b>
	ESXi 10
	Create a Virtual Machine <b>10</b>
	Boot the Virtual Machine <b>15</b>
	Hyper-V 17
	Create a Virtual Machine <b>17</b>
	Configure the disk size <b>21</b>
	Create the network interfaces 23
	Map the network interfaces <b>26</b>
	Boot the Virtual Machine <b>28</b>
CHAPTER 5	Configure the Center 31
	Basic Center configuration <b>31</b>
	Access the basic Center configuration 32
	Accept the End User License Agreement 32

	Select the language to match your keyboard <b>33</b>
	Select the Center type <b>33</b>
	Center 34
	Global Center 35
	Configure the Center's Administration Network Interface <b>36</b>
	Set interfaces (dual or single) 38
	Configure the Center's DNS <b>38</b>
	Synchronize the Center and the sensors to NTP servers <b>38</b>
	Give the Center a name 40
	Set the Center's password 40
	Configure the Center's Collection network interface <b>41</b>
	Authorize networks 41
	Complete the basic Center configuration 42
	Cisco Cyber Vision configuration <b>43</b>
	Install the certificate in your browser <b>43</b>
	Install Cisco Cyber Vision 49
	Configure the user interface security <b>52</b>
	Upload a p12 53
	Generate a CSR 55
	Configure Center data synchronization 57
CHAPTER 6	Configure a Center DPI 61
	Configure a Center DPI 61
CHAPTER 7	Configure the Cisco Cyber Vision Center synchronization 65
	Global Center Configuration 65
	Center enrollment <b>65</b>
	Center unenrollment <b>68</b>
	Force the unenrollement of a Center <b>69</b>
CHAPTER 8	Upgrade procedures 71
	Architecture with a Global Center <b>71</b>
	Check the Global Center and Centers' health 71
	Update the Global Center <b>72</b>

I

I

Cisco Cyber Vision Center VM Installation Guide, Release 4.4.0

	Update the sensors <b>72</b>
	Update hardware sensors 72
	Update IOx sensors <b>73</b>
	Architecture with a single Center <b>74</b>
	Update the Center 74
	Update the sensors <b>74</b>
	Update hardware sensors 74
	Update IOx sensors <b>75</b>
CHAPTER 9	Certificate renewal 77
	Renew the certificate of a Center <b>77</b>
	Update the Global Center fingerprint <b>78</b>
	Update a Center with sync fingerprint 82
CHAPTER 10	Center Backup and Restore 89
	Backup and Restore Constraints 89
	Backup Cyber Vision Center <b>90</b>
	Restore Cyber Vision Center <b>90</b>
	Automate the Backup of the Cyber Vision Center 91
	Bash Script <b>92</b>
	Cron 92

### 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 4.3.0.

## 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.



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 and characteristics**

• Information and Characteristics, on page 3

## **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):



#### 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 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
P5 C:\Users\ > Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List
Algorithm : SHA512
Hash : 1338BF61A17110AF80D751AE7B450F2829CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
18622E480B8BEBB9594D816
Path : C:\Users\ \Downloads\CiscoCyberVision-center-3.2.3.ova

Step 6

ESXi

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

### Software Download

ownloads Home / Security / Network Visi	bility a	Details		×
Q Search	$\frown$	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	$\sim$	Release Notes for 3.	2.3 Advisories 📑	
3	>	VMware OVA (C CiscoCyberVison	Center) - 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"				I Help - I Q Search -
Navigator	esx			
Host       Manage       Monitor       Image       Image	Get vCenter Server ( State: Non Uptime: 20.9	Register VM Shut down Reboot 0 Update 2 (Build 13981272) mal (not connected to any vCenter Server) 8 days	C Refresh   🏠 Actions	CPU FREE 27 GHz 2% USED: 526 MHz CAPACITY: 27 5 GHz MEMORY FREE: 69 30 GB 2,4% USED: 30,53 GB CAPACITY: 127,46 GB STORAGE FREE: 8 TB USED: 475,71 GB CAPACITY: 7,27 TB
	- Hardware		- Configuration	
	Manufacturer	Dell Inc.	Image profile	(Updated) ESXi-6.7.0-20190402001-stan
	Model	PowerEdge R440	vSnhare Hå state	Not configured
	► 🔲 CPU	12 CPUs x Intel(R) Xeon(R) Gold 5118 C PU @ 2.30GHz	<ul> <li>vMotion</li> </ul>	Not supported
	Memory	127.46 GB	- Sustan Information	
	Persistent Memory	0 B	System monitation	Tuesday, January 07, 2020, 12:20:02 UT
	🕨 🔚 Virtual flash	0 B used, 0 B capacity	Dateraine on nost	C
	✓ Q Networking		Install date	Tuesday, August 06, 2019, 15:59:07 UTC
	Hostname	esx	Asset tag	
	IP addresses	1. umid: 10.2.3.18	Serial number	H4Y9JY2
		2 vm0 500 4x0 071/5105	BIOS version	2.2.11
	DNS servers	1.10.2.3.254	BIOS release date	Friday, June 14, 2019, 02:00:00 +0200
Mar (SUI Nor	Recent tasks			

The wizard to create a new virtual machine opens.

