



Cisco Crosswork AI Administration

Table of Contents

Crosswork AI Administration	1
Check system health and collect diagnostics	2
Review system status and resource usage	2
Review application status	3
Collect tech support logs	4
Review pod status	4
Manage software images	6
View installed software	6
Add a software image	6
Back up and restore Crosswork AI	10
Before you begin	10
Create an on-demand backup	10
Schedule recurring backups	11
Restore from a backup	12
Check backup and restore status	13
Manage certificates	15
How are certificates used in Crosswork AI?	15
Features that use certificates	15
Add a trusted CA certificate	15
Add a system certificate	16
Generate a certificate signing request	17
Manage users and roles	19
System-defined roles and permissions	19
Add a role	23
Add a user	24
View active sessions	25
Configure AAA settings	26
Configure and manage SSO	26
Configure session and password settings	26
Review audit logs	29
Configure system settings	30
Configure remote storage	30
Configure network routes	30
Configure DNS	31
Configure NTP	32
Configure an external proxy	32
Configure the pre-login disclaimer	33

Crosswork AI Administration

The Administration menu allows you to monitor and maintain Crosswork AI, manage software and backups, configure security and access, review audit activity, and update system settings.

To access administration, sign in to Crosswork AI and choose **Administration** from the main menu.

For deployment, system bringup, and initial integration setup, refer to **Crosswork AI Getting Started** doc.

Check system health and collect diagnostics

System Details help you monitor the health of the Crosswork AI system, applications, and pods. You can review the system configuration, monitor CPU, memory, and file system usage, and collect diagnostic information when a problem requires further investigation.

Review system status and resource usage

Review the system status and resource usage to confirm that Crosswork AI is operating normally and has sufficient CPU, memory, and file system capacity.

To review the system status and resource usage:

1. Choose **Administration > System Details**.
2. In **Summary**, review the overall status of the system.

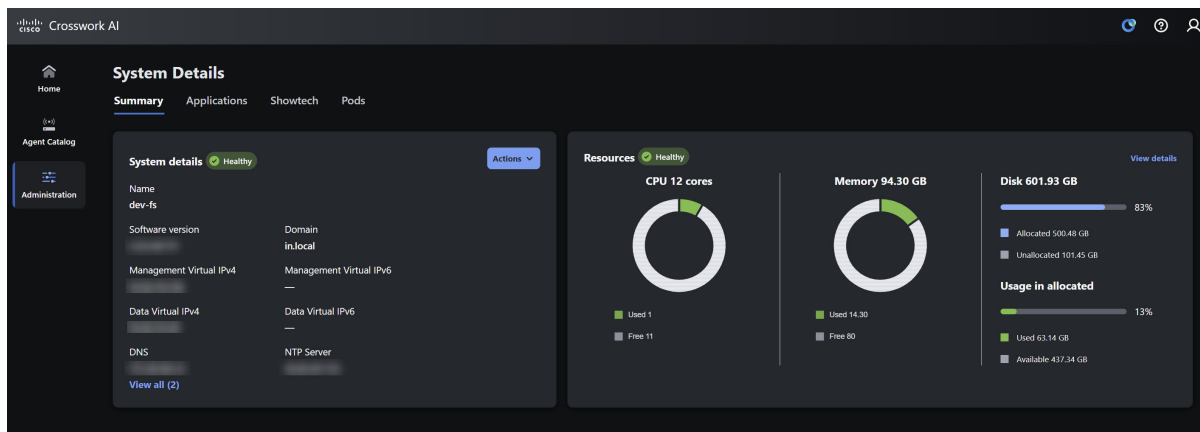


Figure 1. System details - summary

3. Review the system information:
 - o **Name:** Name assigned to the Crosswork AI system during system bringup.
 - o **Software version:** Currently installed Crosswork AI software version.
 - o **Domain:** Domain configured for the system.
 - o **Management Virtual IPv4** and **Management Virtual IPv6:** Virtual IP addresses used for management access.
 - o **Data Virtual IPv4** and **Data Virtual IPv6:** Virtual IP addresses used for the data network.
 - o **DNS:** DNS server configured for the system. If multiple DNS servers are configured, select **View all** to display the complete list.
 - o **NTP Server:** NTP server used to synchronize the system time.
4. In **Resources**, review the overall resource status and current usage:
 - o **CPU** shows the percentage of CPU in use and the number of cores in use.
 - o **Memory** shows the percentage and amount of memory in use.
 - o **Disk and Usage in allocated** shows the percentage and amount of storage capacity in use.
5. Select **View details** to review additional resource information.



Resource metrics are retained for up to two days. Data outside this period is not available.

6. Choose **Actions** to access related administration tasks:

- **System settings** opens the system configuration settings.
- **Software upgrade** opens software management.
- **Request all** generates a Showtech archive that contains logs and diagnostic information. Refer to [Collect tech support logs](#) for instructions.

Review application status

Review the application status to monitor the platform infrastructure or the Crosswork AI application microservices. Each application includes multiple microservices that work together to provide platform or product functionality.

To review application status:

1. Choose **Administration > System Details** and select **Applications**.

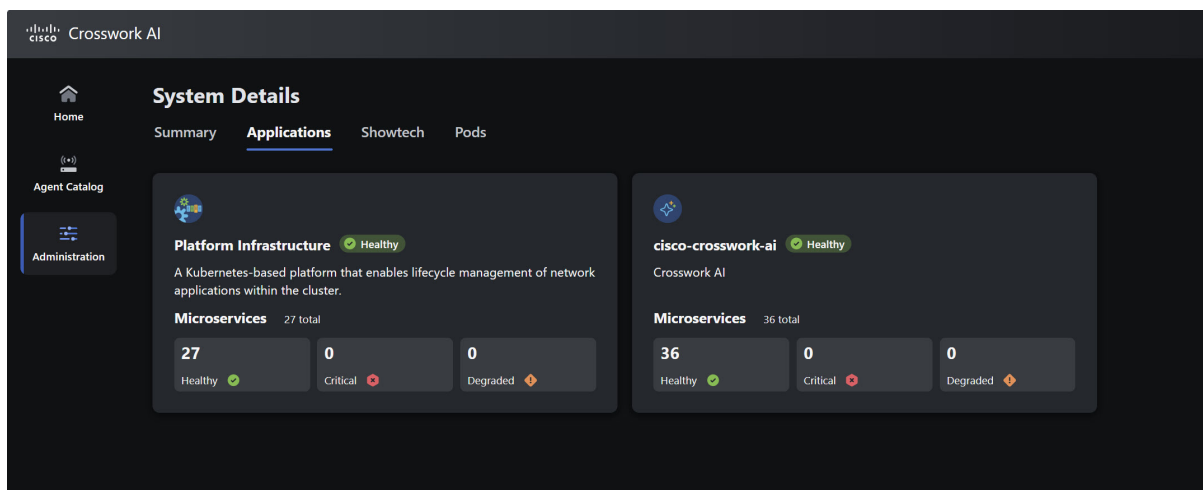


Figure 2. System details - applications

2. Review the overall status of **Platform Infrastructure** and **cisco-crosswork-ai**.
3. For each application, the system displays the total number of microservices and the number reported as **Healthy**, **Critical**, or **Degraded**.
4. Select an application to review more information.
 - In **Overview**, review the overall application details. You can also choose **Actions** to access **System settings** and **Software upgrade**.
 - In **Microservices**, review the services that make up the application. For each microservice, the system displays its name, type, status, creation time, and uptime. Use search or filter by status to locate a specific microservice or identify services that are not operating normally.
 - In **Jobs**, review jobs associated with the application. Use search or filter by health status to locate a specific job or investigate an unsuccessful operation.

Collect tech support logs

Showtech is the primary tool for collecting logs and system information for troubleshooting. If you encounter a problem that you cannot resolve, or if Cisco Support requests diagnostic information, generate and download a Showtech archive.

To collect tech support logs:

1. Choose **Administration > System Details**.
2. Choose **Actions > Request all**.

The system creates a Showtech job and opens **Showtech**. The job can take several minutes to complete while the system collects logs and diagnostic information.

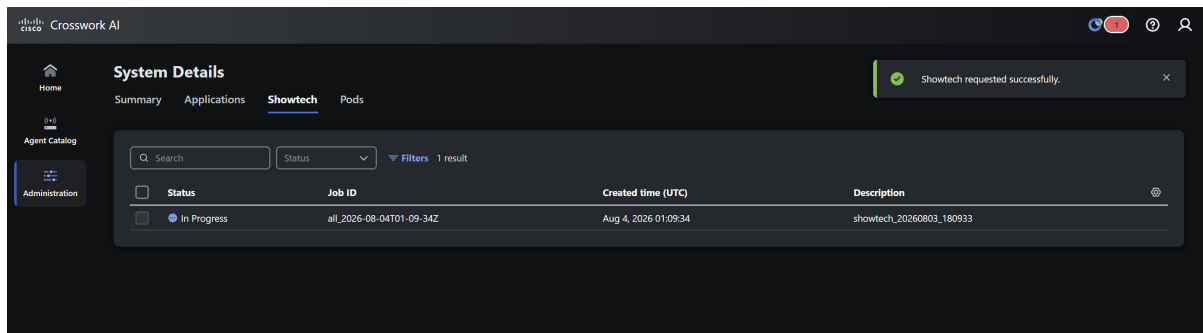


Figure 3. System details - showtech

3. Monitor the job status.
4. After the job is complete, download the Showtech archive.
5. Share the archive file with Cisco Support for further troubleshooting.

Review pod status

Crosswork AI runs platform services, application services, agents, and agent tasks in Kubernetes pods. Review the pod status when an application includes critical or degraded microservices or when you need more detailed information about a system problem.

To review pod status:

1. Choose **Administration > System Details** and select **Pods**.

Name	Service instance type	Status	Create time (PDT)	Up time
appmgr-6f98b5f4d4-ck9hm	Static	Healthy	Aug 3, 2026 08:30:23	9h 38m 6s
asset-deployer-8465c47558-7zwk	Static	Healthy	Aug 3, 2026 08:31:05	9h 37m 24s
auditmgr-67f455b4fc-dvh6p	Static	Healthy	Aug 3, 2026 08:31:29	9h 37m 0s
authy-oidc-df8699cb5-ptmck	Static	Healthy	Aug 3, 2026 08:30:25	9h 38m 4s
authy-765b54c54b-ncpnz	Static	Healthy	Aug 3, 2026 08:30:25	9h 38m 4s
ceti-0	Static	Healthy	Aug 3, 2026 08:31:08	9h 37m 21s
agent-adk-conversation-flow-agent-0-1007-vl5v4-b7rxg	Static	Healthy	Aug 3, 2026 09:23:30	8h 44m 59s
agent-adk-conversation-flow-agent-2-1019-sz2qj-6dqst	Static	Healthy	Aug 3, 2026 10:22:27	7h 46m 2s
agent-config-drift-0-task-0-2-5hd79-vq6pl	Static	Healthy	Aug 3, 2026 08:50:54	9h 17m 35s
agent-config-drift-0-task-0-9-l4z4w-mrvkj	Static	Healthy	Aug 3, 2026 10:01:28	8h 7m 1s

Figure 4. System details – pods

2. Review the name, type, and current status, creation time, and uptime of each pod.

The creation time and uptime indicate when the pod was created and how long it has been running.

3. Use **Search** to locate a specific pod, or use **Status** to display pods with a particular status.

Manage software images

Software Management allows you to view installed Crosswork AI versions, add a new software image, and monitor installation status.

View installed software

Review the currently installed system and application versions before adding or installing a new software image.

To review the installed software:

1. Choose **Administration > Software Management**.

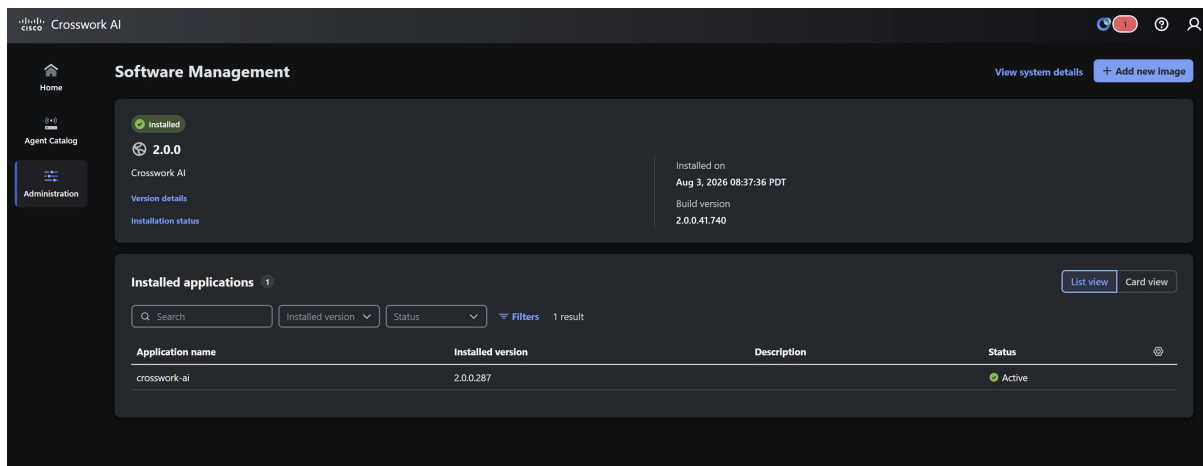


Figure 5. Software management

2. Review the installed Crosswork AI release, installation date, and build version.

The **Installed applications** list also displays the installed version and status of each application.

