cisco.



Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.3.0

First Published: 2021-01-01 Last Modified: 2023-12-21

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 | Getting started 3 |
| | Overview 3 |
| | Prerequisites 4 |
| | Supported features 4 |
| | Limitations 4 |
| | Configure the AWS environment 4 |
| | Create Elastic IPs 5 |
| CHAPTER 3 | — Deploy the Cisco Cyber Vision Center 9 |
| | Create and configure the instance 9 |
| | Allocate an Elastic IP to the instance 17 |
| | Cisco Cyber Vision Center setup 19 |
| | Establish a serial connection 19 |
| | Open an SSH connection from AWS 21 |
| | Basic Center configuration 24 |
| | Accept the End User License Agreement 24 |
| | Select the language to match your keyboard 25 |
| | Select the Center type 25 |
| | Configure the Center's DNS 28 |
| | Synchronize the Center and the sensors to NTP servers 28 |
| | Give the Center a name 29 |
| | Authorize networks 30 |

Set DHCP 30

Complete the basic Center configuration **31**

| CHAPTER 4 | Connect to the Center 33 |
|-----------|--|
| | Using the GUI 33 |
| | Using the console 34 |
| CHAPTER 5 | Configure the Center 35 |
| | Install Cisco Cyber Vision 35 |
| | Cisco Cyber Vision configuration 38 |
| | Install the certificate in your browser 38 |
| | Install Cisco Cyber Vision 44 |
| | Configure the user interface security 47 |
| | Upload a p12 48 |
| | Generate a CSR 50 |
| | Configure Center data synchronization 52 |
| CHAPTER 6 | Deploy sensors 57 |
| CHAPTER 7 | Configure the Cisco Cyber Vision Center synchronization 59 |
| | Global Center Configuration 59 |
| | Center enrollment 59 |
| | Center unenrollment 62 |
| | Force the unenrollement of a Center 63 |
| CHAPTER 8 | Annex – Setup Center ison file 65 |



CHAPIEK

About this documentation

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

Document purpose

Amazon Virtual Private Cloud (Amazon VPC) is for launching Amazon WebServices (AWS) resources into a customized virtual network. This virtual network looks like a traditional network, with the benefits of using the scalable infrastructure of AWS.

This document explains how to deploy Cisco Cyber Vision Virtual on AWS.

This manual 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.



Important In

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



Note

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



Getting started

- Overview, on page 3
- Prerequisites, on page 4
- Supported features, on page 4
- Limitations, on page 4
- Configure the AWS environment, on page 4
- Create Elastic IPs, on page 5

Overview

AWS is a collection of remote computing services offered by Amazon.com, also called web services, that make up a cloud-computing platform. These services operate from 11 geographical regions across the world.

In general, the user should become familiar with the following AWS services when deploying Cisco Cyber Vision Center and Cisco Cyber Vision Global Center:

• Amazon Elastic Compute Cloud (EC2)

A web service that enables you to rent virtual computers to launch and manage your own applications and services, such as a Cisco Cyber Vision Center, in Amazon's data centers.

Amazon Virtual Private Cloud (VPC)

A web service that enables you to configure an isolated private network that exists within the Amazon public cloud. You run your EC2 instances within a VPC.

• Amazon Simple Storage Service (S3)

A web service that provides you with a data storage infrastructure.

You create an account on AWS, set up the VPC and EC2 components (using either the AWS Wizards or manual configuration), and choose an Amazon Machine Image (AMI) instance. The AMI is a template that contains the software configuration needed to launch your instance.



Note

The AMI images are not available for download outside of the AWS environment.

Prerequisites

- An Amazon account.
- An SSH client (required to access the Cisco Cyber Vision Center console).
- Communication path: public/elastic IPs for access to the Cisco Cyber Vision resources.
- An Elastic IP (the default public IP change after a reboot. This can cause an issue for sensors).
- Minimum configuration to run and test the product are 8 vCPU and 16GB RAM.
- SSD disks are mandatory.

Supported features

- Center
- Global Center



For details about Center resources, refer to the Cisco Cyber Vision VM Installation Guide available in cisco.com.

Limitations

The following features or hardware are not supported:

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

Configure the AWS environment

To deploy Cisco Cyber Vision on AWS you need to configure an Amazon VPC with your deployment-specific requirements and settings. In most situations, a setup wizard can guide you through your setup. AWS provides online documentation where you can find useful information about the services ranging from introduction to advanced features.

Refer to https://aws.amazon.com/documentation/gettingstarted/ for more information.

Additional information:

VM sizing

L

Minimum – up to 500 components:

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

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

Create Elastic IPs

When an instance is created, a public IP address is associated with the instance. That public IP address changes automatically when you stop and start the instance. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. Elastic IPs are reserved public IPs that are used for remote access to the Cisco Cyber Vision as well as other instances.

- 1. Access you Amazon account.
- 2. Navigate to Services > EC2.



3. Under Network & Security, click Elastic IPs.

| aws Services v | \ensuremath{Q} [Search for services, features, marketplace products, and | docs | [Option+S] | Σ | ¢ |
|--|--|----------------------|---------------------------------------|--------------------|-------------------|
| Network & Security Security Groups New Elastic IPs New | Welcome to the new EC2 console! We're redesigning the EC2 console to make it eas them and let us know where we can make improv | ier to us vements | se and improve p s. To switch betw | erforma een the | ince. W old co |
| Placement Groups | | | | | |
| Key Pairs | Resources | | | | |
| Network Interfaces New | | | | | |
| Load Balancing | You are using the following Amazon EC2 reso | urces in | the Europe (Irela | nd) Regi | ion: |
| Load Balancers | Instances (running) | 0 | Dedicated Hos | ts | |
| Target Groups New | Elastic IPs | 0 | Instances | | |
| ▼ Auto Scaling | Key pairs | 8 | Load balancer | s | |
| Launch Configurations | Placement groups | 0 | Security aroun | IS | |

4. Click Allocate Elastic IP address.

| Scheduled Instances | | |
|------------------------|--------------------------------------|--------------------------------------|
| Capacity Reservations | | |
| ▼ Images | Elastic IP addresses | Actions Allocate Elastic IP address |
| AMIs | Q Filter Elastic IP addresses | |
| Elastic Block Store | | < 1 > © |
| Volumes | | |
| Snapshots | Name | ▽ Allocated IPv4 add ♡ Type |
| Lifecycle Manager | | |
| Network & Security | | |
| Security Groups New | | |
| Elastic IPs New | | |
| Placement Groups | | |
| Key Pairs | | |
| Network Interfaces New | | |

5. Click Allocate to create the Elastic IP.

| EC2 > Elastic IP addresses > Allocate Elastic IP address | |
|--|-------------------------------|
| Allocate Elastic IP address Info | |
| Elastic IP address settings Info | |
| Public IPv4 address pool | |
| Amazon's pool of IPv4 addresses | |
| Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more 2 | |
| Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more | |
| can help improve the availability and latency for your user traffic by using the Amazon global network. Learn Create accelerator | n more 🔁 |
| Tags - optional A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can your resources or track your AWS costs. | use tags to search and filter |
| No tags associated with the resource. | |
| Add new tag | |
| You can add up to 50 more tag | |
| | Cancel Allocate |

6. Check the new Elastic IP out.



I



Deploy the Cisco Cyber Vision Center

- Create and configure the instance, on page 9
- Allocate an Elastic IP to the instance, on page 17
- Cisco Cyber Vision Center setup, on page 19

Create and configure the instance

Procedure

Step 1 Go to https://aws.amazon.com Amazon Web Services and sign in.



| aws | Services | Q Search | [Op | tion+S] |
|-----|---|--|--|----------------------------------|
| = | EC2 > Insta | nces > Launch an instance | | |
| | Launch Amazon EC2 a following the | an instance Info allows you to create virtual machines, or instance simple steps below. | es, that run on the AWS Cloud | I. Quickly get started by |
| | Name a | nd tags Info | | |
| | Name | | | |
| | e.g. My W | leb Server | | Add additional tags |
| | ▼ Appli An AMI i: launch y | cation and OS Images (Amazon Mac s a template that contains the software configuration (o our instance. Search or Browse for AMIs if you don't see ber vision | nine Image) Info perating system, application serve what you are looking for below | r, and applications) required to |

Step 6 In the AWS Marketplace AMIs menu, select Cisco Cyber Vision BYOL.

