Revised: May 22, 2026

Managing Cyber Vision Centers

Manage Cyber Vision Local Centers with Site Manager

From Cisco Cyber Vision Release 5.5.0, you can manage your Local Centers using the Global Center or the Site Manager. The Site Manager:

- Provides a single pane view of all your connected Centers and Sensors.
- Offers automatic knowledge database (KDB) version updates on connected Centers, and automatic self-updates.
- Displays a map showing the geolocation of all your connected Centers.

You can connect a Local Center to either a Global Manager or Site Manager. You cannot connect a Local Center to both management systems simultaneously.

Site Manager and Global Centers

Site Manager is the counterpart to Global Manager and provides a cloud connection. With this connection, you can:

- Visualize the geolocations of all your connected Centers.
- Automate knowledge database (KDB) version updates on all your connected Centers.
- Automate Site Manager software updates.

Table 1: Comparison Table Title

Feature	Global Center	Site Manager
Local Center management		
Center status and version	Yes	Yes
Knowledge Database (KDB) version	Partially automated. You update the KDB version in the Global Center, and then push the update to all the connected Local Centers.	Fully automated. If you connect your Site Manager to your Cisco Account, you can automate the KDB version update on all your connected Local Centers. The update is triggered as soon as a new KDB version is detected by the Site Manager.
Licensing compliance	No	Yes
Services status	No	Yes
Sensor management extension availability and version	No	Yes
Reports management extension availability and version	No	Yes
Assets count across centers	Yes	No

Feature	Global Center	Site Manager
Network data such as devices, activities, events, components, and vulnerabilities	Yes	No
User groups and presets	Yes	No
Sensor management		
Sensor connection status and version	Yes	Yes
Cloud-enabled management		
Automatic software updates	No	Yes
Cloud connection for center geolocation updates	No	Yes

Advantages of Site Manager

Unlike the traditional Global Center, which relies on manual intervention for certain administrative tasks, Site Manager leverages cloud connectivity to provide automated management, improved health monitoring, and streamlined compliance.

- Automated updates: Site Manager facilitates automatic KDB version updates on connected Centers, as well as Site Manager software updates.
- Enhanced health monitoring: Site Manager provides native support for monitoring Local Center health, including ingestion services and stopped services.
- Centralized compliance and management: Site Manager allows you to monitor licensing compliance, and the software versions related to the Centers and sensors.
- Cloud integration: Site Manager uses cloud connectivity for automatic software updates, and for geolocation information.

Installing Site Manager

To install a Site Manager, download the Cyber Vision Center package for the platform you want to deploy the manager on.

If you deploy Site Manager as a virtual machine, allocate a minimum of 250 GB of hard drive space. The virtual machine requirements for Site Manager differ from the requirements for a Cyber Vision Center.

For guidance on the installation process, see the documentation for setting up a Cyber Vision Center on the desired platform. The installation process differs only at two steps:

1. When prompted to choose a Center type, choose **Site Manager**.
2. After the set up is complete, you are prompted to log in to the Site Manager GUI using the configured web address.

On the initial user creation screen, sign in with a Cisco Account to create the first user for the Site Manager instance. A Cisco Account is the Cisco identity that you use to access Cisco services. If the credentials that you enter are not associated with a Cisco Account, a new Cisco Account is automatically created for you at this login.

Manage user access

Site Manager employs the role-based access control (RBAC) model to define what actions a user can perform. The Site Manager only has the Admin role, which provides comprehensive authority over the platform.

The Admin role is designed for users who require full access to configure, manage, and oversee the entire system. Key permissions include:

- Center Management: View and manage all enrolled centers.
- System: Configure system-wide preferences and manage external connections.
- User Management: Create, view, and manage user accounts, roles, and access levels.
- Dashboard: Access detailed views of enrolled centers and manage scheduled system upgrades.

Add Site Manager administrators

Step 1 In the Site Manager, go to **Configuration** > **User Management**.

Step 2 Click **Add New User**.

Step 3 Enter first name, last name, email ID, and password for the user you want to add.

Step 4 Click **Save** to create the user account.

Enrolling Local Centers to Site Manager

Summary

To manage Local Centers using a Site Manager, you must complete a two-step process for each Local Center.

The key participants in the enrollment process are:

- Site Manager:
- Local Center

Workflow

These are the stages of connecting a Local Center to a Site Manager:

1. Add a Local Center to Site Manager, on page 4

   In the Site Manager, enter the details of the Local Center you want to connect. The Local Center's fingerprint acts as the identifier in this process.

