Cisco Cyber Vision for the Google Cloud Installation Guide, Release 5.5.x

Cisco Cyber Vision
Updated May 20, 2026

Topics included

1 Cyber Vision Deployment on Google Cloud

Topics:

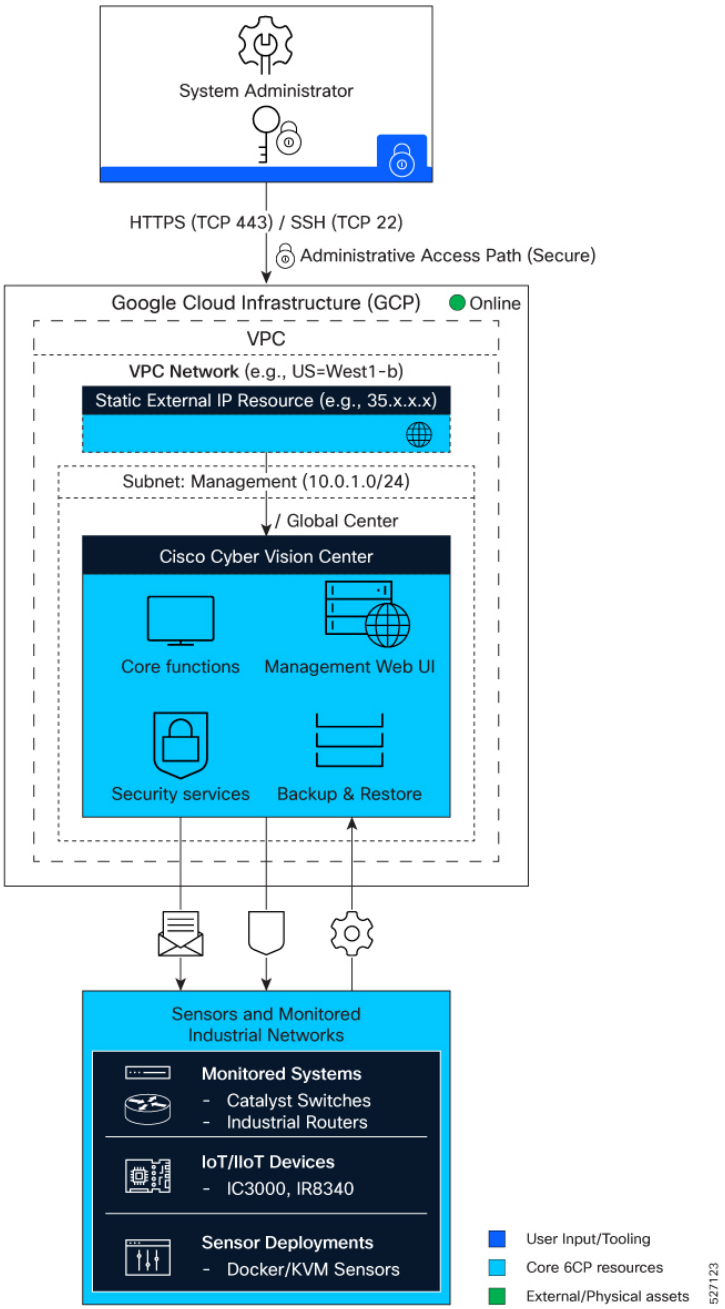
Explains how Cisco Cyber Vision deployments operate on Google Cloud

Cisco Cyber Vision deployments on Google Cloud

Explains how Cisco Cyber Vision deployments operate on Google Cloud and what features they enable for administration and network monitoring.

Cisco Cyber Vision is deployed as a VM on Google Compute Engine. Virtual Private Cloud (VPC) provides the networking resources required for connectivity, administrative access, and communication with other Cisco Cyber Vision components. Static external IP addressing can be used to provide stable remote access and to avoid connectivity changes after instance restart events.

Figure 1: Cisco Cyber Vision on Google Cloud



2 Plan your Cyber Vision deployment

Topics:

Provides guidelines for preparing the environment before deploying Cisco Cyber Vision on Google Cloud.

Prerequisites for deploying Cisco Cyber Vision on Google Cloud

Provides guidelines for preparing the environment before deploying Cisco Cyber Vision on Google Cloud, including account permissions, network configuration, and hardware requirements.

Ensure all prerequisites are met before deploying Cisco Cyber Vision on Google Cloud to avoid deployment failures and connectivity issues.

- Verify that you have a Google Cloud account with sufficient permissions to deploy Compute Engine resources.
- Have access to an SSH client for command-line access to the Cisco Cyber Vision Center.
- Configure static external IP addressing for Cisco Cyber Vision resources.
- Assign a persistent external IP address for the Center or Global Center instance. Ephemeral public IP addresses can change after a stop/start cycle, which can disrupt sensor communication.
- Use SSD persistent disks, as SSD storage is mandatory.
- For Site Manager deployments, provision the VM according to the sizing guidance in Google Cloud VM sizing guidelines on page 8. For Center and Global Center deployments, use the sizing guidance for your deployment profile.

Supported features on Google Cloud

Provides guidelines for identifying the supported deployment types for Cisco Cyber Vision on Google Cloud, enabling users to determine available options for their environment.

The following deployment types are supported on Google Cloud:

- Cisco Cyber Vision Center
- Cisco Cyber Vision Global Center
- Cisco Cyber Vision Site Manager (CVSM)

Google Cloud VM sizing guidelines

Provides guidelines for sizing VMs for Cisco Cyber Vision Site Manager deployments on Google Cloud, based on deployment scale. Helps ensure optimal performance and resource allocation.

Size the Google Cloud VM for Cisco Cyber Vision Site Manager (CVSM) deployments according to the expected number of components.

Proper VM sizing ensures that Cisco Cyber Vision Site Manager operates efficiently and reliably in Google Cloud environments, supporting the required number of components and features.