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

				Q Search 🔹
Navigator	🗆 📔 esx			
✓	😰 New virtual machine			FREE: 27 GHz
Manage Monitor	<ul> <li>I Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Additional settings</li> <li>7 Ready to complete</li> </ul>	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.	РИСЕ 2013 САРАСТ 27.5 окт РИСЕ 2016 САРАСТ 27.6 ок РИСЕ 2016 САРАСТ 27.8 ок САРАСТ 7.27 ТВ 0190402001-stan
	VIIIVaiC			
			Back Next Finish Cancel	102:00:00 +0200
	Recent tasks	1. 10.2.3.204		13,02.00.00 ±0200

**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.

_	1
<ul> <li>1 Select creation type</li> </ul>	Select OVF and VMDK files
2 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
	Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
	X CiscoCyberVision-center-3.2.0.ova
	L
<b>vm</b> ware <sup>*</sup>	
VIIIVGIC	
	Back Next Finish Cancel
🔁 New virtual machine - CCV_Cente	r_dpi
<ul> <li>1 Select creation type</li> </ul>	Select OVF and VMDK files
2 Select OVF and VMDK files	Select the OVF and VMDK files or OVA for the VM you would like to deploy
<ul> <li>3 Select storage</li> <li>4 Deployment options</li> </ul>	
5 Ready to complete	Enter a name for the virtual machine.
	Vidual machine names can contain up to 90 characters and they must be unique within each ESVi instance
	Vindar madime names can contain up to oo characters and urey in bist of unique within each Low instance.
	× 📾 CiscoCyberVision-center-dpi-3.2.0.ova
	× 📾 CiscoCyberVision-center-dpi-3.2.0.ova
	× 📾 CiscoCyberVision-center-dpi-3.2.0.ova
	× 📼 CiscoCyberVision-center-dpi-3.2.0.ova
	×  CiscoCyberVision-center-dpi-3.2.0.ova
	× 🖬 CiscoCyberVision-center-dpi-3.2.0.ova
vmware	× 🖬 CiscoCyberVision-center-dpi-3.2.0.ova
<b>vm</b> ware <sup>,</sup>	× 🖬 CiscoCyberVision-center-dpi-3.2.0.ova

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

L

<b>vm</b> ware <sup>,</sup> Esxi	$\sim$					magnass	Help <del>-</del>	Q Search
" Navigator	🗆 📔 esx							
🔻 🚪 Host	🔁 New virtual machine - Cisco Cyber	Vision VM						EREE 27 ON-
Manage Monitor P P Virtual Machines Storage Q Networking	<ul> <li>✓ 1 Select creation type</li> <li>✓ 2 Select OVF and VMDK files</li> <li>✓ 3 Select storape</li> <li>4 License agreements</li> <li>5 Deployment options</li> <li>6 Additional settings</li> <li>7 Ready to complete</li> </ul>	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 FRE: 90.35 GHE FRE: 90.35 GHE CAPACITY: 127.46 GB FRE: 8.8 TB 6% CAPACITY: 7.27 TB
	<b>vm</b> ware <sup>.</sup>	Name v datastore1	Capacity ~ 7.27 TB	Free ~ 6.8 TB	Type ~ VMFS6	Thin pro ~ Supported	Access v Single 1 items	0190402001-stan 020, 12:30:03 UT 19, 15:59:07 UTC
	Recent tasks	1. 10.2.3.29			Back N	lext Fi	inish Cancel	02:00:00 +0200

### **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		
<ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> </ul>	Deployment options Select deployment options		
4 Deployment options     5 Ready to complete	Network mappings	nat Administration	
	Deployment type	Small Use this configuration for small deployments. This deployment will nee	<ul> <li>✓</li> <li>✓</li> <li>And 2 vC</li> </ul>
	Disk provisioning	PUs and 8GB Memory for the vApp.	
	Power on automatically		
		Back Next Finish	Cance
		Back Next Finish	Canc
🔁 New virtual machine - CCV_Cent	er	Back Next Finish	Canc
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> </ul>	er           Deployment options           Select deployment options	Back Next Finish	Canc
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings	Back Next Finish	Canc
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options 5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings	Back Next Finish	Canc
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VIMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings           Disk provisionin	Back Next Finish	Canc
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings           Disk provisioning           Power on automatically	Back Next Finish	Cance
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VINDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings           Disk provisioning           Power on automatically	Back Next Finish	Cance
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings           Disk provisioning           Power on automatically	Back Next Finish	Cance
<ul> <li>New virtual machine - CCV_Cent</li> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er           Deployment options           Select deployment options           Network mappings           Disk provisioning           Power on automatically	Back Next Finish	Cance
New virtual machine - CCV_Cent <ul> <li>1 Select creation type</li> <li>2 Select OVF and VMDK files</li> <li>3 Select storage</li> <li>4 Deployment options</li> <li>5 Ready to complete</li> </ul>	er          Deployment options         Select deployment options         Network mappings         Disk provisioning         Power on automatically	Back Next Finish	Cance
New virtual machine - CCV_Cent 1 Select creation type 2 Select Storage 3 Select storage 4 Deployment options 5 Ready to complete	er          Deployment options         Select deployment options         Network mappings         Disk provisioning         Power on automatically	Back Next Finish	Canc

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



Your new VM is displayed in the virtual machine list.

Host		😨 Oraște / Register VIA 📗 🧐 Consola	L b Dowor on the	Damar off	anand Defrech		0.0	
Manage			Poweron .	Foweron 11 Su	spend   C Reliesi   🖓	Actions	(Q Searc	1
Wohitor		U. Virtual machine	✓ Status ✓	Used space	✓ Guest OS ✓	Host name	✓ Host CPU	Host mem
🖆 Virtual Machines	13	E. Sim person	•	43.08	(the (64-64)	Uningun	0.58%	0.98
Storage		🗆., 🍘 pag, pantar	•	4.09-08	Other (54-66)	Uningun	0.58%	0.948
🧕 Networking	8	🗆 🐞 Will German	•	10.40.08	Other (54-64)	Uningun	12 181	4.03.08
		🗆 🐞 vitti - Cartler	•	14.45.08	Other (54-64)	Uningun	23 Miles	8.05.08
		E. Steat the		87.61.08	Deban DNULmus 1	Uningun	0.58%	110
		🗆. 🐞 608, x3, x81		18-01-08	(Thur (54-64)	Uningun	211 10010	8.05.08
		D. Still certer		5.41.08	(thur (54-64)	Uningun	0.58%	0.948
		🗆., 🍈 608, X1, M2	•	8.15.08	Other (54-64)	Uningun	17 Miles	4.03.08
		C. RFR-Caus-Fag-Dealter		5.84.08	Ubuffs Liter (54-bit)	Uninput	0.58%	0.100
		🗆. 🐞 11.4, 31, 301		12.71.08	(The (64-64)	Uningun	21.0840	2.21.08
		E		18.08.08	Debian ONULinux 1	Uninput	5.58%	1.89-08
		E. Ann the	•	200.448	Other (54-50)	Uningun	0.58%	0.148
		🔲. 👘 Cisco Cyber Vision VM	No	200 MB	Other (64-bit)	Unknown	0 MHz	0 MB
		Quick filters	~					13 item