Choose an Amazon Machine Image (AMI)

| An AMI is a template that contains the s required to launch your instance. You ca you can select one of your own AMIs. | oftware configuration (opera n select an AMI provided by A | ting system, application server, and applications) WS, our user community, or the AWS Marketplace; or | |
|--|---|--|--|
| Q cyber vision | | | × |
| Quickstart AMIs (0) My A Commonly used AMIs Create | MIs (0) AWS Marketp and by me AWS & trusted to | Hace AMIs (1) Community AMIs (7) hird-party AMIs Published by anyone | |
| Refine results | cyber vision (1 resul | () showing 1 - 1 | <pre>< 1 > @</pre> Sort By: Relevance |
| Categories Infrastructure Software (1) V Publisher Cisco (1) V Pricing model | altalta cisco | Cisco Cyber Vision BYOL By Cisco C Ver 4.1.3 Cisco Cyber Vision is a cybersecurity solution specifically designed for o water distribution, oil & gas, manufacturing and public transportation 1 resilience and safety of their industrial operations. It provides asset own | rganizations in power and to ensure continuity, ners with full visibility into |
| Bring Your Own | | | |



Click Continue.

| Overview Product details Pricing Usage Support Cisco Cyber Vision is a cybersecurity solution specifically designed to ensure continuity, resilience and safety of industrial operations. It automatically discovers monitors industrial assets and processes to detect threats and anomalies and extend IT security to the OT domain through seamless Typical total price 50.042/Hr Latest version Categories 60.042/Hr Security Delivery methods Security Delivery methods Amazon Machine Image ③ Operating systems Other Cyber Vision 4.3.0 Other Cyber Vision 4.1.4 Other Cyber Vision 4.1.4 Security Network Infrastructure | altalu cisco | Cisco Cyber Vision BYOL Cisco Systems, Inc. 🖄 | | |
|--|---|---|--|---|
| Clsco Cyber Vision is a cybersecurity solution specifically designed to ensure continuity, resilience and safety of industrial operations. It automatically discovers monitors industrial assets and processes to detect threats and anomalies and extend IT security to the OT domain through seamless Typical total price Latest version Latest version Categories Catego | Overview | Product details Pricing | Usage Support | |
| 4.3.0 Security 'otal pricing per instance for services hosted on t3.medium nus-east-1. Delivery methods Network Infrastructure Amazon Machine Image ① Operating systems Other Cyber Vision 4.3.0 Other Cyber Vision 4.1.4 Other Cyber Vision 4.1.4 | Jisco Cyber Vis nonitors indus Typical total p | sion is a cybersecurity solution specifica strial assets and processes to detect thr rice | ally designed to ensure continuity, resilienc reats and anomalies and extend IT security Latest version | e and safety of industrial operations. It automatically discovers ar to the OT domain through seamless Categories |
| | 0.042/Hr Fotal pricing per n us-east-1. See additional pr | instance for services hosted on t3.medium ricing information. | 4.3.0 Delivery methods Amazon Machine Image (2) Operating systems Other Cyber Vision 4.3.0 Other Cyber Vision 4.1.4 | Security Network Infrastructure |

Step 8 Slide down to instance type.

| Supported instance families |
|---|
| • C5, C5a, C5ad, C5d, C5n, C6g, C6gd |
| • M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd |
| • R5, R5a, R5ad, R5d, R5dn, R5n, R6, R6gd |
| • T3, T3a, T4g |
| • Z1d |

Step 9

Select an instance type by typing for example "t3.xlarge".

| ▼ Instance type Info Get advice | |
|---|--|
| Instance type t3.medium Family: t3 2 vCPU 4 GiB Memory Current generation: true Q t3.xl | All generations Compare instance types this product. |
| Family: t3 4 vCPU 16 GiB Memory Current generation: true Key pair (login) Info | |

Step 10 Select or create a new key pair.

| ▼ Key pair (login) Info | |
|--|---|
| You can use a key pair to securely connect to your instance. Ensure tha before you launch the instance. | at you have access to the selected key pair |
| Key pair name - <i>required</i> | |
| JMA | C Create new key pair |
| | |

| Key pair name | euroly |
|--|--|
| JMA | curety. |
| he name can include upto 255 ASCII characters. I | t can't include leading or trailing spaces. |
| ley pair type | |
| RSA RSA encrypted private and public key pair | C ED25519 ED25519 encrypted private and public key pair |
| rivate key file format | |
| | |
|) .pem | |
| For use with OpenSSH | |
| .pem For use with OpenSSH .ppk For use with PuTTY | |
| .pem For use with OpenSSH .ppk For use with PuTTY Men prompted, store the private k your computer. You will need it later mero 54 | ey in a secure and accessible location on er to connect to your instance. Learn |

A file called YOURKEYPAIRNAME.pem will be downloaded.

Step 11 Slide down to Network settings and click **Edit**.

| ▼ Network settings Info | | Edit |
|--|---|----------------------------------|
| Network Info | | |
| vpc-015e027ecdf241329 | | |
| Subnet Info | | |
| No preference (Default subnet in any availa | ibility zone) | |
| Auto-assign public IP Info | | |
| Enable | | |
| Firewall (security groups) Info A security group is a set of firewall rules that contrinstance. | rol the traffic for your instance. Add rules to allow | v specific traffic to reach your |
| • Create security group | ○ Select existing security group | |

Step 12 Set Auto-assign public IP to **Disable**.

| ▼ Network settings Info | |
|--|--------------------------------|
| VPC - required Info | |
| vpc-015e027ecdf241329 (default) 172.31.0.0/16 | C |
| Subnet Info | |
| No preference 💌 | C Create new subnet |
| Auto-assign public IP Info | |
| Disable | |
| Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow instance. | specific traffic to reach your |
| • Create security group | |

Inbound Security Group Rules appears.

| Type Info | Protocol Info | Port range Info |
|--|-------------------------------------|-----------------------------|
| ssh 🔻 | ТСР | 22 |
| Source type Info | Source Info | Description - optional Info |
| Anywhere v | Q Add CIDR, prefix list or security | e.g. SSH for admin desktop |
| | 0.0.0.0/0 × | |
| Security group rule 2 (TCP, 443, 0 | .0.0.0/0) | Remove |
| Type Info | Protocol Info | Port range Info |
| HTTPS 🔻 | ТСР | 443 |
| Source type Info | Source Info | Description - optional Info |
| Anywhere v | Q Add CIDR, prefix list or security | e.g. SSH for admin desktop |
| | 0.0.0/0 × | |
| | | |
| 1 | | |

Step 13 Click **Add security group rule** to start configuring AWS firewall settings.

Add the rules that provide access from users or other resources to the Center.