VM sizing recommendations

Use the following recommendations when planning the VM for your Site Manager deployment:

Note: These recommendations apply only to CVSM deployments. In particular, the 16 vCPU minimum is not a Center or Global Center requirement.

- **Minimum supported Site Manager deployment** (up to 500 components):
  - CPU: Intel Xeon, 16 vCPUs
  - RAM: 32 GB minimum
  - Storage: 256 GB SSD

- **Recommended Site Manager deployment** (up to 10,000 components):
  - CPU: Intel Xeon, 32 vCPUs
  - RAM: 128 GB minimum
  - Storage: 1 TB SSD minimum, RAID-10
- **Large-scale Site Manager deployment** (more than 10,000 components):
  - CPU: Intel Xeon, 64 vCPUs
  - RAM: 256 GB minimum
  - Storage: 1 TB SSD minimum, RAID-10

Additional reference information

For general Google Cloud onboarding information, see Get started with Google Cloud.

IPv6 support for Cyber Vision administration services

Lists the Cisco Cyber Vision administration services that support IPv6 and outlines current limitations.

You can use both IPv4 and IPv6 protocols for Cisco Cyber Vision administration services.

You can use IPv6 on Center `eth0` for administration-related access, including:

- Accessing Cisco Cyber Vision from a browser.
- Integrating with external services such as syslog and LDAP.

Consider these limitations:

- License operations work only with direct transport. Transport Gateway and HTTP/HTTPS Proxy are not supported.
- Sensor data collection uses only IPv4, whether performed on `eth0` or `eth1`.

Static external IP addresses in Google Cloud

Describes the functionality of static external IP addresses in Google Cloud and explains how they provide stable connectivity for Cisco Cyber Vision resources and connected systems.

A static external IP address is a fixed, user-reserved public IP address that does not change when a Compute Engine instance stops and starts.

- Remains constant across instance restarts, unlike ephemeral addresses.
- Prevents connectivity issues caused by changing IP addresses.
- Recommended for stable remote access to Cisco Cyber Vision resources and communication with sensors or other systems.

For Google Cloud procedures to reserve and assign a static external IP address, see Configure static external IP addresses.

3 Deploy the Cisco Cyber Vision Center

Topics:

Use this section to deploy Cisco Cyber Vision Center on a VM.

Create and configure a Cyber Vision VM instance

Configures a Cisco Cyber Vision Center instance on Google Cloud to meet deployment requirements and ensures all necessary resources and settings are reviewed before launch.

The Google Cloud Marketplace deployment form includes fields for machine sizing, storage, networking, and API access. Review these settings carefully, as some (like VPC selection) cannot be changed after the instance is created.

Before deploying the Cisco Cyber Vision Center, ensure the following prerequisites are met:

- Sign in to your Google Cloud account with valid credentials.
- Configure SSH keys at the project level. The new instance inherits these keys for CLI access.
- Prepare networking resources: a VPC network, subnet, and a reserved static external IP address.
- Ensure that the required Google Cloud APIs are enabled for Compute Engine and Marketplace deployment.
- Ensure that your account or service account has the IAM roles required to deploy VM instances, attach disks, and configure networking.
- Verify that the Cisco Cyber Vision Marketplace image that you plan to use is available in the selected project, billing account, and deployment region.
- Verify that the target VPC, subnet, and firewall policy allow administrative access and Cisco Cyber Vision traffic.

Procedure

1. Open the Google Cloud Marketplace Offer.
   a) Sign in to Google Cloud Marketplace and search for **Cisco Cyber Vision BYOL**.
   b) Open the offer and click **Launch** to open the deployment configuration form.
2. Create a new deployment.
   a) In the **Deployment name** field, enter a unique name for your instance.
   b) Select the service account to use for the deployment.
   c) Select the deployment zone.
3. Configure compute and storage settings.
   a) To configure machine series, in the **Series** field, select a supported machine series.

      N2 or **C3** series are recommended for production environments to ensure consistent performance.

   b) To select a machine type, in the **Machine type** field, select a configuration that matches the sizing guidance for your deployment profile.

      For Site Manager sizing requirements, see Google Cloud VM sizing guidelines on page 8. For Center and Global Center deployments, use the sizing guidance for your deployment profile.

   c) To configure a boot disk, in the **Boot Disk** section, select **SSD Persistent Disk**. Enter a disk size that matches your deployment requirements based on the Cisco Cyber Vision sizing guidance.

      Use the Cisco Cyber Vision sizing guidance when selecting disk capacity.

4. Configure the network interface.
   a) In the **Networking** section, expand **Network interfaces** and configure the required network settings.
      - Select the pre-configured VPC network and Subnet.
      - Under **External IPv4 address**, change the selection from **Ephemeral** to the **Static IP address** you reserved earlier.
      - If IPv6 is required, select a VPC and subnet configured for IPv6.

- Add additional network interfaces only if required by your specific network architecture.
- Create firewall rules that allow only the required Cisco Cyber Vision traffic.

For Cisco Cyber Vision traffic requirements, see Required ports and protocols on page 15. For Google Cloud procedures to create firewall rules, see Use VPC firewall rules.

5. In the **API Access** section, review the service account and access settings applied to the VM.
   - Use the configuration required by your organization security policy.
   - Prefer least-privilege access for Google Cloud resources.
   - If a custom service account is used, confirm that the required IAM roles are granted before deployment.
6. Review the deployment summary and click **Deploy**.

Results

The VM instance begins the provisioning process.

What to do next

When the status is **Running**, configure Center-specific parameters and confirm that the network is connected.

Configure the instance type for Global Center or Site Manager

Configure the Google Cloud VM metadata to start a newly deployed Cisco Cyber Vision Center as a Global Center or Cisco Cyber Vision Site Manager.

Configure a standard Cisco Cyber Vision Center instance to run as a Global Center or Cisco Cyber Vision Site Manager.

Google Cloud deploys a standard Center from the Marketplace image. To use the instance as a Global Center or Site Manager, configure the VM metadata and reset the application before continuing with feature-specific setup.