3. Select **Installation status** to review the status of the installed image.

The installation status includes the system name, version, overall status, and the checks completed during installation.

4. Use **Search** or filter by installed version and status to narrow the results.
5. To review additional system information, select **View system details**.

Add a software image

To install a new Crosswork AI image, first add the corresponding software image to the system. You can upload the image from your local system or transfer it from an HTTP, SFTP, or SCP server. The image must be in **.iso** format.

Before you begin

Before adding a software image:

- Obtain the **.iso** image for the Crosswork AI release that you plan to install.

- If the image is stored on a remote server, ensure that Crosswork AI can reach the server over the management network.
- For an authenticated HTTP, SFTP, or SCP connection, obtain the server address, image location, and credentials required to access the image.
- For SFTP or SCP, ensure that the account has permission to read the image from the specified server path.

To add a software image:

1. Choose **Administration > Software Management**, and then select **Add new image**.

Add new image ×

First add the image to the system. Then you will be able to install it.

Choose image source

☒ Upload from local ☐ HTTP ☐ SFTP/SCP

i Depending on the size, adding an image may take up to 60 minutes. Increase session and idle timeouts to avoid interruptions or automatic logouts. Update these settings in the [Settings](#) page.

Upload file



Click or drag file to this area to upload

Upload file/images in .iso format only

[Cancel](#) [Add](#)

Figure 6. Add new image

2. Select the image source:
 - **Upload from local:** To upload from the local system, select the upload area to locate the **.iso** image on your system, or drag the image into the upload area.
 - **HTTP:** To upload using HTTP:
 - a. Enter the **URL** of the iso image.

- b. Select **Skip TLS verification** if TLS certificate verification is not required for the connection.
- c. If the server requires authentication, enable authentication and enter the username and password.
- o **SFTP/SCP**: To upload the image from an SFTP/SCP server:
 - a. For **Choose storage server**, choose a configured server or select **Create new server**.
 - b. To create a server, enter a name and, optionally, a description.

The screenshot shows the 'Create new server' form in the Cisco Crosswork AI interface. The form is titled 'Create new server' and is part of the 'Software Management' section. It includes the following fields and options:

- Name**: A text input field.
- Description**: A text input field.
- Protocol**: A radio button selection with **SFTP** selected.
- Hostname or IP address**: A text input field with a hint: 'For example: server.name.com or 192.168.1.100'.
- Port**: A text input field with the value '22'.
- Path**: A text input field with a hint: 'For example: /home/user/backups'.
- Authorization type**: A radio button selection with **Password** selected.
- Username**: A text input field.
- Password**: A text input field with a 'Show' button next to it.
- SCP**: A radio button option.
- Create server**: A button at the bottom left.
- Cancel**: A button at the bottom right.

Figure 7. Create a new server

- c. Select **SFTP** or **SCP**.
 - d. Enter the hostname or IP address of the server.
 - e. Enter the server port. The default port is **22**.
 - f. Enter the path on the server, if required.
 - g. For **Authorization type**, select **Password** or **SSH public key**.
 - h. If you selected **Password**, enter the username and password used to access the server.
 - i. Select **Create server**.
 - j. In the **Add new image** panel, select the new server and enter the **File path** to the **.iso** image.
3. Select **Add**.

The system transfers the image from the selected source. After the image is added successfully, it becomes available for installation.



Depending on the image size, adding an image may take up to 60 minutes. Increase the session and idle timeout values as needed to avoid interruptions or automatic logouts. Update these settings in **Administration > AAA > Settings**.

Back up and restore Crosswork AI

Backup and Restore allows you to protect the Crosswork AI configuration and data. You can create a backup when needed, schedule recurring backups, and restore the system from a previously created backup.

Crosswork AI supports the following backup types:

- **Config-Only:** Includes device configurations, network settings, and user preferences. The estimated backup size is 500 MB.
- **Full:** Includes device data, configurations, logs, and user files. The estimated backup size is 10 GB.

Before you begin

- SCP is the supported remote backup destination. Ensure that you have a secure SCP server with adequate space for backups.
- Obtain the hostname or IP address of the SCP server, a file path on the server for storing backup files, and user credentials with SSH access and read and write permissions to that path.



- Only one local backup can exist at a time.
- Only one schedule can be configured for each backup type.
- Only one backup or restore operation can run at a time.
- Avoid using the system during a backup or restore operation. A backup takes the system offline for about 10 minutes. A restore can take longer and pauses other operations.

Create an on-demand backup

Create an on-demand backup to save either the current configuration data or configuration and operational data.

To create an on-demand backup:

1. Choose **Administration > Backup and Restore** and then select **Create backup**.

Figure 8. Create backup

2. Enter a name for the backup.
3. For **Backup type**, select one of the following:
 - **Config-Only** to back up device configurations, network settings, and user preferences.
 - **Full** to back up device data, configurations, logs, and user files.
4. For **Source**, select **Local download** or **Remote location** as the backup destination.
 - For a remote backup, select a configured SCP server or select **Create remote storage location**.

To create a remote storage location, refer to [Configure remote storage](#).

5. Enter an encryption key.

Store the encryption key securely. You must provide it as the decryption key when restoring the backup.

6. Select **Backup now**.

The system creates a backup job and adds it to the job list with the current status.

7. Monitor the backup progress under **Job details**.

While the backup is running, some operations may be temporarily unavailable or may respond more slowly than usual.

Schedule recurring backups

Schedule recurring backups to create recovery points automatically at regular intervals. Scheduled backups require a configured remote SCP location.