### **Boot the Virtual Machine**

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

**1.** Click the VM in the list.

Manage								
		Create / Register VM   Provide Console	Power on	Power off II Sus	pend   C Refresh   🔅	Actions	Q Search	
Monitor		. Virtual machine	✓ Status ✓	Used space	✓ Guest OS ✓	Host name	✓ Host CPU ✓	Host mem
🖆 Virtual Machines	13	E	•	43.08	Other (54-66)	Uninput	0.58%	0.100
Storage	1	E. se, serier	•	4.00-08	Other (54-55)	Uningun	0.58%	0.00
🔮 Networking	8	E. Butte Server		10.40.08	Other (54-56)	Uninput	12 181	4.03.08
		E. D VIE Certer	•	14.45.08	Other (54-56)	Uningun	23.98%	8.05.08
		E. Start sta		87.81.08	Detran DNULmar 1.	Unknown	0.58%	0.100
		🗆., 🍈 608, x0, x0	•	18.01.08	Other (54-56)	Uningun	211 10010	8.05.08
		E. Statemen		5.41.08	Other (54-64)	Uningun	0.58%	0.100
		🗆., 🍈 608, yi, yii	•	8.15.08	Other (54-56)	Uningun	17 Miles	4.03-08
		. Strik Cause Fag Deacher		5.04.08	Uburtla Linux (54-60)	Uningun	0.58%	110
		🗆., 🍈 144, 93, 991	•	1271-08	Other (54-56)	Uningun	21.0840	2.21.08
			• ***	18.08.08	Detran DNULmus 1.	Uninput	5.58%	1.85-08
		E		200.448	Other (54-56)	Uningun	0.58%	0.10
		Cisco Cyber Vision VM	🕑 No	200 MB	Other (64-bit)	Unknown	0 MHz	0 MB
		(						13 itoms

**2.** Power on the VM.

Vm	ware" esxi"		Help -   Q Search -
	🚯 Cisco Cyber Vision VM		
	📝 Console 🛛 Monitor 📔 🕨 Power of	n 🔳 Power off 🔢 Suspend 💿 Restart   🥜 Edit   🤁 Refresh   🎄 Action	s
🔝 💷 🐂 Navigator	2	Cisco Cyber Vision VM Guest 0S Office (64-bit) Compatibility ESX 6 6 virtual machine VMvare Tools No CPUs 2 Memory 4 GB	O MHZ O MHZ MEMORY O B STORAGE 200 MB
<b>B</b>	VMware Tools is not installed in thi the guest OS, e.g. graceful shutdor	s virtual machine. VMware Tools allows detailed guest information to be displayed a wn, reboot, etc. You should install VMware Tools. 🏠 Actions	as well as allowing you to perform operations on $\times$
	✓ General Information		
	▶ Q Networking	No network information	
	VMware Tools	VMware Tools is not installed.	n Actions
	► Storage	1 disk	
	Notes		🥒 Edit notes
	✓ Hardware Configuration		
	Recent 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							- 🗆 ×
File Action View Help							
🗢 🏟 🖄 📰 🔝 🗊							
Hyper-V Manager	Virtual Machines						Actions
	Name	State	CPU Usage	Assigned Memory	Uptime	Status	WIN-ENHJK2D8JNK
	CCV_V300_01	Off					New
							🕼 Import Virtual Machine
							Hyper-V Settings
							Virtual Switch Manager
							🛃 Virtual SAN Manager
							🚅 Edit Disk
							Inspect Disk
	<						> Ston Service
	Checkpoints	Checkpoints					Remove Server
							B D-frank
			O Kerresh				
							View
							🛛 Help
							CCV_V300_01
							- Connect
							Settings
							3 Start
	CCV V200 01						🔂 Checkpoint
	CC+_+550_01						

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

∎∎ H	yper-	V Manager				
File	Acti	on View Help				
<b>(</b> =		New	>	Virtual Ma	chine	
H		Import Virtual Mach	nine	Hard Disk.		
		Hyper-V Settings		Floppy Disk		
		Virtual Switch Mana	aer		State	CPU
		Virtual SAN Manage	er	_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 4.4.0

### **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 Summary	Location:     C:\Hyper-V\Virtual hard Disks\       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\Vrtual hard Disks\CiscoCyberVision-3.0.0_1.vhdx     Browse
	<ul> <li>Attach a virtual hard disk later</li> <li>Use this option to skip this step now and attach an existing virtual hard disk later.</li> </ul>

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

Before You Begin Specify Name and Location Specify Generation	You have succ 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 e	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 M	anager		
File	Action	View	Help	
🦛 🖷	Co	nnect		
H	Set	tings		tual Machines
	Sta	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	Where is the virtual Location: C:\Hype C:\Hype Citing the follo Citing the follo Choose Actions Choose Ac	hard disk file located? r-V(Virtual hard Disks\CiscoCyberVision-3.0.0_1.vhdx Browse wwing types of virtual hard disks might result in data loss: ard ion	×
	Before You Begin Locate Disk Choose Action Configure Disk Summary	<ul> <li>What do you want to do to the virtual hard disk?</li> <li>Compact</li> <li>This option compacts the file size of a virtual hard disk. The storage capacity of remains the same.</li> <li>Convert</li> <li>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 disk can use a different type and format than the original virtual hard</li> <li>Expand</li> <li>This option expands the capacity of the virtual hard disk.</li> </ul>	the virtual hard disk l hard disk. The new rd disk.
		< 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	What size do you w Current size is betw New size: 250 Completing	ant to make the virtual hard disk? een 0 GB and 1 GB. GB (Maximum: 64 TB) rrd <b>the Edit Virtual Hard Disk Wizard</b>	×
	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	) make the following
		To complete the action and close 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 Machiner							Actions
WIN-ENHJR2D8JNR	News	Chata	CDUUIssas	Assisted Memory	Unting	Shahur		WIN-ENHJR2D8JNR
		State 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 — 🗆 🗙
<ul> <li>Virtual Switches</li> <li>New virtual network switch</li> <li>Global Network Settings</li> <li>MAC Address Range 00-15-5D-00-4A-00 to 00-15-5D-0</li> </ul>	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 computer. An

- 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 Switches     Mew virtual network switch     Admin     Internal only     Global Network Settings     MAC Address Range     00-15-5D-00-4A-00 to 00-15-5D-0	Xirtual Switch Properties       Name:       Admini       Notes:
	Connection type What do you want to connect this virtual switch to? O 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.