List of the ports that need to be added:

• For Global Center <--> Center communication

| Protocol | Port |
|----------|----------------|
| AMPQ | TCP/5671 |
| NTP | UDP/123 |
| Syslog | UDP/TCP 514 |
| SSH | TCP/22 |

• For CS workstation/ntp server <--> Center communication

| Protocol | Port |
|----------|---------|
| HTTPS | TCP/443 |
| SSH | TCP/22 |
| NTP | UDP/123 |

• For Sensor <--> Center communication

| Protocol | Port |
|----------|-----------|
| AMPQ | TCP/5671 |
| Syslog | UDP/10514 |

Example of security configuration:

| Туре | Protocol | Port range | Source type | Description |
|------------|----------|------------|-------------|-------------------------------|
| SSH | ТСР | 22 | 0.0.0/0 | SSH |
| HTTPS | ТСР | 443 | 0.0.0/0 | HTTPS |
| Custom TCP | ТСР | 5671 | 0.0.0/0 | AMPQ |
| Custom UDP | UDP | 123 | 0.0.0/0 | NTP |
| Custom TCP | ТСР | 514 | 0.0.0.0/0 | Syslog (for Global Center) |
| Custom UDP | UDP | 514 | 0.0.0.0/0 | Syslog (for Global Center) |
| Custom UDP | UDP | 10514 | 0.0.0/0 | Syslog (for sensor) |

Step 14

Configure storage by changing the value or ,if needed, adding a new volume.

NoteMake sure to setup the correct disk size as this information will remain and cannot be modified.NoteDo not use the Magnetic (Standard) for Volume Type.

Note Default type will be SSD.

For example, we change 100 GiB default value to 500.

| ▼ Configure storage Info | Advanced |
|--|----------|
| 1x 500 GiB gp2 Root volume (Not encrypted) | |
| Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage | × |
| Add new volume | |
| Olick refresh to view backup information The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies. | C |
| 0 x File systems | Edit |

Step 15 Depending on the Center type, fill the Advanced Details > User data part at the bottom of the page.

| ↑ Choose file | | |
|---------------|------|--|
| , | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

If a json file is used to specify the type of the Center, this step will be skipped during the installation.

- To deploy a Center, leave the textbox empty.
- To deploy a Center with sync, the minimal configuration is:

```
{
  "center-type": "Local Center",
}
• To deploy a Global Center, the minimal configuration is:
  {
  "center-type": "Global Center",
  }
```

For all json parameters, refer to Annex – Setup Center json file.

Step 16 Review the settings on the right summary and click **Launch instance**.

| 1 Software Image (AMI) Cisco Cyber Vision BYOL ami-045d09fc2dd6111e2 Virtual server type (instance type) t3.xlarge Firewall (security group) New security group Storage (volumes) 1 volume(s) - 500 GiB I ree tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
|---|---|
| Software Image (AMI) Cisco Cyber Vision BYOL ami-045d09fc2dd6111e2 Virtual server type (instance type) t3.xlarge Firewall (security group) New security group Storage (volumes) 1 volume(s) - 500 GiB | |
| Cisco Cyber Vision BYOL ami-045d09fc2dd6111e2 Virtual server type (instance type) t3.xlarge Firewall (security group) New security group Storage (volumes) 1 volume(s) - 500 GiB Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| Virtual server type (instance type) t3.xlarge Firewall (security group) New security group Storage (volumes) 1 volume(s) - 500 GiB Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| t3.xlarge Firewall (security group) New security group Storage (volumes) 1 volume(s) - 500 GiB (i) Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| Firewall (security group) New security group Storage (volumes) 1 volume(s) - 500 GiB Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| New security group Storage (volumes) 1 volume(s) - 500 GiB (i) Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| Storage (volumes) 1 volume(s) - 500 GiB (i) Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| 1 volume(s) - 500 GiB Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in | |
| the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet. | < |

The following status should appear.

| EC2 > Instances > Launch an instance |
|---|
| Claunching instance Subscribing to Marketplace AMI G4% |
| ▶ Details |
| Please wait while we launch your instance. |
| Do not close your browser while this is loading. |
| |
| EC2 > Instances > Launch an instance |
| Success Success Successfully initiated launch of instance (i-014b63c1220a99342) |

Allocate an Elastic IP to the instance

1. Click Instances in AWS left menu.



2. Choose your instance on the instances list and copy your instance ID.

| aws Services ▼ | Q Sec | arch for | services, | features, mar | ketplace [Option+ | •S] 🔉 - | 🗘 devops/wbo | udaa@cis | co.com @ 3286-0807 | -8092 🔻 | ✓ Ireland ▼ S | iupport | t v |
|--|-------|----------|----------------|--------------------|-------------------|-------------|------------------|----------|--------------------|----------|----------------------------------|---------|------------|
| New EC2 Experience Tell us what you think | × | Insta | nces (1 | /9) Info | C | Connect | Instance st | ate 🔻 | Actions 🔻 | | Launch instances | | • |
| EC2 Dashboard New | | Q F | ilter insta | ances | | | | | | | < 1 | > | 0 |
| Events | | | Name | \bigtriangledown | Instance ID | | Instance state | e 🗸 | Instance type | ∇ | Status check | | Alarn |
| Tags | | | - | | i-0710fe2b5d36 | ec422 | Θ Stopped | æΘ | t3.small | | - | | No ali |
| Limits | | | - | | i-08a2fda60d27 | '0e4b2 | ⊘ Running | æΘ | t2.micro | | ⊘ 2/2 checks pa | assed | No ali |
| ▼ Instances | | | - | | i-06e504824ccf | 8624f | ⊘ Running | QQ | t2.micro | | ⊘ 2/2 checks pa | assed | No ali |
| Instances New | | | - | | i-08f59928e6f5 | ec898 | ⊘ Running | æΘ | t3.medium | | ⊘ 2/2 checks pa | assed | No al |
| Instance Types | | | - | | i-0c2b04853a5c | ic4d4c | ⊘ Running | QQ | t3.medium | | ⊘ 2/2 checks pa | assed | No ali |
| Launch Templates | | | - | | i-014e278d036 | Of811e | ⊘ Running | æΘ | t3.medium | | ⊘ 2/2 checks pa | assed | No ali |
| Spot Requests | | | - | | i-04beddd7712 | :65b1e | ⊖ Terminate | ed⊕Q | c5a.large | | - | | No ali |
| Savings Plans | | ✓ | - | | i-0b19cd5b75ee | ?7cffa | ⊘ Running | ଇପ | c5a.large | | Initializing | | No ali |
| Reserved Instances New | | | | | | = | = | | | | | | |
| Dedicated Hosts | | Det | | C | Manual Area | C 1 | Charles also | | Mandanatan | | _ | | _ |
| Scheduled Instances | | Det | aits | Security | Networking | Storage | Status chi | ecks | Monitoring | Tags | | | |
| Capacity Reservations | | | | | | | | | | | | | |
| ▼ Images | | • | instance | summary I | nto | | | | | | | | |
| AMIs | | Insta | ance ID | | | Public IPv4 | address | | Private I | Pv4 add | dresses | | |
| | | ð | i-0b19c | d5b75ee7cffa | 3 | - | | | D 17 | 2.31.7.2 | 229 | | |

3. Click Elastic IPs in AWS left menu.

| aws Services v Q Se | arch for services, features, marketplace products, and | docs | [Option+S] | Σ | ¢ |
|--|--|------------------------|---------------------------------------|---------------------|------------------|
| Network & Security Security Groups New Elastic IPs New | Welcome to the new EC2 console! We're redesigning the EC2 console to make it ea them and let us know where we can make impro | sier to us ovements | e and improve po . To switch betwe | erforma en the o | nce. V old co |
| Placement Groups Key Pairs Network Interfaces New | Resources | | | | |
| ▼ Load Balancing | You are using the following Amazon EC2 reso | ources in t | the Europe (Irela | nd) Regi | on: |
| Load Balancers | Instances (running) | 0 | Dedicated Hos | ts | |
| Target Groups New | Elastic IPs | 0 | Instances | | |
| ▼ Auto Scaling | Key pairs | 8 | Load balancers | 5 | |
| Launch Configurations | Placement groups | 0 | Security aroup | s | |