   At the end of this stage, a Local Center is added to the Site Manager with its enrollment status as **Pending Enrollment** and its connection status as **Not Enrolled**.

2. Add Site Manager to Local Center, on page 4

   Then, in the Local Center, add the Site Manager using the Site Manager's fingerprint.

   At the end of this stage, the connection status of the Local Center is updated to **Connected** in the Site Manager.

If the connection between the Site Manager and a Center is interrupted for a prolonged duration, the connection status is updated to **Unreachable**.

Add a Local Center to Site Manager

Before you begin

Get the fingerprint of the Local Center you want to connect. In the Local Center Classic UI, the fingerprint is displayed in the **Center Fingerprint** area of the **Admin** > **System** page.

Step 1 Log in to the Site Manager.

Step 2 Go to **Configuration** > **Center Management**.

Step 3 Click **Add Center**.

Step 4 In the **Add Center** area,

a) Enter the fingerprint of the Local Center you want to add.

b) Enter the location of the Center by choosing a specific point on the map, or using the search field to choose a city.

Step 5 Click **Add**.

The Local Center is listed on the **Center Management** page, with its enrollment status as **Pending Enrollment** and its connection status as **Not Enrolled**.

To edit the location of a Center, click **Edit location** from the **Actions** list for the Center.

Add Site Manager to Local Center

Before you begin

Get the fingerprint of the Site Manager. The fingerprint is displayed in the **Configuration** > **Center Management** page.

Step 1 Log in to the Local Center Classic UI.

Step 2 Go to **Admin** > **System**.

Step 3 Click **Enroll** in the **Enroll to Site Manager or Global Center** area.

Step 4 Enter the fingerprint and IP address of the Site Manager.

Step 5 Click **Enroll**.

- In the Local Center, the **Enroll to Site Manager or Global Center** section shows that the Center is now enrolled with a Site Manager.
- In the Site Manager, the connection status of the Local Center is updated to **Connected**.

Monitor connected Local Centers

Site Manager allows you to monitor connectivity, software versions, licensing compliance, and the overall health of various Centers. Site Manager refreshes data for each connected Center approximately every hour. Because each Center syncs independently, the refresh time can be different for each Center and depends on that Center's last successful data synchronization.

The dashboard displays only enrolled Centers and opens in map view by default, allowing you to see where your connected Centers are deployed across the world. The top of the dashboard provides an overview of these data points:

- Total: The total number of enrolled Centers.

- Unreachable: The number of Centers currently not communicating with the management system.
- Out of date: The number of Centers running software versions that require an update.
- Non-compliant licensing: The number of Centers with active licensing issues.
- Unhealthy: The number of Centers experiencing system process or data flow issues.

To see specific details for connected Centers, click **Table** on the dashboard. These details are displayed for each connected Center.

Table 2: Center information displayed in Site Manager dashboard

Column name	**What the values mean**
Center	The unique identifier or name of the Center.
IP address	The network IP address assigned to the Center.
Connection	The status of the network link between the Center and the Site Manager.
Version	The current software version installed on the Center. Orange statuses indicate that newer versions are available for upgrade. A gray status can appear when Site Manager cannot compare the installed version with the latest version available from Cisco Software Central.
Sensor version	The current software version installed on the sensors connected to the Center. Non-green statuses indicate that the sensor version does not match the Center version. For example, if a Center runs Release 5.5.0 but the connected sensors are running 5.4.0, this difference is flagged for your attention.
KDB	The version of the Knowledge Database running on the Center. Orange statuses indicate that newer versions are available for upgrade. A gray status can appear when Site Manager cannot compare the installed version with the latest version available from Cisco Software Central.
Extensions	The current version of the sensor management and report management extensions running on the Center, if installed on the Center. Orange statuses indicate that the extension versions do not match the Center version and must be updated. A gray status can appear when Site Manager cannot compare the installed version with the latest version available from Cisco Software Central.
License	The status of licensing compliance for the Center.

Column name	What the values mean
Health	The operational status of these Center processes: • Ingestion: Non-green statuses indicate that there is excessive data flow that could overwhelm a Center. • Services: Performs a health check of various services running on the Center.

Center details in Dashboard

In the table view of the dashboard, click a Center from the displayed list to view these details.

The header of the Center details page displays:

- Center name.
- Refresh status: the remaining time for the next Center data refresh.