- Deploy the Cisco Cyber Vision VM instance from the Google Cloud Marketplace image.
- Ensure that you have permission to edit VM metadata in Google Cloud.
- Ensure that you can access the VM command line through SSH or the serial console.

Important: Use this procedure only on a newly deployed Center instance. The `sbs-erase` command resets the application configuration.

Procedure

1. Navigate to **Compute Engine > VM instances**.
2. Open the newly created Center instance.
3. Click **Edit**.
4. Add the metadata key `cyber-vision-config`.

   For a Global Center, use the following metadata value:

```
{
  "center-type": "Global Center"
}
```

For Site Manager, use the following metadata value:

```
{
  "center-type": "Site Manager"
}
```

5. Click **Save**.
6. Connect to the VM command line.
7. Run `sbs-erase`.

Results

The Cisco Cyber Vision application starts as the instance type defined in the metadata.

What to do next

After configuring the instance as a Global Center, continue with the Center synchronization chapter. For Site Manager, use the dedicated Cisco Cyber Vision Site Manager user guide.

Configure connectivity and security settings

Configure the required post-deployment settings to secure access to the Center instance and allow necessary network communications.

Set up the mandatory connectivity and security settings required after deployment.

- Enable serial console access if console-based administration is required.
- Enable HTTPS access.
- Configure firewall rules to allow the required ports and protocols.

After deploying the Center instance, you must complete essential configuration tasks to ensure secure administrative access and to allow the required network communications for Cisco Cyber Vision.

- Ensure you have administrative access to the Google Cloud console.
- Confirm that you have permission to modify VM instance settings and VPC firewall rules.

Procedure

1. Navigate to **Compute Engine > VM instances** .
2. Open the newly created Center instance.
3. Click **Edit** .
4. If console-based administration is required, enable **Enable connecting to serial ports** .
5. Enable **Allow HTTPS traffic** .
6. Click **Save** .
7. On the instance details page, in the network interface section, open `nic0`.
8. Update the VPC firewall rules to allow the required Cisco Cyber Vision traffic.

   For firewall planning, see Required ports and protocols on page 15.

Required ports and protocols

Describes the ports and protocols required for Cisco Cyber Vision components to communicate. Helps users configure network access to ensure proper operation and connectivity between sensors, Centers, and browser access.

Allow the following ports so Cisco Cyber Vision components can communicate correctly:

Configure Google Cloud VPC firewall rules to allow only the required traffic between Cisco Cyber Vision components and administrative clients.

Restrict source IP ranges wherever possible according to your deployment architecture and administrative access policy.

- AMQP over TCP port `5671` for communication between sensors and centers.
- SSH over TCP port `22` for CLI access.
- HTTPS over TCP port `443` for browser access to Cisco Cyber Vision.

Firewall planning guidelines

- Allow HTTPS from trusted administrative networks only.
- Allow SSH only when CLI access is required and restrict it to authorized administrative sources.
- Allow AMQP only between Centers, Global Centers, and sensors that must exchange data.

Incoming communications for Global Center

Table 1: Global Center Incoming Communications

Protocol	Port	Purpose
AMQP	TCP 5671	Communications incoming from connected Centers
SSH	TCP 22	CLI access
HTTPS	TCP 443	Browser access to Cisco Cyber Vision

Incoming communications for Center

Table 2: Center Incoming Communications

Protocol	Port	Purpose
AMQP	TCP 5671	Communications incoming from connected sensors or Centers
SSH	TCP 22	CLI access
HTTPS	TCP 443	Browser access to Cisco Cyber Vision

4 Connect to the Cisco Cyber Vision Center

Topics:

Describes how you can access the Cisco Cyber Vision Center using different interfaces for installation, administration, troubleshooting, or recovery.

Access the Cisco Cyber Vision Center

Describes how users can access the Cisco Cyber Vision Center using different interfaces for installation, administration, troubleshooting, or recovery.

The Cisco Cyber Vision Center can be accessed through multiple interfaces, each suited for specific tasks.

- Use Cisco Cyber Vision for installation and routine administration tasks.
- The Google Cloud serial console is used when direct console access is required for troubleshooting or recovery.

Access the Cisco Cyber Vision Center from a browser

Access the Center through a web browser to perform installation, setup, and routine administration.

Access the Cisco Cyber Vision Center from a browser for installation, configuration, and administration tasks.

Use this procedure when the Center instance is running and HTTPS access is enabled.

- Ensure that HTTPS access is enabled for the instance.
- Identify the external IP address or DNS name of the Center instance.

Procedure

1. Navigate to **Compute Engine > VM instances**.
2. Open the newly created Center instance.
3. In the network interfaces section, locate the external IP address for `nic0` .
4. Download the certificate authority certificate by using one of the following example URLs:

   Replace the placeholder value with the public IPv4 address or public DNS name of your Center.

   - `https://<public-ipv4-address>/ca/crt`
   - `https://<public-dns-name>/ca/crt`

5. Open Cisco Cyber Vision by using the following example URL:

   Replace `<center-address>` with the public IPv4 address or public DNS name of your Center.

   - `https://<center-address>/`

Results

You can then proceed with Cisco Cyber Vision installation and application setup.

Access the CV Center using the console

Accesses the Center directly through the Google Cloud serial console when browser-based access is unavailable or for low-level troubleshooting. Uses the default console credentials for the new instance to enable direct administration or recovery.

Access the Cisco Cyber Vision Center through the Google Cloud serial console for direct console administration or troubleshooting.

Use the serial console when direct access to the instance is required, especially for troubleshooting or recovery tasks.

- Ensure that the Center instance is running.
- Ensure that serial console access is enabled for the instance.

- Identify the instance ID, which is used as the default password for the new Center.

You can connect to the Center by using the Google Cloud serial console.