- **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	~	ŭ   ▲		
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	lad	SCSI Controller		
Memory	bieu	Network Adapter		
8192 MB		RemoteFX 3D Video Adapter		
Processor     1 Virtual processor		Legacy Network Adapter Fibre Channel Adapter		
IDE Controller 0				Add
Hard Drive     GiscoCyberVision-3	0.0 1	Virtual machines are created with one network adapter. You can add	addition	al networ

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			
Tiyper-v Manager	Virtual Machines		
WIN-ENHJR2D8JNR	The dat machines		
	Name	State	CPU Usage
		011	
		Uff	
	🗧 Center	011	
		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 43

## **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.

Cisco Cyl	per Vision Center Setup
	Helcome This is the first boot of your Cisco Cyber Vision Center.
	<pre></pre>

### Accept the End User License Agreement

Ci	isco Cyber Vision Center Setup
	End User License Agreement Effective: May 22, 2017 This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from
	Whom you acquired the Software. "Entitlement" means the license
Ci	isco Cyber Vision Center Setup
	conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. The parties agree that the English version of the EULA will govern in the event of a conflict between it and any version translated into another language. Cisco and the Cisco logo are trademarks or registered trademarks of Diego and/or its affiliates in the ULS and other countries. To view a
	list of Cisco trademarks, go to this URL: WHW.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)
	EXIT >



### Select the language to match your keyboard

Cyber Visi	on Center Setup		
Ch	oose uour keuboa	rd Manning.	
		s American r French	
	d i e	e German t Italian s Spanish	
		(Paper)	
	K 08	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.

- gaster to to to to	Center Setup	
What tupe of	center do uou want to install?	1
What type of	center do you want to install?	]
What type of	center do you want to install? Center Global Center Honitoring multiple centers	
What type of	center do you want to install? Eenter Global Center Honitoring multiple centers	
What type of	Center do you want to install?  Eenter Global Center Frocessing sensor data fronitoring multiple centers  COK > Cancel>	
What type of	center do you want to install?  Center Global Center Monitoring multiple centers  COK > Cancel>	

### Center

If installing a Center, select the first option.

What type	of center do yc	ou want to inst	a11?		]
What type	of center do yc <mark>Center</mark> Global	ou want to inst Proce I Center Monit	all? ssing sensor data oring multiple ce	nters	
What type :	of center do yo <mark>Center</mark> Global	ou want to inst r Proce l Center Monit	all? <mark>ssing sensor data</mark> oring multiple ce	nters	

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
Cancel>

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

### **Global Center**

If installing a Global Center, select the second option.



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

you trying to restore enter and need to aally set the center id
K No > K 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.

co Cyber (	Jision Center Setup
	Please select configuration type for the ACCESS interface HCP Automatic (DHCPv4) Manual Static IP and gateway
	Cancel>

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

• Manually:

Cisco Cyber V	Jision Center Setup
	Please select configuration type for the ACCESS
	Manual Static IP and gateway
	L
Cisco Cyber V	Jision Center Setup
	and the second secon
	Setup Access Network Interface
	IP Address 10.2.3.102
	Netmask 24 Gateway 18.2.3.254
	198%
	< 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.

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.

· ·
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
Cancel>

If you choose the Dual option, you will later be directed to: Configure the Center's Collection network interface, on page 41.

### **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 1 208.67.228.220 Alt 2 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 ent	er some NTP tim	e servers:	
'hey will hich is r	be used to sync equired to gene	hronize the Cente rate correct cert	er's clock, ificates.
he server server i ey ID and eparated ormat: se eave this	s must be separ s composed by i an AES 128 CMA by semicolon. rver_address[;k field empty to	ated by whitespac ts address and op C key value (32 h ey_id;key_value] use local time o	e. utionally by a nex character) unly.
10.2.3.25	4		
	( 01 )	(Cancel)	

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

Cisco Cyl	ber Vision Center Setup	
	Please enter some NTP time servers: They will be used to synchronize the Center's clock, which is required to generate correct certificates. The servers must be separated by whitespace. A server is composed by its address and optionally by a key ID and an AES 128 CMAC key value (32 hex character) separated by semicolon. Format: server_address(;key_id;key_value] Leave this field empty to use local time only. 10.0.5, 10;1;9:06132554ad5a369370f00d536fa0fc9	
	Cance 1>	

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 no	ом: Tue Oct 29 16	5:37:43 2019 UTC	
If this is below (MMI	s incorrect, plea DDhhmm[[CC]YY][.s	use specify current UTC ti ss])	ме
Leave empt	ty or cancel to s	skip.	
_			
-			
	< 0X >	<cancel></cancel>	

### Give the Center a name

yber V	Jision 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 <u>← OK →</u> <cancel></cancel>	

Enter the Center name provided by your administrator or type 'Default' which is a secure value.



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.



Confirm the password.

Cisco Cuber Vision Cente	er Setun
	* 000kp
	Please confirm the cu-admin password
	-
	Cancel>

### **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 38 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.
	192.168.69.1/24

### **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.

Please pro on the adm are author	ovide networks au Ministration inte rized Local net	uthorized to contact erface. By default a work is: 192 168 72	the center 11 networks
fultiple i	networks must be	COMMa-separated.	0, 21
<u>0</u> .0.0.0/0	3		
	< 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.