Update history

Use the global **Update history** page to view Local Center update activity managed by Site Manager. To review update activity for one Local Center, open the Center details page for that Center and view its **Update history**.

Table 3: Center-specific summary information

Section name	The details that are displayed
Center details	• Center IP address • Connection status • Center version • Knowledge DB version • GeoLocation DB version • Licensing compliance
Health	• The status of ingestion services • Number of services that are currently down.
Extensions	The current version of the sensor management and report management extensions running on the Center, if installed on the Center.

Section name	The details that are displayed
Sensor details	For each sensor connected to the Center, these details are displayed on the Center details page: • Name • Model • IP address • Version: Non-green statuses indicate the sensor status does not match the Center status. • Serial number • Health • Processing • Features: Indicates whether Intrusion Detection Service (IDS), Secure Equipment Access (SEA), and Active Discovery (AD) are active on the sensor. • Uptime

System configurations

The Site Manager offers various features to help you streamline and optimize Local Center management. You can enable each of these features in the **Configuration** > **System** > **Setup** page.

Table 4: Site Manager system configurations

Feature	Is this feature enabled by default?	Why you should enable this feature
Cisco Software Central connection	No	Connect to Cisco Software Central using a Cisco Account that has the required licenses and entitlements. Enabling this feature allows you to automate the update process for: • Site Manager software updates • Local Center KDB updates The Site Manager checks for new software files between 12:00 a.m. and 2:00 a.m., UTC. If new software is available, the Site Manager initiates the update process.

Feature	Is this feature enabled by default?	Why you should enable this feature
Cisco Cloud connection	No	Connect to Cisco Cloud for Center geolocation updates. During the initial connection setup, link Site Manager to the Cisco Cloud cluster that your deployment uses, such as the US cluster or the EU cluster. Geolocation updates use a separate weekly update process from Site Manager software and KDB updates. When a new geolocation database is available, Site Manager updates it through the Cisco Cloud connection.
Data monitoring preferences	Yes	Enable telemetry and Interactive Help features to allow Cyber Vision to collect anonymous diagnostic and usage data, and to receive helpful in-product guidance.

After you add a Cisco Software Central or Cisco Cloud connection, both connections include a **Remove account** button. You may need to remove and reestablish a connection for troubleshooting purposes.

Configure system connectivity and security

Site Manager relies on essential system configurations such as DNS, NTP, proxy, and web server certificates, to ensure secure external connections and optimized performance.

Setting up these parameters correctly is vital to maintain a secure, synchronized, and reliable operational environment for your Cyber Vision deployment.

Table 5: Site Manager system settings.

Setting	Purpose
NTP	NTP ensures that your system clock remains perfectly synchronized with a reliable time source, which is critical for accurate event logging and security certificate validation. Without precise time synchronization, you might not be able to maintain secure communications or conduct reliable forensic analysis of network events
DNS	DNS acts as the network's directory service, translating human-readable domain names into the IP addresses required for system communication. This setting allows your Site Manager to reliably resolve and connect to external Cisco services, such as software update repositories and cloud intelligence feeds.

Setting	Purpose
Proxy	Proxy settings enable your Site Manager to securely route external traffic through an intermediary server. This configuration is essential for environments that restrict direct internet access. This configuration ensures that critical integrations such as Smart Licensing and threat intelligence function while remaining compliant with your organization's network security policies.
Web Server Certificate	The web server certificate provides the cryptographic identity for your Site Manager, ensuring that connections to the web interface are both authentic and encrypted. By establishing this trust, the certificate helps you protect your administrative sessions from interception and prevents unauthorized access to your management console.

Configure Site Manager date and time

Configure the date and time for the Site Manager. It is recommended to use an NTP server to ensure consistency across the Site Manager, Centers, and sensors. Differences in date and time settings can result in ineffective data reporting.

Step 1 In the Site Manager, go to **Configuration** > **System** > **Network & Time**.

Step 2 Click **Date and Time**.

Step 3 You can configure the date and time for Site Manager in two ways.

Date and time method	Steps to be taken
(Recommended) Connect to an NTP server	**a.** Choose **NTP Servers**. **b.** Click **Add New NTP Server**. **c.** Enter the NTP server address. **d.** Optionally, enter a Key ID or AES-CMAC for secure authentication. **e.** Click **Test Connection** to verify that the configuration is accurate.
Manually set the time, in UTC	• Choose **Manually set time (UTC)**. • Enter a time for the Site Manager.