Procedure

1. Navigate to **Compute Engine > VM instances**.
2. Open the newly created Center instance.
3. Click **Connect to serial console**.
4. Log in with the default user `cv-admin`.
5. Use the instance ID as the default password for the new Center.

Results

You access the Cisco Cyber Vision Center directly through the serial console, enabling administrative actions or troubleshooting.

5 Configure the Cyber Vision Center

Topics:

Describes how to perform the initial setup of Cisco Cyber Vision Centers after deployment.

Configuring Cisco Cyber Vision Centers

Describes how to perform the initial setup of Cisco Cyber Vision Centers after deployment.

The initial setup process for Cisco Cyber Vision Centers ensures that the Center is installed and prepared for further configuration and integration into the network.

The process includes installation, certificate model selection, and a decision to synchronize the Center or deploy sensors based on the deployment plan.

These stages describe the initial setup of Cisco Cyber Vision Centers.

1. The administrator installs Cisco Cyber Vision on the deployed Center.
2. The administrator selects the certificate model for browser access to the Center.
3. The administrator proceeds to either synchronize the Center or deploy sensors, according to the deployment plan.

The Center is configured and ready for synchronization or sensor deployment. It can now support Cisco Cyber Vision operations within the network architecture.

Install Cisco Cyber Vision

Installs Cisco Cyber Vision by guiding the user through the first-access wizard and initial configuration steps.

- The Center VM is deployed and running
- HTTPS access to the instance is enabled
- You know the DNS name or IP address of the Center
- If you plan to use the DNS name for browser access, DNS resolution for that name is already in place.

Procedure

1. In a web browser, open `https://<CENTERNAME>/`.

   If the DNS name is not yet available, you can access the Center by IP address for the initial setup. In that case, the browser displays a certificate warning until the certificate trust path is configured.
2. Verify that the Cisco Cyber Vision first-access wizard is displayed.
3. Create an administrator account.
   a) In the administrator account section, create the first local administrator account.
   b) Enter the required account information, including username, email address, and password.
4. Accept the software license agreement and finish the installation.
5. Finish the installation.

Results

The Center is now installed and ready for use.

What to do next

Click **Start to Explore** to open the Cisco Cyber Vision interface.

Note: To reset local users later from the Center CLI, use `sbs-db reset-users`.

Choose the Center certificate method

Choose whether to use the default self-signed certificate or an enterprise certificate for secure browser access to the Center.

Choose the certificate method for the Center to enable secure browser access and proper authentication.

After the first-access wizard is complete, choose how the browser will trust the Center certificate.

- Complete the Center installation and note the URL provided in the setup wizard.
- Verify browser compatibility (Chrome 54, Firefox 49, or later).

Procedure

1. Decide which certificate method to use for the Center.
   - **Default self-signed certificate**:
     - Install the certificate in your browser before accessing the Center for normal operations.
     - Follow your browser's instructions to import the certificate.
   - **Enterprise certificate**:
     - Complete the initial Center installation.
     - Configure the Center certificate by uploading a `.p12` bundle or generating a certificate signing request (CSR) as required by your organization's certificate authority.
2. After configuring the certificate method, access the Center using your compatible browser.

Results

Secure browser access to the Center is enabled by either importing the self-signed certificate into the browser trust store or configuring an enterprise certificate on the Center.

Install the certificate in your browser on macOS

Installs a Cisco Cyber Vision self-signed certificate in the browser to establish trust for secure connections.

- Download the Cisco Cyber Vision certificate authority certificate from one of the following example URLs. Replace the placeholder value with the public IPv4 address or public DNS name of your Center.
  - `https://<public-ipv4-address>/ca/crt`
  - `https://<public-dns-name>/ca/crt`
- These instructions are specific to macOS using Keychain Access. For other platforms, use the appropriate operating system or browser certificate management documentation.

Procedure

1. In your browser, open the certificate management settings.
2. Open the certificate management page so that **macOS Keychain Access** opens.
3. In **Keychain Access**, select the **System** keychain.
4. From the menu bar, choose **File > Import Items**, and select the Cisco Cyber Vision certificate file that you downloaded earlier and import it into the **System** keychain.

5. In **Keychain Access**, open the imported certificate, expand **Trust**, and configure the trust settings required by your organization.
6. Finish the import.

Results

The browser now trusts the Cisco Cyber Vision certificate.

What to do next

Return to Cisco Cyber Vision and continue with Center configuration.

Replace the Center web certificate

Replace the default Center certificate with an enterprise certificate to secure browser access and meet organizational certificate requirements.

Perform this task if you need to replace the default certificate with one issued by your organization's certification authority.

Install an enterprise certificate to secure browser access to the Center.

Cisco Cyber Vision must already be installed, and you must have access to **Admin > Center certificate**.

Procedure

1. In Cisco Cyber Vision, navigate to **Admin > Center certificate**.
2. Choose one of the following certificate methods:
   - **Upload a .p12**
   - **Generate a CSR**

Results

If you already have a certificate bundle issued by your certification authority, proceed to Upload a .p12 certificate on page 24. If you need Cisco Cyber Vision to generate a certificate signing request, proceed to Generate a CSR and import the signed certificate on page 25.

Upload a .p12 certificate

Uploads a PKCS#12 certificate bundle to Cisco Cyber Vision for Center authentication. Ensures secure connectivity by replacing the default certificate with one issued by your certification authority.

Uploads a `.p12` or `.pfx` certificate bundle issued by your certification authority to Cisco Cyber Vision.

Make sure that:

- You can access **Admin > Center certificate**.
- The **.p12** or **.pfx** file contains the private key that matches the certificate.
- You know the password for the certificate bundle
- The certificate includes the DNS name that users enter in the browser in the **X509v3 Subject Alternative Name** field.

Procedure

1. In Cisco Cyber Vision, navigate to **Admin > Center certificate**.
2. Select **Upload a .p12**.

3. Click **Import a PKCS#12 file**, or drag and drop the certificate file into the import area.
4. Select the **.p12** or **.pfx** file generated by your certification authority.
5. Enter the certificate password.
6. Click **Save**.
7. When prompted, click **Reload**.
8. In your browser, reconnect to the Center by using its DNS name.