To schedule recurring backups:

1. Choose **Administration > Backup and Restore**, and then select **Schedule backup**.

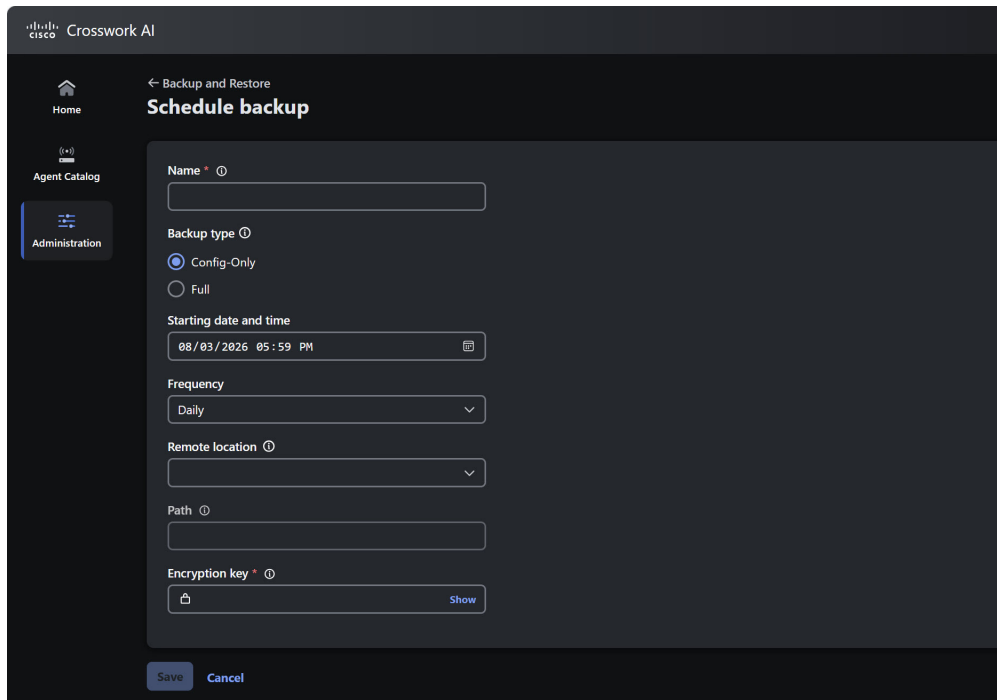


Figure 9. Schedule backup

2. Enter a unique name for the schedule.
3. For **Backup type**, select one of the following:
 - **Config-Only** to back up device configurations, network settings, and user preferences.
 - **Full** to back up device data, configurations, logs, and user files.
4. Specify the date and time when the schedule should begin.
5. For **Frequency**, select how often the backup should run.
6. For **Remote location**, select a configured SCP server or select **Create remote storage location**.

To create a remote storage location, refer to [Configure remote storage](#).

7. Enter an encryption key to secure the backup files.

Store the encryption key securely. You must provide it as the decryption key when restoring a backup created by this schedule.

8. Select **Save**.

After saving the schedule, select **Schedules** to verify that the schedule was created.

Restore from a backup

Use **Restore** to recover the Crosswork AI configuration and data after data loss or a service-impacting issue.

Before you begin, ensure you have:

- The backup file that you want to restore.
- The decryption key that corresponds to the encryption key used when the backup was created.

To restore from a backup:

1. Choose **Administration > Backup and Restore**, and then select **Restore**.

The screenshot shows the 'Restore' page in the Cisco Crosswork AI interface. The left sidebar contains navigation links for 'Home', 'Agent Catalog', and 'Administration'. The main content area is titled 'Restore' and includes the following fields and controls:

- Backup type**: Two radio buttons, 'Config-Only' (selected) and 'Full'.
- Source**: A dropdown menu currently set to 'Local Download'.
- Backup file for local restore**: A dashed box with an upload icon and the text 'Click or drag file to this area to upload'.
- Decryption key**: A text input field with a 'Show' button to its right.
- Buttons**: 'Restore', 'Validate', and 'Cancel' buttons at the bottom.

Figure 10. Restore backup

2. From **Source**, select the location of the backup:
 - a. For a **Local download**, select the upload area to locate the backup archive on your system (for example a .tar.gz file) or drag the file into the upload area.
 - b. For a **Remote location**, select the remote SCP server and the backup file that you want to restore.
3. Enter the decryption key associated with the backup.
4. Select **Validate** to validate the backup file.
5. After validation completes successfully, select **Restore**.

Check backup and restore status

Check the status of a backup or restore operation to confirm whether it completed successfully or requires further investigation.

To check the operation status:

1. Choose **Administration > Backup and Restore**.
2. In **Backup jobs**, review active and completed backup jobs.

Review the start and end times, status, backup type, destination, and the user who started the backup. Use **Search**, **Status**, and **Type** to narrow the results.

3. Select **History** to review details of previously started backup and restore operations.

Review the operation, start and end times, status, type, details, and the user who started the operation. Use search or filter by status to narrow the results.

Manage certificates

Certificates help Crosswork AI authenticate systems and protect communications using TLS. A certificate associates an identity with a public key. The corresponding private key is stored separately and must be protected.

Use **Certificate Management** in Crosswork AI to view, upload, and manage certificates.

How are certificates used in Crosswork AI?

Crosswork AI supports the following certificate types:

- **Trusted CA certificates:** Establish trust with certificates issued by a certificate authority. A trusted CA certificate can establish general trust or be assigned to a specific certificate role.
- **System certificates:** Provide a certificate and corresponding private key for a specific certificate role.

Features that use certificates

You can associate a certificate with one or more of the following features:

- **Web Server:** Replaces the default self-signed web server certificate with a user-provided certificate to secure browser connections to Crosswork AI.
- **Cyber Ark:** Secures TLS communication between Crosswork AI and a configured Cyber Ark server.
- **Observability External TLS:** Secures TLS connections used to send observability data to external destinations using HTTPS or gRPC over TLS.

Add a trusted CA certificate

Add a trusted CA certificate to establish general trust or associate the certificate with specific features.