Cisco Cyl	ber 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/
	<u>&lt; 0</u> R >

Enter OK to finish the basic Center configuration.



**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 43 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 49.

#### 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.

I

ersonal Other Pe	eople	Intermediate Certification	Authorities Tru	sted Root Certificat	ion
Issued To		Issued By	Expiratio	Friendly Name	^
Contractors.	-	Address Extend CA.	845,000	India (Million)	61
California Calif	-	Ballmore CuberTrust	12/10/2012	Deploy I Ballener -	
Carlue CA		Carlum CA	1,04,000	Centure	
Garlus Trails	6.78	Carture Trusted Netwo	111200	Centure Trusted	
Case Real CA	1.04	Caso Root CA 3248	14033-000	-Clarge >	
Caro Real CA		Caro Rost (A.P.)	10111-0010	(Term)	
Cana Reat CA		Caso Roat (A.H)	10111-001	-Charge -	
Caro Real CA	1.00	Caro Rost CA NJ	12112	-Charles -	
Case Rot, AL		Caso RHC #2	1000 1000	(Tere)	~
Import E Certificate intended Server Authenticati Stamping, Encrypti Iser	Export. d purpo ion, Clie ng File S	Remove ses ent Authentication, Secure System, IP security tunnel	Email, Code Sign termination, IP se	ing, Time ecurity View	vance

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.



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

	·				
Certificate Sto Certificat	ore e stores are sys	tem areas whe	re certificates	are kept.	
Windows the certif	can automatical icate.	lly select a certi	ificate store, o	or you can spec	ify a location fo
	tomatically selec	ct the certificate	e store based	on the type of	certificate
Pla	ce all certificate	s in the followin	ng store		
Ce	ertificate store:				
٦	rusted Root Cer	rtification Autho	orities		Browse

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

🗲 🛛 ᡒ Certificate Import Wizard	×					
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 Authoriti	es					
Content Certificate						
Fin	ish Cancel					

#### What to do next

Install Cisco Cyber Vision, on page 49

## **Install Cisco Cyber Vision**

Access the Cisco Cyber Vision installation wizard:

#### Procedure

Step 1	With yo	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	The setu	p wizard used for the first access to Cisco Cyber Vision is displayed:			
Step 3	Create	an admin account:			

	Please follow this few steps to be fully ready to use the product	
2 Create the first user	$\overrightarrow{\mathbb{P}_{\mathcal{R}}}$ Agree to the license terms	🕢 Done
Firstname :	Lastname ':	
Email *:		
Password *:	Confirm password *:	
Suggested password: \$kvIH2Qq*odz90fj0E3	O C	

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:

	 cisco	
	Welcome to Cyber Vision	
	Please follow this few steps to be fully ready to use the product	
Create the first user	Agree to the license terms	⊘ Done
End User License Agreement		
Effective: May 22, 2017		
"Using" means to download, insta	· · ·	
computer programs and any Upgrad "Documentation" is the Cisco use applicable to the Software and mm (ii) the Cisco authorized resells "Entitlement" means the license of (PID) published on Cisco's price updates, upgrades, bug fixes, err copies thereof. Table of Contents	11, activate, access or otherwise use the Software. es made available to You by an Approved Source and r or technical manuals, training materials, specifi ade available to You by an Approved Source. "Approv er, distributor or systems integrator from whom you detail; including license metric, duration, and qua list, claim certificate or right to use notification ror corrections, enhancements and other modification	. "Software" means the Cisco licensed to You by Cisco. ications or other documentation ved Source" means (i) Cisco or u acquired the Software. antity provided in a product ID ion. "Upgrades" means all ons to the Software and backup
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 of (PID) published on Cisco's price updates, upgrades, bug fixes, ern copies thereof. Table of Contents 1. Acceptance of Terms	11, activate, access or otherwise use the Software. es made available to You by an Approved Source and r or technical manuals, training materials, specifi ade available to You by an Approved Source. "Approv er, distributor or systems integrator from whom you detail; including license metric, duration, and qua list, claim certificate or right to use notificati ror corrections, enhancements and other modification	. "Software" means the Cisco licensed to You by Cisco. ications or other documentation ved Source" means (i) Cisco or u acquired the Software. antity provided in a product ID ion. "Upgrades" means all ons to the Software and backup
computer programs and any Upgrad "Documentation" is the Cisco use applicable to the Software and mm (ii) the Cisco authorized resells "Entitlement" means the license of (PID) published on Cisco's price updates, upgrades, bug fixes, err copies thereof. Table of Contents 1. Acceptance of Terms 2. License	Il, activate, access or otherwise use the Software. es made available to You by an Approved Source and r or technical manuals, training materials, specifi ade available to You by an Approved Source. "Approv er, distributor or systems integrator from whom you detail; including license metric, duration, and qua list, claim certificate or right to use notification ror corrections, enhancements and other modification Acopy of the license can be found at cisco.com	. "Software" means the Cisco licensed to You by Cisco. ications or other documentation ved Source" means (i) Cisco or u acquired the Software. antity provided in a product ID ion. "Upgrades" means all ons to the Software and backup

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 52.

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 57.

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 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	
1	
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.

•••••	Ø	
File selected: CenterA	D2019.2019lab.local1.pfx	
		6
le Corro		

#### Step 5 Click Reload.

Step 4

**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		۲		
٩	Cookies	2 in use	ß		
۵	Site settings		Z	r -	
-					

#### What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 57.

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		
CSR has been generated. Please import the certificate.	]	
FQDN: CenterAD2019.2019lab.local		
	র	
Import a complete PEM bundle (concatenated CA, subCA, certificate)		
. 1		
Choose a file or drag and drop to upload		
	Discard	
		o 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.