   The browser warning no longer appears, and the connection is secure.

Results

The Center uses the uploaded certificate for secure connections, and browser warnings are resolved.

What to do next

- If you are installing a Global Center or a synchronized Center, proceed to Center synchronization.
- If you are installing a standalone Center, proceed to sensor deployment.

Generate a CSR and import the signed certificate

Generates a certificate signing request (CSR) and imports the signed certificate into Cisco Cyber Vision. This process ensures secure communication by validating the Center's identity with a certification authority.

Verify the following prerequisites before generating a CSR and importing the signed certificate:

- Cisco Cyber Vision is already installed.
- You can access **Admin > Center certificate**.
- The Center FQDN is defined and registered in DNS. This FQDN must match the DNS name that users enter in the browser.
- Your certification authority can issue a certificate for that FQDN.

Procedure

1. In Cisco Cyber Vision, navigate to **Admin > Center certificate**.
2. Select **Generate a CSR**.
3. Enter the Center FQDN as registered in your DNS server.
4. Click **Generate and download CSR**.

   A message confirms that the CSR has been generated.

5. Download the generated CSR file and submit `FQDN.csr` to your certification authority to request a signed PEM certificate.
6. After the signed certificate is issued, return to Cisco Cyber Vision and import the complete PEM bundle.
7. Click **Save**.
8. When prompted, click **Reload**.
9. In your browser, reconnect to the Center by using its DNS name.

Results

The browser warning no longer appears, and the connection is secure.

What to do next

- If you are installing a Global Center or a synchronized Center, proceed to Center synchronization.

- If you are installing a standalone Center, proceed to sensor deployment.

Sensor deployment options

Describes the available deployment platforms for Cisco Cyber Vision sensors based on network architecture and hardware models.

Use the sensor installation guide that matches the platform where you plan to deploy Cisco Cyber Vision sensors.

The following deployment options are available for Cisco Cyber Vision sensors:

- For supported switches and routers, use the Cisco Cyber Vision Sensor installation guide for switches and routers.
- For Cisco IC3000 platforms, use the Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000.
- For Cisco IR8340 platforms, use the Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340.
- For Cisco IR1101 and IR1800 platforms, use the Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101 and IR1800.
- For supported Cisco switches that use the sensor application, use the Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide.

6 Configure Center synchronization with Global Center

Topics:

Describes the process for synchronizing a Center with a Global Center so that data from multiple Centers can be viewed in a single application.

Synchronizing Global Centers

Describes the process for synchronizing a Center with a Global Center so that data from multiple Centers can be viewed in a single application.

Use this process to synchronize a Center with a Global Center so that data from multiple Centers can be viewed in a single application.

This process includes registering the Center, enrolling it with the Global Center, completing the initial synchronization, and monitoring synchronization status.

These stages describe the synchronization process.

1. Register the Center in the Global Center.
2. Enroll the Center with the Global Center.
3. Allow the initial synchronization to complete.
4. Monitor the synchronization status in the Global Center.
5. Unenroll the Center when synchronization is no longer required.

After enrollment succeeds, the Global Center displays synchronized data and status information for the enrolled Center.

Synchronize a Center with a Global Center

Register a Center with a Global Center and enroll the Center so that synchronization can begin.

Use this procedure to establish synchronization between a Global Center and a Center.

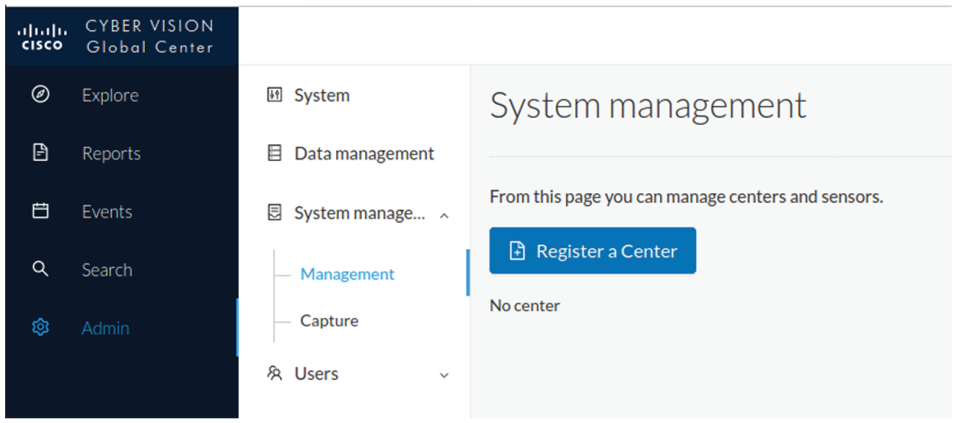
This procedure applies to a Global Center and the Centers that synchronize with it.

To complete this procedure, open the user interface of both the Global Center and the Center.

- Ensure that the Global Center is installed and accessible.
- Ensure that the Center is installed and accessible.
- Ensure that the required network connectivity between the Center and the Global Center is in place.
- Ensure that certificate fingerprints can be retrieved from both systems.