4. Click the created Elastic IP.

| | aws Services v | Q Search for services, features, marketplace [Option+S] D ↔ devops/wboudaa@cisco.com @ 3286-0807-8092 ▼ | Ireland 🔻 Support 🔻 |
|---|--|---|---------------------|
| | Capacity Reservations | | |
| • | Images AMIs | Elastic IP addresses (1/1) | stic IP address |
| • | Elastic Block Store Volumes | Q. Filter Elastic IP addresses Public IPv4 address: 54.195.222.37 X Clear filters | (1) () |
| | Snapshots Lifecycle Manager | ☑ Name | |
| • | Network & Security Security Groups Elastic IPs | - 54.195.222.37 Public IP | eipalloc-0 |

5. Click Associate Elastic IP address.

| aws Services v | Search for services, features, marketplo | ace [Option+S] 🗵 🗘 | devops/wboudaa@cisco.com @ 32 | 86-0807-8092 ▼ Ireland ▼ Suppor |
|--|--|------------------------|--------------------------------|---------------------------------|
| Capacity Reservations Images AMIs | EC2 > Elastic IP addresses 54.195.222.37 | > 54.195.222.37 | Actions 🔻 | Associate Elastic IP address |
| Elastic Block Store | | | - | |
| Volumes | Summary | | | |
| Snapshots | | | | |
| Lifecycle Manager | Allocated IPv4 address | Туре | Allocation ID | Association ID |
| Network & Security | D 54.195.222.37 | D Public IP | eipalloc- 047232ca6e635d00c | - |
| Security Groups | Scope | Associated instance ID | Private IP address | Network interface ID |
| Elastic IPs | D VPC | - | - | - |
| Placement Groups | | | | |
| Key Pairs | Network interface owner account ID | Public DNS | NAT Gateway ID | Address pool |
| Network Interfaces New | - | - | - | |
| Load Balancing | | | 1 | |

6. Select Instance.

7. Paste the instance ID previously copied.

- 8. Click in the field and select the private IP address of the created Center.
- 9. Click Associate.

| Elastic IP address: 54 | 1.195.222.37 |
|---|---|
| Resource type Choose the type of resource with Instance Network interface | h which to associate the Elastic IP address. |
| A | |
| ▲ If you associate an E previously associate ☑ | clastic IP address to an instance that already has an Elastic IP address associated, this d Elastic IP address will be disassociated but still allocated to your account. Learn more |
| If you associate an E previously associate instance i-0b19cd5b75ee7cffa | Elastic IP address to an instance that already has an Elastic IP address associated, this d Elastic IP address will be disassociated but still allocated to your account. Learn more |
| ▲ If you associate an E previously associate ☑ Instance Q i-0b19cd5b75ee7cffa Private IP address The private IP address with which | Elastic IP address to an instance that already has an Elastic IP address associated, this d Elastic IP address will be disassociated but still allocated to your account. Learn more |
| If you associate an E previously associate instance i-Ob19cd5b75ee7cffa 'rivate IP address 'he private IP address with whic 172.31.7.229 | Elastic IP address to an instance that already has an Elastic IP address associated, this d Elastic IP address will be disassociated but still allocated to your account. Learn more X C h to associate the Elastic IP address. X |

The following status should appear.



Cisco Cyber Vision Center setup

Establish a serial connection or open an SSH connection from AWS and then proceed to the basic Center configuration.

Establish a serial connection

Procedure

Step 1 In the Instances menu, select the instance you just created and click **Connect**.

| EC2 Dashboard X | Instances (1/1) Info | C Connect | Instance state Actions | Launch instances | • |
|-------------------------|------------------------------------|--------------------|---------------------------|--------------------------|----------|
| EC2 Global View | Q Find Instance by attribute or ta | g (case-sensitive) | | < 1 > | ۲ |
| Events | ✓ Name ∠ ▼ Instar | ice ID Instance | state v Instance type v | Status check Alar | m status |
| Console-to-Code Preview | CenterJMA i-014 | o63c1220a99342 | ing € ⊖, t3.xlarge | ⊘ 2/2 checks passed No a | larms - |
| Instances | | | | | |
| Instances | | | | | |
| Instance Types | | | | | |

Step 2 Click EC2 serial console.

| EC2 > Instances > i-014b63c1220a99342 > Connect to | instance | | |
|--|----------------------------|--------|---------|
| Connect to instance Info Connect to your instance i-014b63c1220a99342 (CenterJMA) | using any of these options | | |
| EC2 Instance Connect Session Manager SSH c | lient EC2 serial console | | |
| Instance ID D i-014b63c1220a99342 (CenterJMA) | Serial port | | |
| | | Cancel | Connect |

Step 3 Click Connect.

Step 4 A new window with a shell prompt opens in the browser.

Step 5 Press Enter.

The Cisco Cyber Vision Center Setup appears.



Step 6 Press Enter.

Open an SSH connection from AWS

1. Go to instances to check the information of the created machine.

| aws Services v | Search for services, features, marketplace products, and | docs [Option+S] D A devops/wbouda | a@cisco.com @ 3286-0807-8092 ▼ Ireland ▼ Suppo |
|--|--|--|--|
| New EC2 Experience Tell us what you think | EC2 > Instances > i-0b19cd5b75ee7cffa | | |
| EC2 Dashboard New | Instance summary for i-0b19cd5b75 | ee7cffa Info | C Connect Instance state |
| Events | Updated less than a minute ago | | |
| Tags | Instance ID | Public IPv4 address | Private IPv4 addresses |
| Limits | i-0b19cd5b75ee7cffa | 54.195.222.37 open address 🖸 | ₫ 172.31.7.229 |
| Instances | | Dublic ID of DMC | Delivery ID-4 DNC |
| Instances New | | Public IPV4 DNS | Private IPV4 DNS |
| Instance Types | | 1 compute amazonaws com Lopen address 12 | □ Ip-172-31-7-229.eu-west-1.compute.inter |
| Launch Templates | | | |
| Spot Requests | Instance type | Elastic IP addresses | VPC ID |
| Savings Plans | c5a.large | 54.195.222.37 [Public IP] | D vpc-77b96d0e 🖸 |
| Reserved Instances New | AWS Compute Optimizer finding | IAM Role | Subnet ID |
| Dedicated Hosts | Opt-in to AWS Compute Optimizer for | - | 🗇 subnet-919a9cf7 🔼 |
| Scheduled Instances | recommendations. Learn more 🖸 | | |
| Capacity Reservations | | | |
| Images | Details Security Networking S | storage Status checks Monitoring Tag | IS |
| AMIs | | | |
| Flastic Block Store | ▼ Instance details Info | | |
| Volumos | Platform | AMI ID | Monitoring |
| Snapshots | Linux/UNIX (Inferred) | ami-0ddb5a307abb22bd2 | disabled |
| Lifecycle Manager | Platform details | AMI name | Termination protection |
| Notwork & Cocurity | D Linux/UNIX | Cyber Vision Center - 4.0.0-RC4 | Disabled |

The key previously created or chosen will be automatically added to /data/etc/ssh/userkey/root.



Note It is possible to add multiple keys on that file if an access is needed from another device that is not using the same certificates than the installed one.

This key is downloaded locally or already exists.

Please follow the steps below to connect using SSH and finalize the installation.