To add a trusted CA certificate:

1. Choose **Administration > Certificate Management**, and then select **Add certificate**.

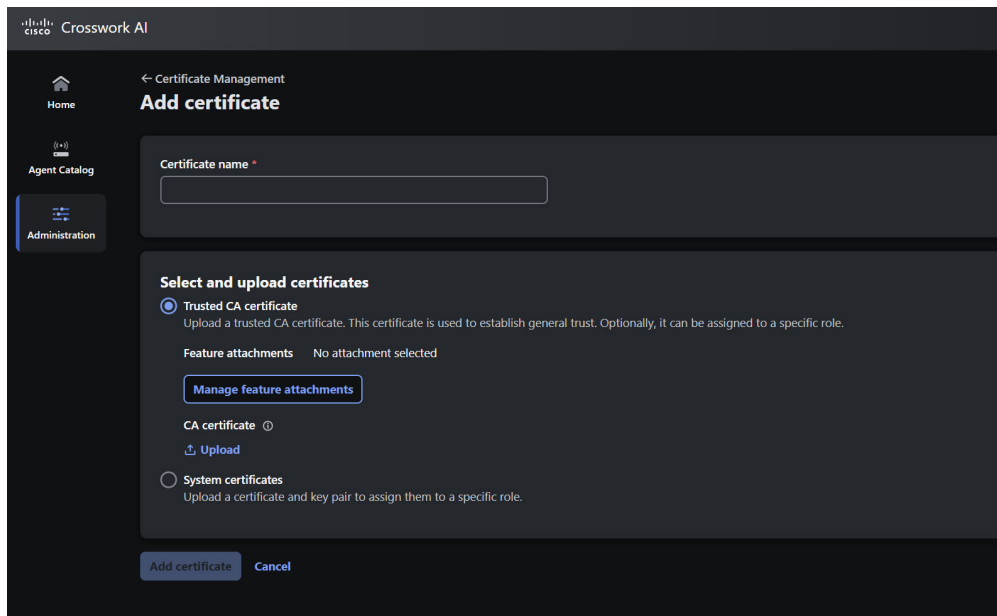


Figure 11. Add certificate

2. Enter a certificate name.
3. Select **Trusted CA certificate**.
4. To associate the certificate with specific features, select **Manage feature attachments**.
5. Select one or more of the following feature attachments, and then select **Save**:
 - o **Web Server**
 - o **Cyber Ark**
 - o **Observability External TLS**

Leave all feature attachments unselected to use the certificate for general trust.

6. Under **CA certificate**, select **Upload** and choose the trusted CA certificate.
7. Select **Add certificate**.

Add a system certificate

Provide a certificate and corresponding private key for use by specific features.

To add a system certificate:

1. Choose **Administration > Certificate Management**, and then select **Add certificate**.
2. Enter a certificate name.
3. Select **System certificates**.

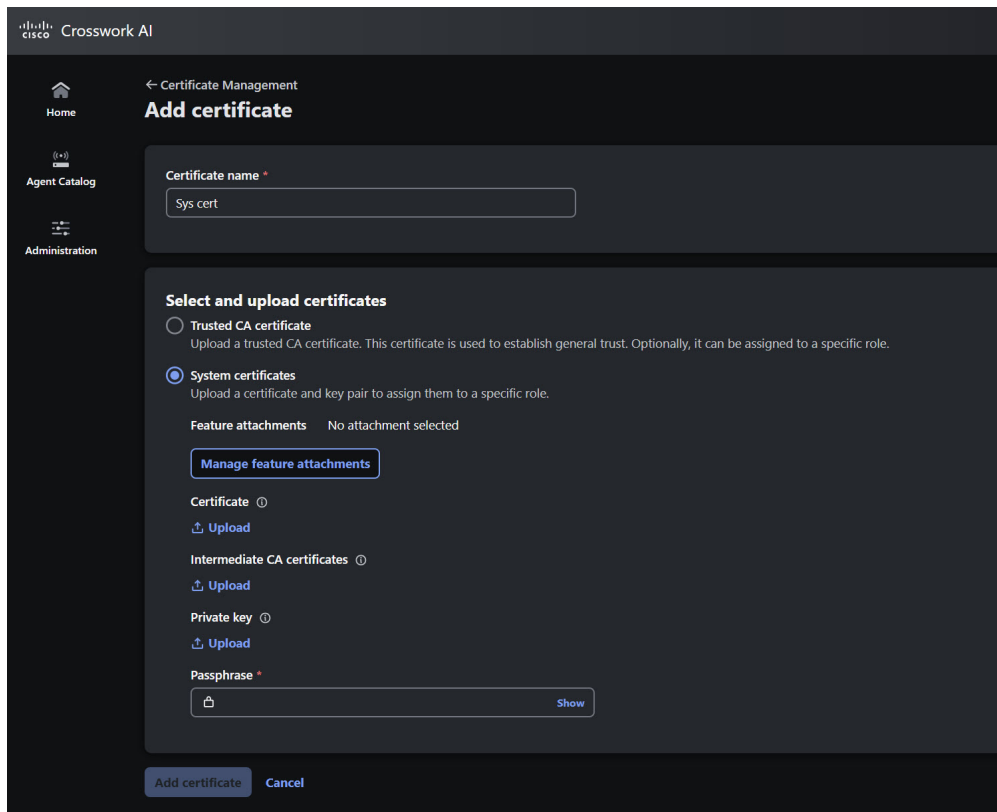


Figure 12. Add system certificate

4. Select **Manage feature attachments**.
5. Select one or more of the following feature attachments, and then select **Save**:
 - **Web Server**
 - **Cyber Ark**
 - **Observability External TLS**
6. Under **Certificate**, select **Upload** and choose the system certificate.
7. If the certificate requires intermediate CA certificates, select **Upload** under **Intermediate CA certificates** and choose the applicable certificate files.
8. Under **Private key**, select **Upload** and choose the private key that corresponds to the system certificate.
9. Enter the private-key passphrase.
10. Select **Add certificate**.

Generate a certificate signing request

Generate a certificate signing request (CSR) when you need a certificate authority to issue a system certificate for Crosswork AI.

Before generating the CSR, obtain the subject information and key requirements specified by your certificate authority. Identify all IP addresses and fully qualified domain names that clients use to access Crosswork AI.

To generate a certificate signing request:

1. Choose **Administration > Certificate Management**, and then select **Certificate signing request**

(CSR).

2. Select **Generate CSR**.
3. Enter a certificate name.
4. For **Certificate role**, choose **System**.
5. For **Subject details**, enter the FQDN of the server or a unique name, along with other details such as the country, state, locality, organization, and organizational unit.
6. Under **Subject alternate names (SAN)**, enter the IP address and FQDN used to access the Crosswork AI deployment.

Add any additional IP addresses or FQDNs if they are required for certificate validation.

7. For **Key**, choose the key type, key size, and digest required by your organization's certificate policy.
8. Select **Generate CSR**.

Manage users and roles

Users and Roles in Crosswork AI allows you to create users, assign roles, create custom roles, and view active user sessions.

Users are assigned roles that determine what they can do in Crosswork AI. Each role contains access profiles that define permissions for specific product capabilities. For example, the **AI Agent Catalog** access profile controls permissions to view or manage agents and their settings in the catalog.

Access profile permissions apply whether the capability is used through the Crosswork AI user interface or through an API.

System-defined roles and permissions

Crosswork AI provides system-defined roles for AI operations and system administration. You can assign these roles to users or create new roles with access profiles tailored to your requirements.