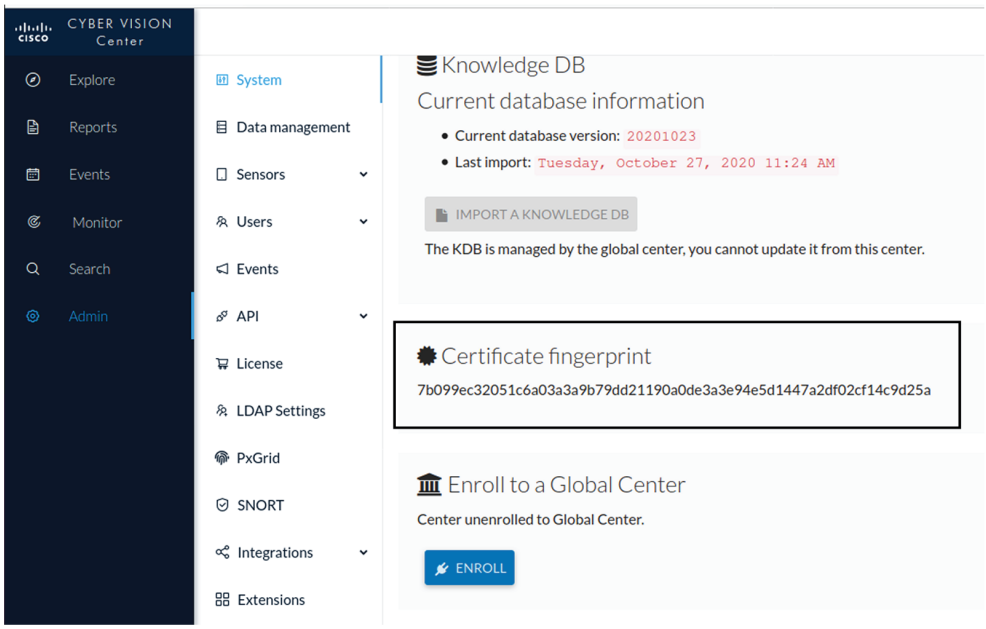
Procedure

1. In the Global Center, navigate to **Admin > System Management > Management**.
2. Click the **Register a Center** button.

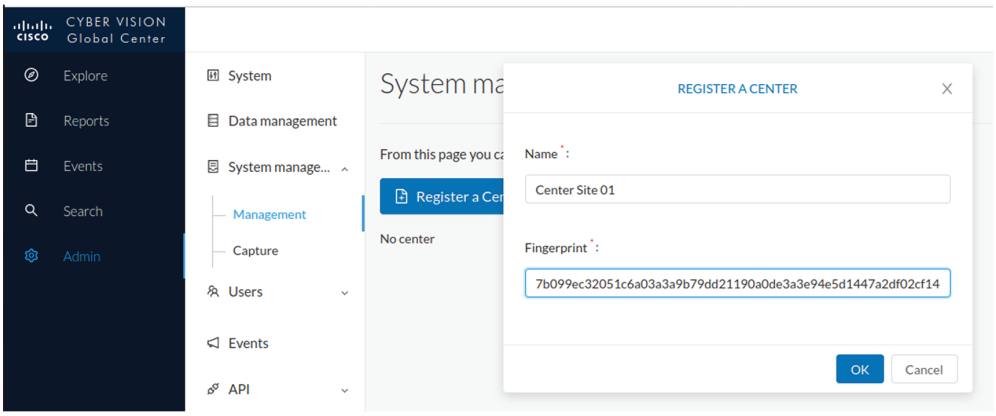


The Register a Center window opens. Leave it open while you retrieve the Center fingerprint.

3. In the Center, navigate to **Admin > System**.
4. Scroll down to Certificate fingerprint and copy it.

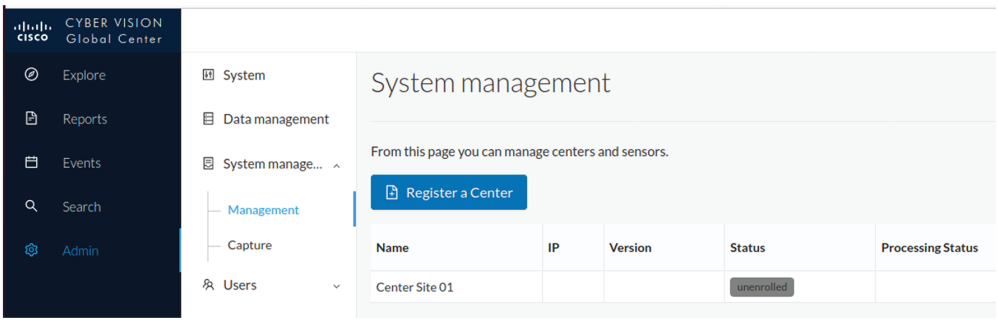


5. In the Global Center, enter a name for the Center and paste the Center fingerprint into the corresponding field.



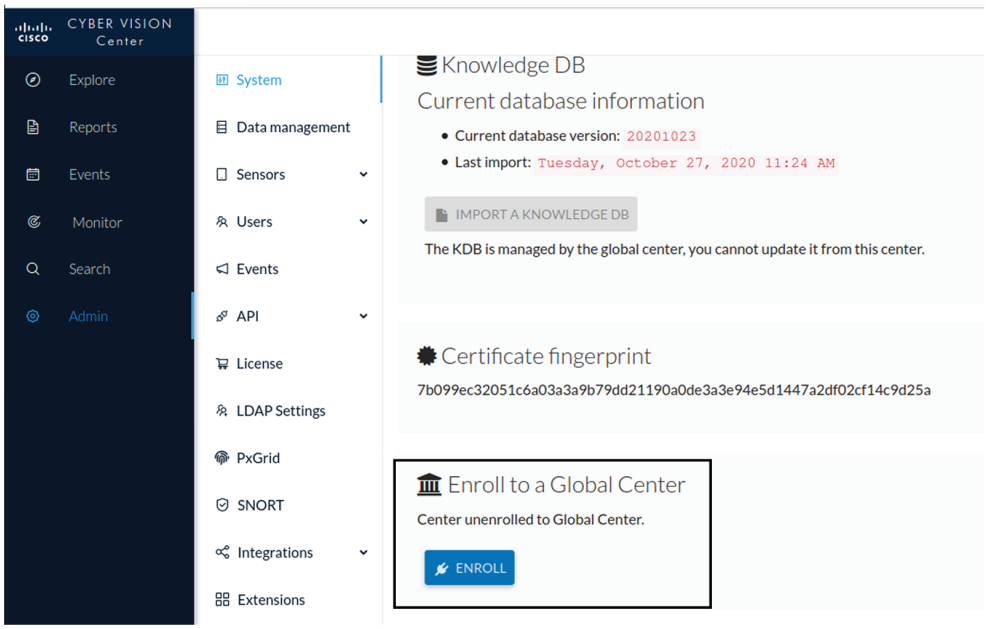
6. Click **OK**.