- 2. In the AWS EC2 management console, click Instances (1).
- 3. Choose the needed instance and click the Connect button (2).

| | | | | | 2 | | | | | | | | |
|---------|---------------------------|--------|-------------|--------------------|-------------------|--------------------|--------------------|------------|-------------------|---------------------|----------------------------------|--------|------------|
| | aws Services v Q s | learch | for service | s, features, ma | rketplace Option+ | s] 🔈 4 | 🗘 devops/wbo | udaa@cisco | .com @ 3286-0807- | 8092 🔻 | v Ireland ▼ S | upport | : v |
| | New EC2 Experience | Ins | tances | (1/9) Info | C | Connect | Instance st | ate 🔻 | Actions v | | Launch instances | | • |
| _ | EC2 Dashboard New | 0 | Filter in | stances | | | | | | | < 1 | > | ۲ |
| (1) | Events | | Nam | e 🗸 | Instance ID | | Instance state | ∇ | Instance type | ∇ | Status check | | Alarn |
| \prec | Tags | | - | | i-0710fe2b5d36 | ec422 | Θ Stopped | QQ | t3.small | | - | | No ali |
| | Limits | | - | | i-08a2fda60d270 | 0e4b2 | ⊘ Running | ଭ୍ର | t2.micro | | ⊘ 2/2 checks pa | issed | No ali |
| | ▼ Instances | | - | | i-06e504824ccf8 | 3624f | ⊘ Running | ଭ୍ର | t2.micro | | ⊘ 2/2 checks pa | issed | No ali |
| | Instances New | | - | | i-08f59928e6f5e | ec898 | ⊘ Running | ⊛Q | t3.medium | | ⊘ 2/2 checks pa | issed | No ali |
| | Instance Types | | - | | i-0c2b04853a5d | c4d4c | ⊘ Running | ⊛Q | t3.medium | | ⊘ 2/2 checks pa | issed | No ali |
| | Launch Templates | | - | | i-014e278d0360 |)f811e | ⊘ Running | €Q | t3.medium | | ⊘ 2/2 checks pa | issed | No al |
| | Spot Requests | | - | | i-04beddd7712c | :65b1e | Θ Terminate | d⊛Q | c5a.large | | - | | No al |
| | Savings Plans | | - | | i-0b19cd5b75ee | 7cffa | ⊘ Running | æΘ | c5a.large | | Initializing | | No al |
| | Reserved Instances New | | | | | | _ | | | | - | | |
| | Dedicated Hosts | 1 | Details | Security | Networking | Storage | Status che | ecks | Monitoring | Tags | | | |
| | Capacity Reservations | - | ▼ Instan | ce summarv | Info | | | | | | | | |
| | ▼ Images AMIs | h | nstance ID |) 9cd5b75ee7cfl | fa | Public IPv4 ; – | address | | Private II | Pv4 ado 2.31.7.2 | dresses | | |

4. Access the SSH Client menu (3) and follow the steps described in it.

| Connect to instance Info Connect to your instance I-0b19cd5b75ee7cffa using any of these options |
|--|
| EC2 Instance Connect Session Manager EC2 Serial Console |
| Instance ID |
| 🗗 i-0b19cd5b75ee7cffa |
| 1. Open an SSH client. |
| 2. Locate your private key file. The key used to launch this instance is wbo.pem |
| Run this command, if necessary, to ensure your key is not publicly viewable. chmod 400 wbo.pem |
| 4. Connect to your instance using its Public DNS: |
| D ec2-54-195-222-37.eu-west-1.compute.amazonaws.com |
| ∑ Example: |
| ssh -i "wbo.pem" root@ec2-54-195-222-37.eu-west-1.compute.amazonaws.com |
| |
| (3) Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name. |

- 5. Copy and paste the example (4) into the ssh client and replace 'root' with 'cv-admin', like below: ssh -i wbo.pem cv-admin@ec2-54-195-222-376.eu-west-1.compute.amazonaws.com
- 6. Once connected to the Center, type the following command:

sudo -i

7. Type the following command:

setup-center

| SBS 4.0.0 |
|--------------------------------------|
| cv-admin@ec2-52-31-40-71:~\$ |
| cv-admin@ec2-52-31-40-71:~\$ |
| cv-admin@ec2-52-31-40-71:~\$ sudo -i |
| root@ec2-52-31-40-71:~# |
| root@ec2-52-31-40-71:~# setup-center |

8. Press Enter.

The Cisco Cyber Vision Center Setup appears.



9. Press Enter.

Basic Center configuration

Accept the End User License Agreement

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

<Accept > <Decline>

Select the language to match your keyboard



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

| Choose your keyboard mapping. IS American fr French de German it Italian es Spanish (DK) (Cancel) | Cisco Cyber V | Jision Center Setup |
|---|---------------|--|
| Cancel> | | Choose your keyboard Mapping. IS American fr French de German ii Italian e: Spanish |
| | | 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.

| What type of center do you want to install? | |
|--|---|
| Center Processing sensor data Global Center Monitoring multiple centers | |
| Cance1> | - |

Center

If installing a Center, select the first option.

| Cisco Cyber | Vision | Center | Setup | | | | |
|-------------|---------|---------|-------------------------|--------------------------|------------|--------------------------|------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| _ | | | | | | | |
| What | type of | f cente | r do you want t | o install? | | | |
| | | | Center Global Center | Processing Monitoring | sensor dat | <mark>a</mark> enters | |
| | | | diobal center | nonreorrig | marcipic c | CITCEI 3 | |
| | | | <u> </u> | | Cancell | | - |
| | | | × UN Z | | Cancerz | | |
| | | | | | | | |

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

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

| Cisco Cyber Vision Cent | ər Setup |
|-------------------------|--|
| | Are you trying to restore a Center and need to Manually set the center id ? |
| | |
| | |

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

| Cisco Cyber Vision Cent | er Setup |
|-------------------------|--|
| | Are you trying to restore a Center and need to Manually set the center id ? |
| | <pre> Ko → K Yes →</pre> |
| | |

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 |
|--|
| |
| 1 |
| 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.

| oraco oguer vraton com | ter Setup | | |
|------------------------|---|--|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | 1 |
| What type of cen | nter do you want t | o install? | |
| What type of cen | nter do you want t Center | o install? Processing sensor data | |
| What type of cer | nter do you want t Center Global Center | o install? Processing sensor data Monitoring multiple centers | |
| What type of cer | nter do you want t Center Global Center | o install? Processing sensor data Monitoring multiple centers | |
| What type of cer | nter do you want t Center Slobal Center | o install? Processing sensor data Monitoring multiple centers (Cancel) | |
| What type of cen | nter do you want t Center Slobal Center (OK) | o install? Processing sensor data <u>Monitoring multiple centers</u> «Cancel» | |

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

| Are you trying to restore a Center and meed to Hanually set the center id |
|---|
| ? < ⊻es > |
| |

You will be directed to the next step.

Configure the Center's DNS

Type a DNS server address and optional fallbacks.

| Setup DNS configuration Up to three maximum, leave blank |
|---|
| unnecessary fields Preferred 208.67.222.222 Alt 1 208.67.220.220 < OK < Cancel> |
| |

Synchronize the Center and the sensors to NTP servers

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

| Cisco Cy | 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 ARS 128 CHMC key value (32 hex character) separated by semicolon. Format: server_address[;key_id;key_value] Leave this field empty to use local time only. | |
| | [18.2.3.254 | |
| | Cancel> | |
| | | |

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



The synchronization takes a few seconds.

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



Note The time is set in UTC standard.

| If this is incorrect, please specify current UTC time below (MMDDDhhmm[[CC]YY][.ss]) Leave empty or cancel to skip. | |
|---|---|
| Leave empty or cancel to skip. | is is incorrect, please specify current UTC time (MMDDbhmm[[CC]YY][.ss]) |
| _ | empty or cancel to skip. |
| L | |
| | |

Give the Center a name



Note 7

This name will be used in the Center certificate.

| | · · · |
|--|--|
| Please enter the FQDM | I name: |
| (It will be used as a certificate of this s DNS configuration for authentication) | common name for the TLS erver, so it must match a proper TLS |
| <u>C</u> enter | |
| < 0X > | <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.