- **cw-ai-viewer:** View Crosswork AI agents, LLMs, operations, Knowledge Graph, and related AI services in read-only mode.
- **cw-ai-operator:** Run AI operations and perform day-to-day updates to agents, LLMs, and supporting AI services.
- **cw-ai-admin:** Manage Crosswork AI capabilities, including agent catalog and instance management, knowledge graph, LLMs, observability destinations and UI access, AI operations, platform settings, AI service configuration, context service, DRA gateway, and MCP gateway.
- **observer:** View system resources for monitoring and troubleshooting in read-only mode.
- **support-engineer:** Manage system resources for maintenance and troubleshooting.
- **super-admin:** Manage all system capabilities and settings.

The table lists the roles and permissions required for Crosswork AI capabilities.

Table 1. Roles and permissions by capability

Capability	Action	Access profile	Minimum access	System-defined roles
Configuration Drift Detection	Create and manage logical groups	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Train a model	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Run inference on demand	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Schedule inference	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Manage anomaly feedback, including importing and exporting feedback	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
Toxic Factor Identification	Run toxic factor analysis	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Schedule toxic factor analysis	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
Deep Network Troubleshooting	Start or continue a troubleshooting investigation	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Review, add, or remove hypotheses and start validation	AI Operations	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
AI operations	View existing threads, messages, and task results	AI Operations	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator

Capability	Action	Access profile	Minimum access	System-defined roles
Knowledge Graph	Explore graph schema and entity data, and run GraphQL queries	AI Knowledge Graph	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Ingest data and run GraphQL mutations	AI Knowledge Graph	Edit	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Manage schema extensions and other Knowledge Graph administration	AI Knowledge Graph	Manage	Crosswork AI Admin Super Administrator
Observability	View configured external observability destinations	AI Observability	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Update an existing external observability destination	AI Observability	Edit	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Create or delete external observability destinations	AI Observability	Manage	Crosswork AI Admin Super Administrator
	Access the Observability UI and view logs, metrics, traces, and dashboards	AI Observability	Manage	Crosswork AI Admin Super Administrator
Agent management	View agents and their settings	AI Agent Catalog	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Register or update agents and their settings	AI Agent Catalog	Edit	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Delete agents	AI Agent Catalog	Manage	Crosswork AI Admin Super Administrator

Capability	Action	Access profile	Minimum access	System-defined roles
LLM management	View LLM providers, models, associations, and default settings	AI LLM Management	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Create or update LLM providers, models, associations, and default settings	AI LLM Management	Edit	Crosswork AI Operator Crosswork AI Admin Super Administrator
	Delete LLM configuration	AI LLM Management	Manage	Crosswork AI Admin Super Administrator
Context Service	View and search collections and documents	Context Service Management	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Manage collections and documents	Context Service Management	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
DRA Gateway	View DRA Gateway instances, types, operations, and discovery information	DRA Gateway	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Manage DRA Gateway instances, types, and operations	DRA Gateway	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator
MCP Gateway	View MCP Gateway resources, tools, probes, and tasks	MCP Gateway	View	Crosswork AI Viewer Crosswork AI Operator Crosswork AI Admin Super Administrator
	Manage MCP Gateway resources and related configuration	MCP Gateway	Manage	Crosswork AI Operator Crosswork AI Admin Super Administrator

Capability	Action	Access profile	Minimum access	System-defined roles
System administration	View system resources for monitoring and troubleshooting	Observer System Access	View	Observer Support Engineer Super Administrator
	View backup status, history, and schedules	Observer System Access	View	Observer Support Engineer Super Administrator
	Create and schedule system backups	Support Engineer System Access	Manage	Support Engineer Super Administrator
	Collect tech support information	Support Engineer System Access	Manage	Support Engineer Super Administrator

Add a role

Create a new role with the required access profiles and permission levels.

To add a role:

1. Choose **Administration > Users and Roles**, select **Roles**, and then select **Add role**.

Figure 13. Add a new role

2. Enter a name and, optionally, a description for the role.
3. Select **Next**.

Figure 14. Select access profiles

4. For each access profile required for the role, assign the appropriate access level:

- **No access**
- **View**
- **Edit**
- **Manage**

The available access levels can vary by access profile. Use **Search** or filter by category to locate specific access profiles.

5. Select **Next**.

6. Review the role details and selected access levels.

7. Select **Confirm**.

Add a user

Create a new user and assign the appropriate roles based on the user's responsibilities.

To add a user:

1. Choose **Administration > Users and Roles**, and then select **Add user**.

Figure 15. Add a new user

2. Enter the user details.

- Enter a **Username**.
- Enter and confirm the password.
- Optionally, enter the user's first name, last name, and email address.

3. Select **Next**.

4. The access domain determines the resources governed by your role permissions. For **Access domain**, choose **All-access**. All-access is the only domain currently available for selection.

5. For **Role**, choose one or more roles for the user.

Assign only the roles required for the user's responsibilities.

6. Select **Next**.

7. Review the user details and assigned roles.

8. Select **Confirm**.

View active sessions

View active sessions to identify users who are currently connected to Crosswork AI and check their recent session activity.

To view active sessions:

1. Choose **Administration > Users and Roles**, and then select **Active sessions**.

Users and Roles							Last updated: Aug 6, 2026 00:20:22 PDT Refresh	
Users		Roles		Active sessions				
Q Search		Login method		Session type		Filters 6 results		
☐	Session ID	Username	Login method	Session type	Login time (PDT)	Last activity time (PDT)	Session duration	
☐	f7e15740d6784238842bc18eeb00d30	admin	LOCAL	UI	Aug 5, 2026 21:13:12	Aug 6, 2026 00:20:04	03h 01m 12s	...
☐	90910c724eb8499c3a2a96d5a4448c36	admin	LOCAL	UI	Aug 5, 2026 23:39:33	Aug 6, 2026 00:20:14	40m 51s	...
☐	76b84063416a40368ba849959b47f40	admin	LOCAL	UI	Aug 5, 2026 23:44:00	Aug 6, 2026 00:01:39	36m 24s	...
☐	7131a51a830b4b1cb66ed6dffa6631a	admin	LOCAL	UI	Aug 6, 2026 00:09:23	Aug 6, 2026 00:20:24	10m 51s	...
☐	ce06cd172d45424d964f754193913d2d	admin	LOCAL	UI	Aug 6, 2026 00:13:21	Aug 6, 2026 00:19:26	07m 03s	...
☐	0feaf894c31c4454af0982bcb172d1e8	admin	LOCAL	UI	Aug 6, 2026 00:16:16	Aug 6, 2026 00:20:17	04m 08s	...