Step 4 Click **Save Changes**.

Configure proxy

Configure a proxy to enable secure network connectivity for feature that require external connectivity, such as cloud connections and product integrations.

Step 1 In the Site Manager, go to **Configuration** > **System** > **Network & Time**.

Step 2 Click **Proxy**.

Step 3 Click the **Enable proxy** toggle switch to enable the feature.

Step 4 Enter the IP address (IPv4 or IPv6) and port details for the proxy server.

Step 5 If your proxy requires authentication, enter the username and password.

Step 6 Click **Test connection** to verify that the proxy is correctly configured.

Step 7 Click **Save changes** to apply the configuration.

Configure DNS server

Connect a DNS server to resolves hostnames to IP addresses. The resolution is necessary for the Site Manager to communicate with external services.

Step 1 In the Site Manager, go to **Configuration** > **System** > **Network & Time**.

Step 2 Click **DNS**.

Step 3 Click **Add new DNS server**.

Step 4 Enter the IP address of the DNS server.

You can add up to four DNS servers.

Step 5 Click **Test connection** to verify that the Site Manager can reach the DNS server.

Step 6 Click **Save changes** to apply these settings.

Update web server certificate

Update a web server certificate before it expires to ensure uninterrupted connectivity with onboarded Local Centers.

You can choose from three types of web server certificate methods, based on the requirements of your organization.

Method	Purpose
Upload a .p12 file	Import an existing, pre-generated certificate package.
Generate a Certificate Signing Request (CSR)	Request a certificate from your organization's internal or an external Certificate Authority (CA).
Use the ACME protocol	Automate certificate issuance and renewal using a supported CA.

Step 1 In the Site Manager, go to **Configuration** > **System**.

Step 2 Click **Change Certificate** in the **Web Server Certificate** area.

Step 3 In the **Update web server certificate** page, choose the update method you want to use by clicking the corresponding radio button.

Method	Steps to follow
Upload .p12	**a.** Enter the certificate password. **b.** Add your .p12 file in the upload area. **c.** Click **Save**.
Generate a CSR	**a.** Enter the FQDN (Fully Qualified Domain Name).

Method	Steps to follow
	b. Select an encryption key type from the **Key Type** drop-down list. **c.** Click **Generate and Download CSR**. **d.** Upload a complete PEM bundle, which includes the concatenated certificate, CA, and sub CA. **e.** Click **Save**.
Use ACME protocol	**a.** Enter the FQDN. **b.** Choose **Let's Encrypt** or **Custom CA** as your certificate authority. **1.** For Let's Encrypt, enter your email ID. **2.** For Custom CA, enter your email ID, and the server URL, EAB Key ID, and EAB HMAC key for the CA. **c.** Choose **HTTP** (if the Site Manager is publicly accessible) or **DNS** (if the Site Manager is on a private network behind a firewall) as the challenge method. **1.** If you choose the DNS challenge method, enter the IP address, key name, key algorithm, and key secret for the DNS server. **d.** Click **Generate and Save**.

Step 4 When you save the certificate, the page refreshes automatically. If your browser displays a certificate warning, accept it to return to the **System** page.

What to do next

If you have used a custom certificate and need to troubleshoot this configuration, click **Restore default certificate**. The custom certificate is replaced with a default certificate from the Site Manager.

Backup and restore

If you need to reinstall Site Manager to host the manager elsewhere or for extreme troubleshooting, you can use the backup and restore method to retain existing data.

Backup and restore commands

Use these commands in the CLI of Site Manager to carry out the backup and restore process:

1. Use the **sbs-backup export** command to export the Site Manager backup files.
2. To include existing downloaded update files in the backup, use the **sbs-backup export --include-update-files** command.
3. In the target Site Manager instance, use the **sbs-backup import /path/to/backup-file** command to import the backed-up data.

Verification after restoring data

The backup and restore process may not retain active cloud connections. You must log in to the Site Manager and reconnect to Cisco Software Download and Cisco Cloud.

Troubleshooting with logs

You can generate and download Site Manager logs from the **Diagnostic** section on the **Configuration** > **System** page.

Diagnostic files include logs for these events:

- Local Center status changes
- Site Manager status changes
- Cisco Cloud connection status changes
- Cisco Software Central connection status changes
- Site Manager and KDB software file downloads

  The logs only list the names and versions of the downloaded software files. The logs exclude the contents of the downloaded files.