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	
	Discard 🗈 Sav

Step 7

#### 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.

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

 centerad2019.2019lab.local
 ×

 Connection is secure
 •

 Cookies
 2 in use

 Site settings
 2

#### What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 57.

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 1In the Global Center's Cisco Cyber Vision GUI, navigate to Admin > System Management > Management.Step 2Click 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.

- **Step 3** In the Center's Cisco Cyber Vision GUI, navigate to Admin > System.
- **Step 4** Scroll down to Certificate fingerprint and copy it.



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



Step 6

#### field Click OK.

The Center appears in the list as unenrolled.

 cisco	CYBER VISION Global Center						
Ø		년 System	System manag	emen	t		
Ð	Reports	Data management					
Ħ		System manage ^	From this page you can mana	ge centers :	and sensors.		
م		— Management	Register a Center				
\$	Admin	— Capture	Name	IP	Version	Status	Processing Status
		冬 Users ~	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.



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 browser is the same time.	not refresh
Global Center Ingerprint - _fc3fe05036f06028d1a0b3cde545b6bde5b18ccdc67c3bcd87	ac5fac7513126
Global Center IP address* 192.168.72.17	
	🗲 Enroll Cancel

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



## **Configure a Center DPI**

• Configure a Center DPI, on page 61

## **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	I System	Sensors
B	🗏 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 rehorded, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.
<b></b>	& Network Organization	
¢	Sensors	No sensors found.
Q	- Sensors	Please check the following:
۵	- Capture	Sensor(s) are powered on     Sensor(s) are connected to the same network as the Center 'COLLECTION' interface.
	육 Users 🗸	AMANAGE CREDENTIALS
	< Events	
	.d ADI	

# Step 2Open the Center shell prompt and type the following command:<br/>sbs-netconf



**Step 3** In the case of a single interface, select the eth1 interface.

In the case if a dual interface, select eth2.

× + ×	,	-	•	×
	Network configuration			
	ethe 3c:57:31:ff:10:de			
	th1 3c:57:31:ff:10:df			
	< OV > <cancel></cancel>			

**Step 4** Select the interface as DPI+Snort port.

A second state ×	+ ~	-	۵	×
	Con Company and Man			
	Please select configuration type: Please select configuration type: Manual Static IP and gateway DHCP Automatic (DHCPW) Bridge Add to SSS bridge PI-Snort port Set ethl as DPI-Snort interfae			
	< OK > <cancel></cancel>			

**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.



For example, you can type "not arp".

× + ~		-	•	×
	Capture filter: not arp Capture filter: cost arp Capture filter:			

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

uludu. cisco								Ŀ	₫ 8 -
ø	I System	Sensors							
Ð	🗄 Data Manage 👻	From this page, you can man and securely rebooted, shut	age sensors in onli down, and erased.	ne and offline modes and g When a sensor connects f	generate provisioning or the first time, you r	packages to deploy Cisco Cyb nust authorize it so the Center	per Vision on remote s r can receive its data.	ensors. Sensors can also	be remotely
	& Network Organization								
¢	Sensors ^	Name	IP	Version	Status	Processing status	Active	Capture Mode <sup>@</sup>	Uptime
Q	<ul> <li>Sensors</li> </ul>						status		
۲	<ul> <li>Capture</li> </ul>	▼ CENTER-ETH1	N/A	N/A	Running	Waiting for data	Unavailable	not arp	N/A
	条 Users 🗸 🗸	Name: CENTER-ETH1							
	< ⊂ Events	Status: Running Processing status: Misi	ing for data						
	ø API ∽	Active discovery: Unav	ailable				1 Remov	e Capture Mode	Disable IDS
	₩ License	Deployment: Automati Capture mode: not ar	c via DHCP P						
	条 LDAP Settings	<ul> <li>Start recording sense</li> </ul>	or						
					-	MANAGE CREDENTIALS	1 UPDATE CISCO DEV	ICES + DEPLOY CIS	CO DEVICE
	O SHOL					+1	NSTALL SENSOR MANU		FLINE FILE
	Risk score								

I



## **Configure the Cisco Cyber Vision Center** synchronization

Global Center Configuration, on page 65

## **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.



- **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

cisco	CYBER VISION Global Center			
Ø	Explore	া System	System managem	REGISTER A CENTER X
Đ	Reports	🗐 Data Management 🛛 💙	From this page you can manage cer	N
Ħ	Events	System management	Register a Center	Name : My Center UI
۹	Search	— Management		Fingerprint : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61
¢		条 Users 🗸 🗸		OV Correl
		🖾 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 manage centers and sensors.									
ŀ	Register a Center			Fingerprin	at: 72826cf919857c0b6b21ec9	4418d24f74d4d2cf2bc742e76844	4554078abaa0c 🗊		
	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


**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	×
r er	S Enrollment succeeded.	
a	<ul> <li>Connection test with global center 192.168.72.22 succeeded</li> <li>Calculated size of data to transfer: 78.6 kB</li> </ul>	
r bi	<ul> <li>Synchronization started</li> <li>Data is being synchronized with the global center. You can follow synchronization progress on Admin page.</li> </ul>	
al C	Lenter	ОК

#### 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 th	is page you can manage	e centers	s and senso	rs.							
₽ R	egister a Center					Fir	gerprint: 72	826cf	919857c0b6b21ec94418c	124f74d4d2cf2bc742e7684	44554078abaa0c โ
	Center Name	ter Name IP Version		Enrollment status		Up time (		Connectivity Status	Action		
•	My Center 01	192.1	68.72.21	SBS: 4.1.0+2 KDB: 20220	02201171404 117	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	68.69.21 4.1.0+202201		171423 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 th	rom this page you can manage centers and sensors.									
₽ R	egister 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.

L

# **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	n this page you can manag	e centers and se	nsors.				
Ð	Register a Center			Fingerpri	nt: 72826cf919857c0b6b21ec9	4418d24f74d4d2cf2bc742e768444	1554078abaa0c 🗓
	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.