Figure 16. User active sessions

2. Use **Search** or filter by login method and session type to narrow the results.

3. Review the session ID, username, login method, session type, login time, last activity time, and session duration.

4. To investigate activity associated with a session, choose **... > Audit log** for that session.

The **Audit Log** displays the related audit records. You can download the displayed audit records in CSV or JSON format.

5. Select **Refresh** to retrieve the latest session information.

Configure AAA settings

AAA in Crosswork AI provides settings for single sign-on (SSO), user session timeouts, and local password policies.

Configure and manage SSO

SSO for cross-launch from Crosswork Network Controller is typically configured during the initial Crosswork AI setup. In this configuration, Crosswork Network Controller acts as the SAML identity provider (IdP) and Crosswork AI acts as the service provider (SP).

Use **AAA > SSO** to manage the Crosswork AI side of the SSO configuration. You can add identity provider metadata and download the Crosswork AI service provider metadata.

For the complete SSO configuration between Crosswork Network Controller and Crosswork AI, including the configuration required in Crosswork Network Controller, refer to **Set up SSO for cross-launch from Crosswork Network Controller** in the Crosswork AI Getting Started guide.

To manage SSO metadata:

1. Choose **Administration > AAA**.
2. Select **Add identity provider**.

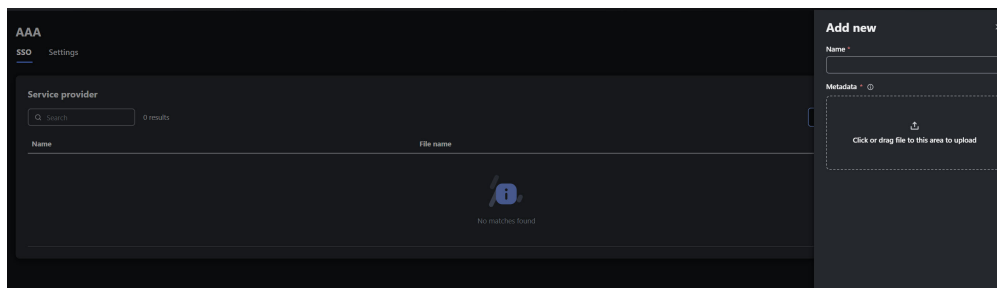


Figure 17. Add a new IdP

3. Enter a name for the identity provider.
4. Upload the IdP metadata XML file.
5. Select **Add**.
6. To download the Crosswork AI service provider metadata, select **Download SP metadata**.



The role provided by the identity provider must have a matching role in Crosswork AI. Refer to [Manage users and roles](#) for information about Crosswork AI roles.

Configure session and password settings

Use **Settings** to control idle user sessions and configure password and account lockout requirements for locally authenticated users.

To configure session and password settings:

1. Choose **Administration > AAA**, and then select **Settings**.

AAA

SSO **Settings**

Global idle timeout

Session timeout ⓘ
20 Minutes

Logout all idle users after ⓘ
60 Minutes

Local password policy

Maximum failed login attempts
0

☐ Duration unlock

Lock duration
300 Seconds
For UI admin user and SSH rescue user

Minimum password length
8

☐ Strong password check

Reuse restriction limit
5

Password expiry duration ⓘ
0 Days

Save **Cancel** No changes have been made yet

Figure 18. Configure AAA settings

- Under **Global idle timeout**, configure the session timeout settings as required:



Changing the session timeout settings restarts Crosswork AI services. The application and APIs are temporarily unavailable during the restart, and users may see a connection error or need to sign in again.

- **Session timeout:** Specifies how long a user session can remain idle before the session expires.
 - **Logout all idle users after:** Specifies when all idle users are signed out.
- Under **Local password policy**, configure the settings required for your security policy:
 - **Maximum failed login attempts:** Specifies how many unsuccessful sign-in attempts are allowed before the account is locked.
 - **Duration unlock:** Enables automatic unlocking after the configured **Lock duration**.
 - **Lock duration:** Specifies how long the account remains locked after the maximum failed login attempts is reached. The lock duration applies to the UI admin user and the SSH rescue user.

- **Minimum password length:** Specifies the minimum number of characters required for a local user's password.
- **Strong password check:** Enables additional password-strength requirements.
- **Reuse restriction limit:** Specifies how many previously used passwords a user cannot reuse.
- **Password expiry duration:** Specifies the number of days before a local user's password expires. A value of 0 disables password expiration. When a password expires, the user must change it before signing in.

4. Select **Save**.

Review audit logs

Audit Log provides a record of user activity in Crosswork AI. Audit records help you investigate sign-in attempts, identify who performed an action, such as adding or removing an agent, and determine when and from which device the action occurred.

To review audit logs:

1. Choose **Administration > Audit Log**.

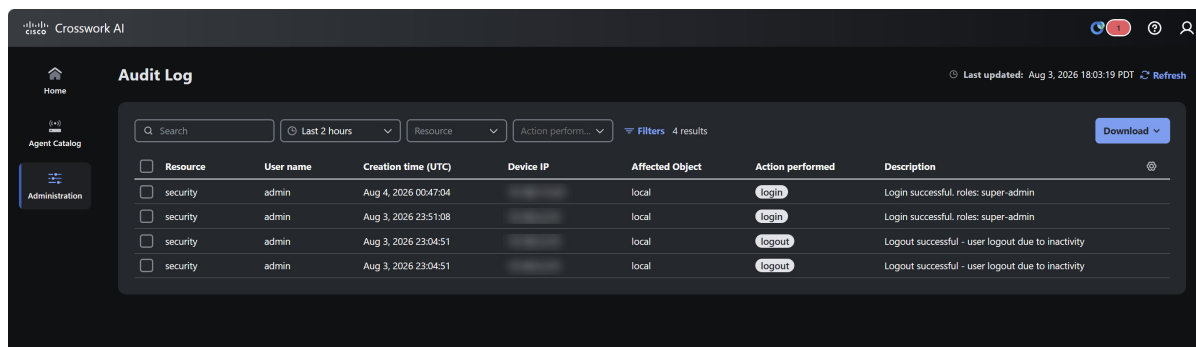


Figure 19. Audit logs

2. To narrow the results, use **Search** or filter by period, resource, and action performed. Select  to change the table density or choose which columns are displayed.
3. Review the audit record details:
 - **Resource**: System resource associated with the activity.
 - **User name**: User that performed the action.
 - **ID**: Unique identifier for the audit record.
 - **Creation time (UTC)**: Date and time when the activity was recorded.
 - **Device IP**: IP address from which the action originated.
 - **Affected Object**: Object affected by the action.
 - **Action performed**: Action recorded by the system, such as a login or logout.
 - **Description**: Additional information about the action and its result.
4. Select **Refresh** to retrieve the latest audit records.
5. To download the displayed audit records, choose one of the following:
 - **Download > Download CSV**
 - **Download > Download JSON**

The selected file is downloaded to your system.