The Center appears in the list as unenrolled.

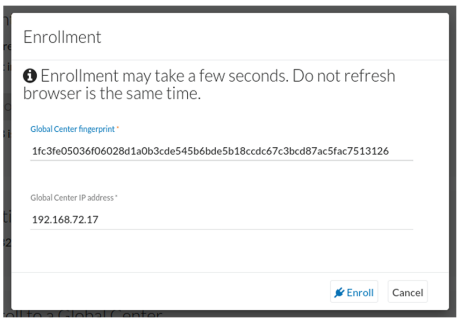


Switch to the Center and enroll it with the Global Center.

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



8. In the Global Center, copy the Global Center fingerprint from the System administration page.
9. Enter the Global Center fingerprint and IP address, and click **Enroll**.



The Center is shown as enrolled with the Global Center after synchronization is complete.

Results

The Center is enrolled with the Global Center, synchronization begins, and the Center status changes to connected in the Global Center.

What to do next

If additional Centers must be synchronized, repeat this procedure for each one.

Unenroll the Center

Unenroll a Center from a Global Center when the Center is being replaced, moved, or removed from synchronization.

Use this procedure to remove a synchronized Center from a Global Center.

Use this procedure when a Center must be removed from synchronization, for example during maintenance or replacement of the Center or the Global Center.

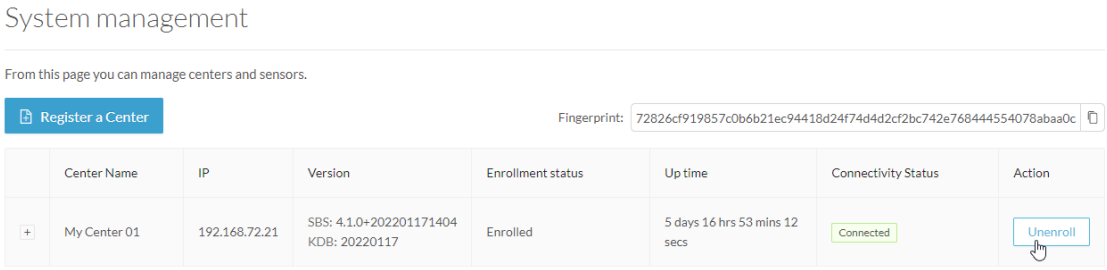
You can unenroll a Center when you need to replace, move, or remove it from a Global Center. Unenrollment deletes the Center data from the Global Center.

Procedure

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

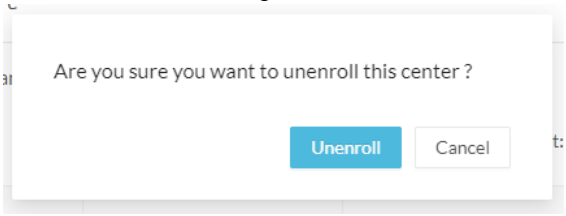
   All Centers associated with the Global Center are listed.

2. Click **Unenroll** for the required Center.



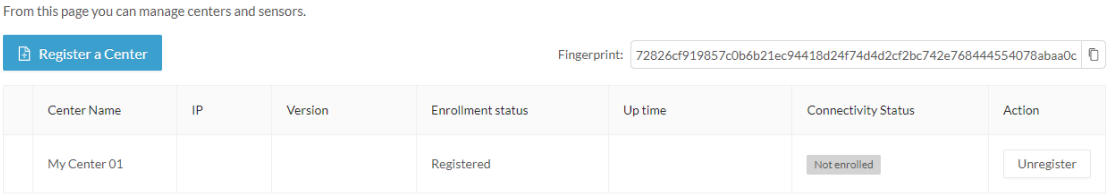
   If you are replacing a Global Center, unenroll all its synchronized Centers.

3. In the confirmation dialog box, click **Unenroll** to start the process.



   All Center data is deleted from the Global Center. The Center is ready to be enrolled again in the same Global Center or in another Global Center.

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



Results

The Center is unenrolled from the Global Center and can be enrolled again in the same Global Center or in another Global Center later.

What to do next

If you are replacing a Global Center, repeat this procedure for each synchronized Center before decommissioning the original Global Center.

Force unenrollment of a Center

When a synchronized Center has been disconnected for a long time, for example because of a hardware failure, you can force its unenrollment from the Global Center. This deletes all data for that Center from the Global Center and allows the Center to be replaced.

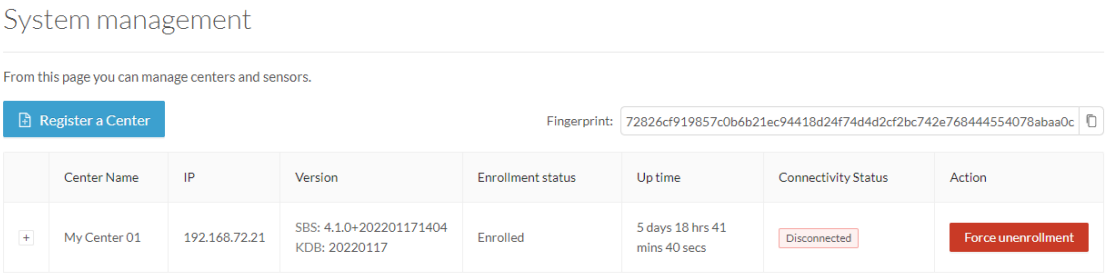
Important: Make sure that the disconnected Center is permanently unavailable before performing this action. Because all data for the Center is deleted from the Global Center, a Center that later attempts to send data again can cause significant data synchronization issues.