$\sim$			
51	ictom	mana	annant
$\mathcal{I}$	JULIII	mana	SCHICHU

From th	-rom this page you can manage centers and sensors.									
₽ R	legister a Center	Fingerprint:			72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c					
	Center Name	IP	Version	Enrollment status	Uptime	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 71
- Architecture with a single Center, on page 74

## **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:
	<pre>sbs-update install /data/tmp/CiscoCyberVision-update-sensor-<version>.dat</version></pre>

#### **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 <b>Update</b> 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



# **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



A message indicates that the certificare has expired.

I

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 <b>10.2.2.206</b> . 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.
	in 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.
	Go Back (Recommended) Advanced
	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
	View Certificate
	Go Back (Recommended) Accept the Risk and Continue

- 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.

$\leftarrow$	C O	https:/	/10.2.2.20	5/#/admin/system-ma	anagement		ŝ	$\bigtriangledown$	500	Ŧ	ර	≡	
uluili cisco										~	8	$\sim$	
Ø	⊌¶ System		Syst	tem manag	ement								
Ð	🗄 Data Manager	ment ~	From th	From this page you can manage centers and sensors									
Ë	System manage	gement						0-50050-400500-564-04-04-04-0050750					
۹	冬 Users ~				ringerprint. 76	ur / obulu3270e556e66ic6	074060818218	e1275270140	15101070	123103	13717		
¢	⊲ Events		Center Name	IP	Version	En	rollment stat	us		Up tim	ie		
	ଟ API	~	+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+2023071 KDB: 20230712	20954 Ou fin	utdated globa gerprint 🕕	l center		4 days secs	17	

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 th	iis page you can manage	centers and senso	rs.				
₽ R	egister a Center		Fingerprint:	78d7768dfd3a9de558e68fc8d940e0af82f8e129529df4d31d169623183f37f9			
	Center Name	IP	Version	Enrollment status	Up time The center needs to be informed of		
+	Center 10.2.2.106	10.2.2.206	SBS: 5.0.0+202307120954 KDB: 20230712	Outdated global center fingerprint ①	the new fingerprint of the Global Centers 17 hrs 37 mins 39 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.

$\leftarrow \rightarrow$	C	🔿 🔓 https://1	0.2.2.206/#/			<del>ک</del>	$\bigtriangledown$	500 U	Η	ර	≡
.ılı.ılı. cısco				습 Home ▼	System issues Action required	▲ 78	days rema Evaluatio	aining n Mode	~	8	)~
Ø											
£				•							
Ë				$\underline{\land}$							
¢				System ale	rts						
٩				The Global Center finge	erprint has changed						
¢	III 🕑	Protocol distribution	1	Please update it in: Sy	rstem page						
	Prot	ocol distribution			ОК						
						Global C	Center fin	gerprint	has	×	
					Jul 12 2023 4-5	cnanged					

#### Step 7 Click OK.

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

$\leftarrow \  \  \rightarrow$	C 🗘 https://10.2.2.206/#/			ŝ	ତ 😻 🚺	Ŧ	പ =			
ululu cisco	🔂 Home	•	System issues     Action required	<b>∆ 78</b>	days remaining Evaluation Mode	~	8~			
Ø										
Ð	Welcom	ne to Cis	co Cyber Visio	n						
Ħ	Last 30 days overview									
¢	Opera	ational overview	Security overview							
<u>م</u> ه	✓ All ✓ Protocol distribution ✓ Most critical events (	Presets highlight								
	Protocol distribution		Most critical events			C				

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.

¢	System issues Action required	<b>∆ 78</b>	days remaining Evaluation Mode					
	The Global Center fi	ngerprint ha	as changed					
$\otimes$	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.



The Update Global Center fingerprint window pops up.

Current database version: 20230712     UPDATE GLOBAL CENTER FINGERPRINT X									
* Global Center fingerprint :									
Update Cano	el d'								



Paste the Global Center fingerprint and click Update.

Current database vers	ion: 20230712								
UPDATE GLOBAL CENTER FINGERPRINT X									
* Global Center fingerprint :	eOaf82f8e129529df4d31d169623183f37f9								
LADII CJ. JCD IT, LUZJ	Update Cancel								

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

$\leftarrow$	C C https	://10.2.2.206/#/admin/system	☆	. 🔊 🔊	•	பி	≡
uluilu cisco			▲ 7	8 days remaining Evaluation Mod	e L~	2 8	· ~
Ø	년 System	Current database information					
Ē	🗐 Data Management 🛛 🗡	<ul> <li>Current database version: 20230712</li> <li>Last import: Wednesday, July 12, 2023 4:57 PM</li> </ul>					
Ħ	& Network Organization	The KDB is managed by the global center, you cannot update it from this	center.				
C	. Sensors ~						
Q	Q Active Discovery	Center fingerprint	050 0/04 17/ 4				
ŝ	冬 Users ~	Fingerprint: 2467927254bda15561dc48bc26116d14b6ee00b Expires: Sep 14, 2025	258a9631d76ae1	b91fd/56894			
	⊲ Events						
	s <sup>or</sup> API ~	命 Enroll to a Global Center					
	₽ License	Center enrolled to a Global Center.					
	条 External Authentic ×						
	⊙ Snort	▲ Reset Unroll the center on the Global Center Administration page t	Global Cen updated.	ter fingerprint s	uccessful	ly ×	
	@ Dick score						

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

$\leftarrow \rightarrow$	C	O 🔓 http	ps://10.2.2	.205/#/admin/syster	m-management		\$	9	ළ අ ව ≡			
uluilu cisco									<u>⊬</u> 8×			
Ø	태 System		Syst	tem mana	gement							
£	🗄 Data Managen	nent ~	From th	iis page you can mar	nage centers and s	sensors.						
Ħ	🗵 System manag	ement					04040-0-60360-130E304643314460633403637					
۹	冬 Users	~	ΗR	egister a Center		Fingerprint: 78d7768	dtd3a9de558e68tc8d940e	20af82f8e129529df4d3	10169623183f37f9			
¢	Sector Events			Center Name	IP	Version	Enrollment status	Up time	Connectivity Status			
	ø API	~	+	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.