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 provide networks on the administration in are authorized. Local ne | authorized to con nterface. By defau etwork is: 192.160 | ntact the center ult all networks 3.72.0/24 |
|---|---|---|
| Multiple networks must | be comma-separated | ι. |
| <u>0</u> .0.0.0/0 | | |
| | | |
| < 0K > | <cancel></cancel> | |

Set DHCP

Procedure

Step 1 If the following message appears, select OK.



Step 2 Select DHCP.

| Please : interfa | select co ce | nfigurat | ion typ | e for th | e ACCESS |
|---------------------|-----------------|--------------------------------|---|------------------------------|----------|
| | DHCP Manual | <mark>Automat</mark> Static | <mark>ic (DHC</mark> IP and | <mark>Pv4)</mark> gateway | |
| | < 0 | к > | <can< td=""><td>icel></td><td></td></can<> | icel> | |

Complete the basic Center configuration

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



Enter OK to finish the basic Center configuration.





- **Note** 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).



Connect to the Center

You can connect to the Center:

- Using the Using the GUI.
- Using the Using the console.
- Using the GUI, on page 33
- Using the console, on page 34

Using the GUI

The Public IP address and FQDN of your instance will be available on the Instance summary page:

| New EC2 Experience Tell us what you think | EC2 > Instances > i-0b19cd5b75ee7cf | fa | |
|---|--|--|--|
| EC2 Dashboard Events | Instance summary for i-0b19c Updated less than a minute ago | d5b75ee7cffa Info C | Connect Instance state |
| Tags Limits | Instance ID D i-0b19cd5b75ee7cffa | Public IPv4 address D 54.195.222.37 open address Z | Private IPv4 addresses D 172.31.7.229 |
| Instances New Instance Types Launch Templates | Instance state | Public IPv4 DNS Classical control con | Private IPv4 DNS D ip-172-31-7-229.eu-west- 1.compute.internal |
| Spot Requests Savings Plans Reserved Instances New | Instance type c5a.large | Elastic IP addresses D 54.195.222.37 [Public IP] | VPC ID |
| Dedicated Hosts Scheduled Instances Capacity Reservations | AWS Compute Optimizer finding ③Opt-in to AWS Compute Optimizer for recommendations. Learn more | IAM Role - | Subnet ID subnet-919a9cf7 🖸 |

- 1. In your browser, use the public IP address or the FQDN to download and save the certificate:
 - https://<Public IPV4 address>/ca/crt
 - https://<Public IPV4 DNS>/ca/crt
- 2. In your browser, use the following address to access Cisco Cyber Vision: https://<CENTERNAME>/.

You can proceed with Install Cisco Cyber Vision.

Using the console

You can connect to the Center using the AWS serial console.

Note Serial Console is only supported in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (Oregon), Europe (Ireland), Europe (Frankfurt), Asia Pacific (Sydney), Asia Pacific (Tokyo), Asia Pacific (Singapore).

To use the serial console, click Actions > Monitor and troubleshoot > EC2 Serial Console.

| New EC2 Experience Tell us what you think X EC2 Dashboard Events | Instances (1/5) Info C Connect Q Filter instances | Instance state | Launch instances Launch instance from template Connect | <mark>nch ir</mark> | istances 🔻 | < 1 | > |
|---|---|---------------------|--|---------------------|---------------------------------|----------|-------------|
| Tags | name 🗸 | Instance ID | Stop instance | \bigtriangledown | Instance type | ∇ | Stati |
| Limits | – | i-0410d9d9b(| Start instance | Q | t2.medium | | - |
| ▼ Instances | - | i-0710fe2b5d | Reboot instance | Q | t3.small | | - |
| Instances New | - | <u>i-0b19cd5b75</u> | Hibernate instance | Q | c5a.large | | ⊘ 2, |
| Instance Types | | 1.024524076 | Instance settings | Get Get | system log instance screensh | ot | <u>_</u> |
| Launch Templates | Instance: i-0b19cd | 5b75ee7cffa | Networking | ► Man | age detailed mon | itoring | |
| Spot Requests | | 1 | Security | Man | age CloudWatch | alarms | |
| Savings Plans | Details Security | / Networking | Image and templates | EC2 | Serial Console | | |
| Reserved Instances New | | | Monitor and troubleshoot | Rep | lace root volume | | |
| Dedicated Hosts | Instance summary | y Info | | | | | |

The root password by default will be the instance ID of the Center you created.

Supported instance families:

- A1
- C5, C5a, C5ad, C5d, C5n, C6g, C6gd
- M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd
- R5, R5a, R5ad, R5d, R5dn, R5n, R6, R6gd
- T3, T3a, T4g
- Z1d



Configure the Center

- Install Cisco Cyber Vision, on page 35
- Cisco Cyber Vision configuration, on page 38

Install Cisco Cyber Vision

Access the Cisco Cyber Vision installation wizard:

Procedure

| Step 1 | With you | r browser, access https:// <centername>/.</centername> |
|------------------|-----------------------|---|
| | Note | Accessing the Center using its name enables HTTPS secure interface. Yet, this requires a DNS or local host configuration to associate the name and the IP address. The Center access through its IP address is possible but the connection is not secure. |
| Step 2 Step 3 | The setuj Create a | o wizard used for the first access to Cisco Cyber Vision is displayed: n admin account: |

| EA Agree to the license terms | (V) Done |
|-------------------------------|---------------------|
| | |
| Lastname : | |
| | |
| Confirm password : | |
| | |
| | Confirm password *: |

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 | | |
| nd User License Agreement | | | | |
| ffective: May 22, 2017 | | | | |
| "Using" means to download, install | . activate. access or otherwise use the Software. | "Software" means the Cisco | | |
| Using" means to download, install computer programs and any Upgrades 'Documentation" is the Cisco user pplicable to the Software and mad ii) the Cisco authorized reseller Entitlement" means the license de PID) published on Cisco's price 1 pdates, upgrades, bug fixes, erro opies thereof. able of Contents | I, activate, access or otherwise use the Software. s made available to You by an Approved Source and I or technical manuals, training materials, specific de available to You by an Approved Source. "Approve ', distributor or systems integrator from whom you tail; including license metric, duration, and quan list, claim certificate or right to use notificatio or corrections, enhancements and other modification | "Software" means the Cisco Licensed to You by Cisco. sations or other documentation ad Source" means (1) Cisco or acquired the Software. tity provided in a product ID on. "Upgrades" means all is to the Software and backup | | |
| Using" means to download, install computer programs and any Upgrades Documentation" is the Cisco user upplicable to the Software and mac ii) the Cisco authorized reseller Entitlement" means the license de PID) published on Cisco's price 1 pdates, upgrades, bug fixes, erro opies thereof. Table of Contents . Acceptance of Terms | I, activate, access or otherwise use the Software. s made available to You by an Approved Source and J or technical manuals, training materials, specifi de available to You by an Approved Source. "Approve r, distributor or systems integrator from whom you etail; including license metric, duration, and quan list, claim certificate or right to use notificatio or corrections, enhancements and other modification | "Software" means the Cisco Licensed to You by Cisco. sations or other documentation ed Source" means (i) Cisco or acquired the Software. ntity provided in a product ID on. "Upgrades" means all as 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 47.

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 52.

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.

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 38 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 35.