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

   All Centers associated with the Global Center are listed.

2. For the disconnected Center, click **Force unenrollment** in the **Action** column.

All data for that Center is deleted from the Global Center, and the Center is removed from the list.



7 Center Backup and Restore

Topics:

Describes how Cisco Cyber Vision Center backup and restore operations support migration, replacement, and recovery workflows.

The Cisco Cyber Vision Center command-line interface (CLI) provides commands to back up and restore a Center. Use these commands to migrate a Center from one appliance or VM to another, such as from a cloud VM to a UCS appliance.

The backup archive includes the following information:

- Operating system settings, such as IP addresses, names, and certificates.
- Cisco Cyber Vision settings.
- Cisco Cyber Vision data.

After the restore is complete, the restored Center uses the network identity and data from the backed-up Center.

Backup and restore requirements and limitations

Lists the requirements and limitations that apply before restoring a Cisco Cyber Vision Center backup archive.

Before restoring a backup archive, make sure that the target Center meets the following requirements:

- The target appliance or VM has the same number of network interfaces as the backed-up Center.
- The target Center has the required base network configuration before the archive is transferred. At minimum, configure the `eth0` IP address.
- The target Center interface mode, such as single-interface or dual-interface mode, matches the backed-up Center.

Observe the following limitations when restoring a backup archive:

- If the restored Center reuses the network identity of the original Center, power off the original appliance before bringing the restored Center online.
- The Cisco Cyber Vision license is not included in the backup archive. Return the license from the original Center to the Smart Account server if required, and install a license on the restored Center.
- Report extension packages are not restored automatically. Install the report extension on the restored Center if your deployment requires it.

Back up the Cisco Cyber Vision Center

Create a backup archive of a Cisco Cyber Vision Center so that its configuration and data can be restored later during migration, replacement, or recovery operations.

Use this procedure to create a backup archive of the Cisco Cyber Vision Center before migration, appliance replacement, or recovery operations.

Use this procedure to create a backup archive from an existing Cisco Cyber Vision Center. The backup is generated locally on the Center and can then be copied to another appliance for restore or to another storage location for safekeeping.

- Ensure that the Cisco Cyber Vision Center is running and accessible.
- Ensure that you have CLI access to the Center through SSH or console access.
- Verify that sufficient free space is available on the Center to generate the backup archive.
- If you plan to copy the backup file off the Center, ensure that a secure transfer method and target location are available.

Procedure

1. Connect to the Center through SSH.
2. Run the following command:

   ```
   sbs-backup export
   ```

   A backup file is generated in the `/data/tmp/ccv-center-backup/` directory.

   In the following example, the generated file is named `ccv-center-backup-Center224433labautomccvlocal-5.4.0-20240405112443.tar.gz`.

3. Copy the backup file to the target appliance or to a secure storage location for restore.

Results

A backup archive of the Cisco Cyber Vision Center is available in `/data/tmp/ccv-center-backup/` and is ready to be transferred or used during a restore procedure.

What to do next

Use the backup archive during the restore procedure or transfer it to a secure storage location for retention according to your operational policy.

Restore the Cisco Cyber Vision Center

Restore a previously exported Cisco Cyber Vision Center backup archive to a prepared Center during migration, replacement, or recovery operations.

Use this procedure to restore Cisco Cyber Vision Center configuration and data from an existing backup archive.

Before you start the restore procedure, copy the Center backup archive to the new Center in the `/data/tmp/` directory.

- Ensure that the backup archive is already copied to the `/data/tmp/` directory on the target Center.
- Ensure that you have CLI access to the Center through SSH or console access.
- If the restored Center will reuse the previous Center network identity, ensure that the old appliance is powered off.

Procedure

1. Connect to the Center through SSH.
2. Run the following command:

```
sudo -i sbs-backup import <path to the center backup>
```

3. Type `reboot` to restart the Center.
4. Install the report management extension if your deployment requires it.
5. Install a license on the restored Center.

Results

The Cisco Cyber Vision Center is restored from the backup archive and is ready for any required post-restore tasks, such as report extension installation and licensing.

Automate Cisco Cyber Vision Center backups

Automates the export and transfer of Cisco Cyber Vision Center backup files using file-transfer tools. This procedure enables the synchronization of backup data with remote storage systems.

You can use file-transfer tools to automate Cisco Cyber Vision Center backup export and transfer.

`rclone` is a command-line program for managing files across local and remote storage systems. You can use it to move or synchronize Center backup files with a remote location.

Procedure

1. Configure `rclone` for the remote storage system.

```
sudo -i
                          rclone config
```

For configuration options, see rclone documentation .

2. Use the `rclone` command to move the backup directory to the remote location.

   Syntax:

   ```
   rclone [options] subcommand <parameters> <parameters...>
   ```

   For example:

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

   In this example, `rclone` moves the backup files stored in `/data/tmp/ccv-center-backup/` to the remote location `lab_sftp:/srv/pub/` .

Automate backup export and transfer with a Bash script

Provides a Bash script to automate the generation of backup archives and their subsequent transfer to remote storage locations. This approach streamlines data management tasks by executing necessary commands in a single sequence.

This reference provides a Bash script example to automate the generation of a backup archive and its transfer to a remote location.

The script performs the following operations:

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

```
#!/bin/bash
                sbs-backup export
                rclone move /data/tmp/ccv-center-backup/ lab_sftp:/srv/pub/
```

Schedule the backup script with cron

Schedules a Bash script with cron to back up Cisco Cyber Vision data and transfer the backup file to a remote location.

You can schedule a Bash script with `cron` to back up Cisco Cyber Vision data and send the backup file to a remote location.

Procedure

1. Edit the crontab file:

   ```
   crontab -e
   ```

2. Add the cron entry.

   The following example runs `/data/tmp/backup.sh` every Saturday at 1:00 a.m.:

   ```
   00 01 * * 6 bash /data/tmp/backup.sh
   ```