L



#### 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.

$\leftarrow \  \  \rightarrow$	C A https://10.2.2.206/#/			☆	. 😌 🔤		Ε	ב כ
.ı ı.ı ı. cısco		☆ Home ▼	System issues     Action required		<b>78</b> days remaining Evaluation Mode		~	8~
Ø	_							
Ē.								
Ħ								
C		System alerts						
۹	All Protocol distribution	This center is out of sync with the Global Center	abal Center to					
礅		update it						
_	Protocol distribution		ок					
		201 mij m	(x)	This ce	nter is out of sync wit	h the		×

#### Step 4 Click OK.

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

I

$\leftarrow \  \  \rightarrow$	C 🗘 https://10.2.2.206/#/	☆	ତ 🦉		Ŧ	பி	≡
uluilu cisco	☆ Home ▼ Q System issues Action required	▲ 7	8 days remainin Evaluation M	g ode	~	٩	~
ø							
ß	Welcome to Cisco Cyber Vision	n					
Ħ	Last 30 days overview						
¢	Operational overview Security overview						

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

☆ Home ▼		System issues Action required		<b>∆ 78</b>	days remaining Evaluation Mode
Contentiation of the System Ma	nc with the Global Center	obal 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.

~	$\rightarrow$	С	🔿 🔒 http:	s://10.2.2.206/#/admin/system		<u>ک</u>	⊌ 😌	Ŧ	ර =
رارر دری	 sco				System issues Action required	▲ <b>78</b> day Eva	s remaining luation Mode	~	<b>8</b> ~
Ģ	Ð	If System		E Knowledge DB					
E	P-	🗄 Data Manage	ement ~	Current database information <ul> <li>Current database version: 20230712</li> </ul>					
Ė	<b>3</b>	್ಲಿ Network Org	ganization	Last import: Wednesday, July 12, 2023 4 The KDB is managed by the global center, you cannot update it	: 57 PM				
	3	. Sensors	~						
c t	ک چ	Active Disco	overy ~	⊘ Center fingerprint					
		冬 Users	~	Fingerprint: 2467927254bda15561dc48bc26116d14	b6ee00b258a9631d76ae1	b91fd756894			
		⊲ Events		Expires: Sep 14, 2025					
		& API	~	命 Enroll to a Global Center					
		₩ License		Center enrolled but disconnected, due to the u	pdate of the certificate of tl	nis center.			
		祭 External Aut	hentic 🗡	Certificate fingerprint must be updated in the G	lobal Center System Manag	ement page.			
		⊘ Snort							
		② Risk score		Keset Unroll the center on the Global Center Administration	page to be able to reset a C	enter.			

**Step 5** Access the **Global Center**.

$\leftarrow \   \rightarrow \   {\tt G}$		○ A https://10.2.2.205/#/explore	e/		☆	🖂 颜 🚺	中 む	≡			
.ı ı.ı ı. cısco				Explore		System issues Action required	<u>~</u> 8	) ~			
Ø	Pres	ets + New Preset					88	:=			
Ē	All N	ly preset Basics Asset management Conti	rol Syst	ems Management IT Communication Management Sec	curity Net	twork Management					
Ë	My preset										
۹		Namo		Description							
~		Name		Description							
τέτ	+	All data grouped	٩	All devices and activities are listed in this preset. This preset should not be used and other more well defined preset 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							
	Basic	25									
	Name Des			iption							

#### **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
$\otimes$	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.

$\leftarrow \  \  \rightarrow$	C	0 🔓 h	ttps://10.2	.2.205/#/admin/syste	em-management			☆	ତ 🐓		$\pm$	ර =
 cisco								C Syste	m issues <b>n required</b>		~	8~
Ø	해 System		Syst	em manag	gement							
£	🗐 Data Manageme	ent ~	From th	is page you can mana	age centers and se	ensors.						
Ħ	System manager	ment										
۹	冬 Users	~				ringerpri		10034191007437097	J0a4524r3	00131.	20050	5603 1
٩	⊲ Events			Center Name	IP	Version	Enrollment status	Up time	Con	nectivit	y Statı	ıs
	s <sup>ợ</sup> API	~	+	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	Inac	tive for	6 mins (	35 secs

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

An Update Center fingerprint window pops up.

٦		UPDATE CENTER FINGERPRINT	×
u	* Center fingerprint :		
٦		Update Cancel	

#### **Step 8** Paste the Center fingerprint.

٦		UPDATE CENTER FINGERPRINT	
u	* Center fingerprint :	26116d14b6ee00b258a9631d76ae1b91fd756894	
١		Update Cancel	

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.

0

$\leftarrow$	C C A h	https://10.2.2.205/#/admin/syste	m-management			\$	v 👺 🚺 🕂	ර =
ululu cisco							~	8~
Ø	If System	System manag	ement					
£	🗏 Data Management 🗠	From this page you can mana	ge centers and se	ensors.				
Ħ	System management	Register a Center		Fingerpr	int: cdaa48be19440f302	fd5df651c63419f6674a7c	970da4524f3b01312cd5c	3e83 🗓
۹	冬 Users ~							
\$		Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Actic
	ø <sup>⊄</sup> API Ý	+ 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
	糸 External Authentic ヾ							
	< Integrations 🗸 🗸							
	Extensions							
	Web Server Certificate							
	∕⊃ SNMP					Center finger updated. Plea list to be fully	print successfully se wait for the centers updated.	×

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





# **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, on page 89
- Backup Cyber Vision Center, on page 90
- Restore Cyber Vision Center, on page 90
- Automate the Backup of the Cyber Vision Center, on page 91
- Bash Script, on page 92
- Cron, on page 92

## **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	I 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, fi	rst return the ticense 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-back	xup/ccv-center-backup-Center2244331abautomccvlocal-4.4.0-20240405112443.tar.gz

In the above given example, the created file is called:: ccv-center-backup-Center2244331abautomccvlocal-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-Center2244331abautomccvlocal-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:~#

**Step 2** Relone 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, relone 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/



## 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