Procedure

| Step 1 | Open your browser. |
|--------|---|
| Step 2 | Enter 'http:// <centeripaddress>/ca.crt' inside the search bar.</centeripaddress> |
| | The certificate is downloaded. |
| Step 3 | Save the certificate on your computer. |

Step 4In the browser, access the settings.Example: Chrome

| | - | - c | J × | |
|-----------------|-------------|------------|----------|---|
| | ☆ | \bigcirc | 0: | |
| New tab | | | Ctrl+T | |
| New window | | | Ctrl+N | |
| New incognito w | indow | Ctrl | +Shift+N | |
| History | | | | Þ |
| Downloads | | | Ctrl+J | |
| Bookmarks | | | | Þ |
| Zoom | - 100 | % + | 53 | |
| Print | | | Ctrl+P | |
| Cast | | | | |
| Find | | | Ctrl+F | |
| More tools | | | | Þ |
| Edit | Cut | Сору | Paste | |
| Settings | | | | |
| Help | | | | Þ |
| Exit | | | | |
| Managed by you | r organizat | ion | | |

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 | Ľ |
| Manage security keys Reset security keys and create PINs | ÷ |
| Site Settings Control what information websites can use and what content they can show you | ÷ |
| Clear browsing data Clear history, cookies, cache, and more | • |

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

| ersonal Other Peop | le Intermediate Certification | Authorities Tru | sted Root Certificati | on |
|-----------------------|---------------------------------|--|-----------------------|------|
| Issued To | Issued By | Expiratio | Friendly Name | |
| and the bran | 4 - Althurthand Ch. | 8,01,018 | Inclus (Million) | |
| "Address (she' | hu. Minore Cyberhult - | 1200200 | DepCart Ballenar - | |
| -Carbon CA | Carlum CA | 11,000,0017 | Certure | |
| gianten husted | re Cartus Trusted Nets. | 11112 | Carlus Trusted | |
| Theo Real (A.3 | PR Case Rest CA 3948 | 14000.000 | -marie - | |
| Caro Rost CA.R | Caro Real CA PD | 100.00 | -Charter - | |
| Class Read CA.W | Caro Real CA PO | 100.000 | -mare - | |
| Case Name Call | Case Nam CA Mg | 101110 | - There - | |
| - and one of | 10000 1000 1000 | and a strength of the strength | | |
| Import Exp | Remove | | Adv | ance |
| ertificate intended p | urposes | | | |
| erver Authentication | , Client Authentication, Secure | Email, Code Sign | ing, Time | |
| tamping, Encrypting | File System, IP security tunnel | termination, IP s | ecurity View | v |

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 S | tore | | | | |
|--------------------|-----------------------------|-------------------|------------------|-----------------|--------------------|
| Certifica | ite stores are s | ystem areas wh | ere certificate | es are kept. | |
| Window the cert | s can automatic ificate. | cally select a ce | rtificate store, | or you can spe | cify a location fo |
| | utomatically sel | ect the certifica | te store base | d on the type o | fcertificate |
| • P | ace all certificat | tes in the follow | ing store | | |
| c | ertificate store | : | | | |
| ſ | Trusted Root C | Certification Aut | horities | | 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 Certifi | cate Import Wizard |
| The certificate will be imported after | r you dick Finish. |
| You have specified the following set | ttings: |
| Certificate Store Selected by User | Trusted Root Certification Authorities |
| Content File Name | Certificate C:\Users\jmaffet\Downloads\ca.crt |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Finish Cancel |

What to do next

Install Cisco Cyber Vision, on page 35

Install Cisco Cyber Vision

Access the Cisco Cyber Vision installation wizard:

Procedure

| Step 1 | With your browser, access https:// <centername>/.</centername> | | | |
|------------------|--|---|--|--|
| | Note | Accessing the Center using its name enables HTTPS secure interface. Yet, this requires a DNS or local host configuration to associate the name and the IP address. The Center access through its IP address is possible but the connection is not secure. | | |
| Step 2 Step 3 | The setu Create a | p wizard used for the first access to Cisco Cyber Vision is displayed: an admin account: | | |

| O Constanting Constanting | | |
|---|--|----------|
| Create the first user | $\stackrel{\text{CR}}{=}$ Agree to the license terms | (V) Done |
| Firstname : | Lastname : | |
| Email : | | |
| Password : | Confirm password : | |
| Suggested password: \$kvIH2Qq*odz90fj0E3 | 0 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:

| | vilialia cisco Welcome to Cyber Vision | |
|--|---|--|
| | Please follow this few steps to be fully ready to use the product | |
| A Create the first user | Agree to the license terms | ⊘ Done |
| End User License Agreement | | |
| Effective: May 22, 2017 | | |
| This is an agreement between You an Software. "You" and "Your" means th "Using" means to download, install, computer programs and any Upgrades "Documentation" is the Cisco user o applicable to the Software and made (ii) the Cisco authorized reseller, "Entitlement" means the license det (PID) published on Cisco's price li updates, upgrades, bug fixes, error copies thereof. | d Cisco Systems, Inc. or its affiliates ("Cisco e individual or legal entity licensing the Soft activate, access or otherwise use the Software made available to You by an Approved Source and r technical manuals, training materials, specif e available to You by an Approved Source. "Appro distributor or systems integrator from whom yo all; including license metric, duration, and qu st, claim certificate or right to use notificati corrections, enhancements and other modificati | p") and governs your Use of Cisco cware under this EULA. "Use" or . "Software" means the Cisco d licensed to You by Cisco. ications or other documentation oved Source" means (i) Cisco or ou acquired the Software. unantity provided in a product ID tion. "Upgrades" means all tons to the Software and backup |
| Table of Contents | | |
| 1. Acceptance of Terms | | |
| | A copy of the license can be found at cisco.com | ⊘ Agree |

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 47.

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 52.

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

Configure the user interface security

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

Before you begin

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

Procedure

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



| 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, Alternative Name" must contain the Center DNS name. | a passw | word, and the field "X509v3 Subje | ect |
| | Procedure | | | |
| Step 1 | Select Upload a .p12. | | | |
| | Update with a new web server certificate: | | | |
| | ● Upload a .p12 ○ Generate a CSR (RSA 2048) | | | |
| | | Ø | | |
| | Please import a PKCS#12 file | | | |
| | <u>1</u> | | | |
| | Choose a file or drag and drop to upload | | | |

🔊 Save

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

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

| | Update with a new web server certificate: | | |
|--------|---|---|----------|
| | Upload a .p12 Generate a CSR (RSA 2048) | | |
| | | Ø | |
| | | | |
| | E | | |
| | File selected: CenterAD2019.2019lab.local1.pfx | | |
| | | | ි Save |
| Step 4 | Click Save. | | |
| | The following message appears: | | |
| | Certificate successfully updated. Please refresh your page | | C Reload |
| Ston 5 | Click Reload | | |

Step 5 Click Reload.

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

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

| ~ | centerad2019.2019lab.local/#/admin/center-certificate | | | | | | | |
|-----|---|----------|---|-----|--|--|--|--|
| cen | terad2019.2019lab.local | × | | | | | | |
| | Connection is secure | • | | | | | | |
| \$ | Cookies | 2 in use | ß | | | | | |
| \$ | Site settings | | Ľ | 1 | | | | |
| | _ | | | 1-1 | | | | |

What to do next

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 52.

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.

I

Generate a CSR

| Update with a new web server certificate: | | | |
|---|--------|--------------|----------|
| Upload a .p12 | | | |
| | | | |
| | | | |
| | | | |
| | | 🖸 Generate a | and down |
| | | I Generate a | and down |
| Enter the Center FQDN as registered on your DNS s | erver. | Generate a | and down |
| Enter the Center FQDN as registered on your DNS s Click the Generate and download CSR button. Update with a new web server certificate: | erver. | Generate a | and down |
| Enter the Center FQDN as registered on your DNS s Click the Generate and download CSR button. Update with a new web server certificate: Upload a.p12 • Generate a CSR (RSA 2048) | erver. | Generate a | and down |
| Enter the Center FQDN as registered on your DNS s Click the Generate and download CSR button. Update with a new web server certificate: Upload a.p12 | erver. | Generate a | and down |
| Enter the Center FQDN as registered on your DNS s Click the Generate and download CSR button. Update with a new web server certificate: Upload a.p12 | erver. | Generate a | and down |
| Enter the Center FQDN as registered on your DNS s Click the Generate and download CSR button. Update with a new web server certificate: Upload a.p12 | erver. | Generate a | and down |

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 | | |
| CSR: download 1 | | |
| Import a complete PEM bundle (concatenated CA, subCA, certificate) | | |
| L | | |
| Choose a file or drag and drop to upload | | |
| | 🖞 Discard | 🗟 Save |

A <FQDN>.csr file is downloaded.

- **Step 5** Use the <FQDN>.csr file to generate a pem certificate from your enterprise Certification Authority.
- **Step 6** Once the pem certificate is generated, return to Cisco Cyber Vision and click the Import a complete PEM bundle button (2) or drag and drop it to import it.

| Upload | d a .p12 Generate a CSR (RSA 2048) CSR has been generated. Please import the certificate. | |
|---------------|--|---------------|
| FQDN: CSR: | CenterAD2019.2019lab.local download | |
| | File selected: CenterAD2019.2019lab.local.crt | |
| | | Discard 🖸 Sav |



The following message appears:



Step 8 Click Reload.

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

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

2 in use [🛽

[2]

What to do next

Cookies

Site settings

ക

ń

If you are installing a Global Center or a synchronized Center, proceed with Configure Center data synchronization, on page 52.

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

Configure Center data synchronization

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

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



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

Procedure

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

I



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.

| .ılı.ılı. cısco | CYBER VISION Center | | |
|--------------------|---|--------------------|---|
| ۲ | Explore | System | Knowledge DB Current database information |
| | Reports | Data management | Current database version: 20201023 |
| Ē | Events | 🗋 Sensors 🗸 🗸 | • Lastimport: Tuesday, October 27, 2020 11:24 AM |
| ¢ | Monitor | 冬 Users 🗸 🗸 | IMPORT A KNOWLEDGE DB |
| Q | | ⊲ Events | The KDB is managed by the global center, you cannot update it from this center. |
| ۲ | | S API 🗸 | |
| | | 꾜 License | Certificate fingerprint |
| | | 糸 LDAP Settings | /0097ec32051coa03a3a70/70021170a0de3a3e74e50144/a20102c114c7025a |
| | | 🖗 PxGrid | |
| | SNORT Center unenrolled to Global Center. | | Enroll to a Global Center Center unenrolled to Global Center. |
| | | 📽 Integrations 🗸 🗸 | 💉 ENROLL |
| | | 器 Extensions | |

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.

| .iji.iji. cisco | CYBER VISION Global Center | | | | | | |
|--------------------|-------------------------------|-------------------|---|----|---------|------------|-------------------|
| Ø | | 团 System | System management From this page you can manage centers and sensors. | | | | |
| Ð | Reports | 🗏 Data management | | | | | |
| 8 | | 🛛 System manage 🔿 | | | | | |
| ٩ | | — Management | | | | | |
| ¢ | 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 * 1fc3fe05036f06028d1a0b3cde545b6bde5b18ccdc67c3bcd87 | ac5fac7513126 |
| Global Center IP address * | |
| 192.168.72.17 | |
| | |
| | Fince Cancel |

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



Deploy sensors

• Deploy sensors, on page 57

Deploy sensors

On standard conditions:

- No tunnels are configured.
- Both switches and sensors have internet access.

The deployment procedure is the same as described on the sensors installation guides. The only difference is that the Center's public IP address must be specified in the menu below:

| Manual sensor installation | | |
|--|---|-----------|
| The manual sensor installation is provided to install Cisco IOx Sensor, Cisco IC3000 Industrial Compute Gateway and sensors that a Center's DHCP server for automatic configuration. Please fill the fields below to configure your sensor and generate a provisioning ① This package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up or adde IOx Application. Select a hardware model: Cisco IOx Application | ire not allowed to a package. d in the right locatior | ccess the |
| Sensor configuration Serial number : Sensor's serial number as printed on the side panel FCW2445P6X5 | | |
| | Create Sensor | Cancel |



Configure the Cisco Cyber Vision Center synchronization

Global Center Configuration, on page 59

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 | 됀 System | System managem | REGISTER A CENTER X |
| Ð | Reports | 🗐 Data Management 🛛 💙 | From this page you can manage cer | N |
| Ħ | Events | System management | Register a Center | Name : My Center 01 |
| م | Search | — Management | | Fingerprint : 9e5b4c8c185457e446acb0946e114b3433ee8f40524d61 |
| © | | 첫 Users 🗸 | | OK Cancel |
| | | 🖾 Events | | OK Calicer |

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 | rom this page you can manage centers and sensors. | | | | | | | | | |
|------|---|----|---------|-------------------|----------------------------|-------------------------------|-----------------|--|--|--|
| Ð | Register a Center | | | Fingerprir | t: 72826cf919857c0b6b21ec9 | 4418d24f74d4d2cf2bc742e768444 | 1554078abaa0c 「 | | | |
| | 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 | Enrollment succeeded. | |
| | Connection test with global center 192.168.72.22 succeeded Calculated size of data to transfer: 78.6 kB Synchronization started | |
| r bi | Data is being synchronized with the global center. You can follow synchronization progress on Admin page. | |
| 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 this page you can manage centers and sensors. | | | | | | | | | | | |
|--|---|-------|----------|----------------------------|--------------------|------------------|-----------|----------------------------------|-------------------|---------------------|----------|
| ₽ R | Bingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c D | | | | | | | | | | |
| | Center Name | IP | | Version | | Enrollment state | ıs | Up | time | Connectivity Status | Action |
| • | My Center 01 | 192.1 | 68.72.21 | SBS: 4.1.0+2 KDB: 20220 | 02201171404 117 | 171404 Enrolled | | 5 days 16 hrs 52 mins 12 secs | | Connected | Unenroll |
| | Sensor Name | | IP | | Version | | Status | | Processing Status | Capture mode | Up Time |
| | Sensor My Sensor 1 | | 192.168 | .69.21 | 4.1.0+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 | From this page you can manage centers and sensors. | | | | | | | | | |
|--|--|---------------|--|-------------------|-------------------------------|---------------------|--------|--|--|--|
| B Register a Center Fingerprint: 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e76844455403 | | | | | 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 | | | | |

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 | rrom this page you can manage centers and sensors. | | | | | | | | | |
|------|--|----|---------|-------------------|-----------------------------|-------------------------------|--------------|--|--|--|
| Ð | Register a Center | | | Fingerpri | nt: 72826cf919857c0b6b21ec9 | 4418d24f74d4d2cf2bc742e768444 | 554078abaa0c | | | |
| | Center Name | IP | Version | Enrollment status | Uptime | 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 | From this page you can manage centers and sensors. | | | | | | | | | |
|----------------------------------|--|---------------|--|--|----------------------------------|---------------------|--------------------|--|--|--|
| B Register a Center Fingerprint: | | | | 72826cf919857c0b6b21ec94418d24f74d4d2cf2bc742e768444554078abaa0c | | | | | | |
| | Center Name | IP | Version | Enrollment status | Up time | Connectivity Status | Action | | | |
| + | My Center 01 | 192.168.72.21 | SBS: 4.1.0+202201171404 KDB: 20220117 | Enrolled | 5 days 18 hrs 41 mins 40 secs | Disconnected | Force unenrollment | | | |



Annex – Setup Center json file

• Annex – Setup Center json file, on page 65

Annex – Setup Center json file

• keys:

SSH public keys to add in the authorized keys.

• dns:

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

• dhcpd-enabled:

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

• single-interface:

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

• center-type:

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

• center-id:

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

• fqdn:

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

• ipset:

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

Examples:

- To deploy a standalone Center, leave the textbox empty.
- To deploy a Local Center, the minimal configuration is:
- {

"center-type": "Local Center",
}
• To deploy a Global Center, the minimal configuration is:

{

"center-type": "Global Center",

}