Configure system settings

System Settings in Crosswork AI allows you to update network settings, remote storage, and other system-level settings.

DNS, NTP, and proxy settings are initially configured during system bringup. You can update these settings later as your environment changes.

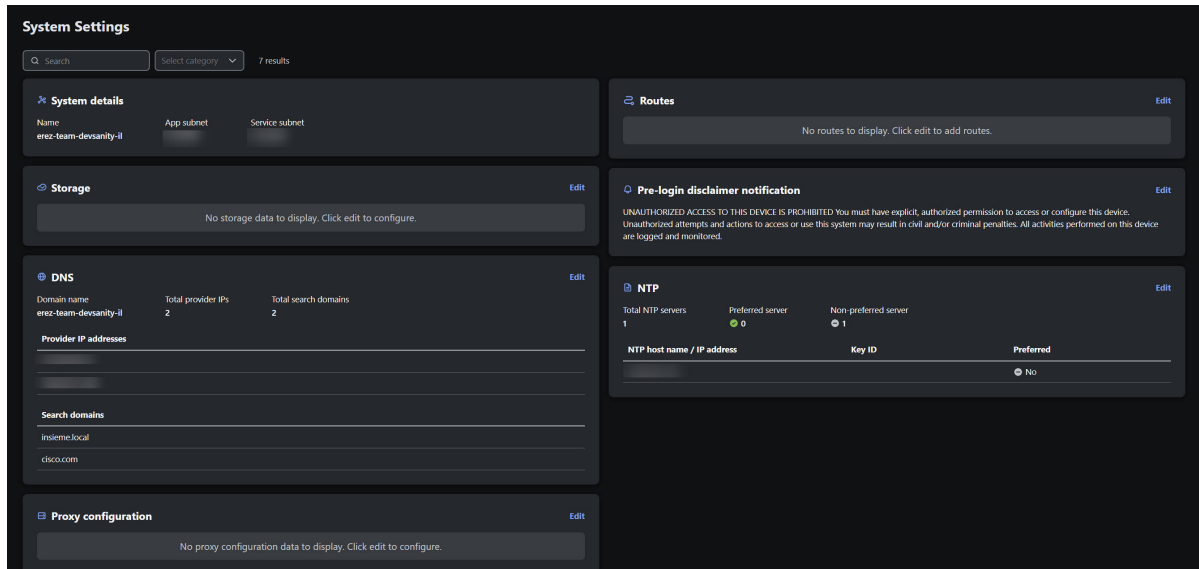


Figure 20. System settings

Configure remote storage

Configure an SCP location that Crosswork AI can use for remote storage.

Before you begin, ensure that the SCP server is reachable from Crosswork AI and that the user account has the required access to the remote path.

To configure or update a remote storage location:

1. Choose **Administration > System Settings**.
2. Under **Storage**, select **Edit**.
3. Select **Add location** to configure a new remote storage location, or select the edit icon for an existing location.
4. Enter a name and, optionally, a description for the remote location.
5. Enter the SCP server hostname or IP address.
6. Enter the path on the server, if required.
7. Enter the username and password used to access the server.
8. Select **Save**.

Configure network routes

Configure routes when Crosswork AI needs to reach additional networks through the management or data network.

The management network is used to access the Crosswork AI VM and UI. The data network is used internally by Kubernetes.

To configure or update network routes:

1. Choose **Administration > System Settings**.
2. Under **Routes**, select **Edit**.
3. Add the route to the appropriate network:
 - o To enter a management route, select **Add management route**. To edit a management route, select the edit icon.
 - o To enter a data route, select **Add data network route**. To edit a data route, select the edit icon.
4. Enter the destination IPv4 subnet in CIDR notation, for example, **192.168.1.0/24**.
5. Add additional routes as required.
6. Select **Save**.

Configure DNS

DNS provider IP addresses and search domains are configured during system bringup. Update the DNS configuration if the DNS servers or search domains used by Crosswork AI change.

To configure or update DNS:

1. Choose **Administration > System Settings**.
2. Under **DNS**, select **Edit**.

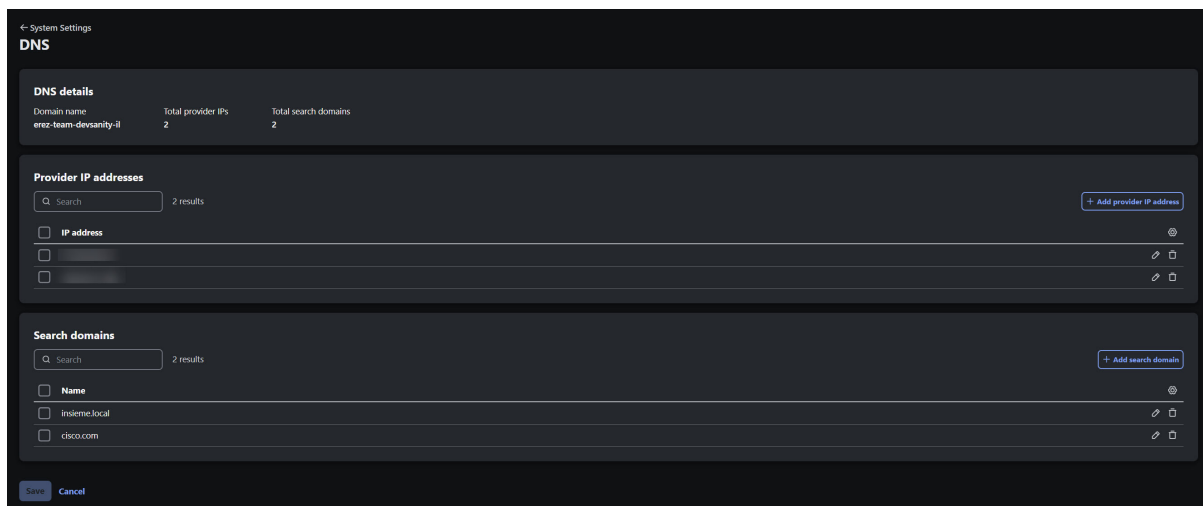


Figure 21. DNS settings

3. Under **Provider IP addresses**, add, edit, or remove DNS server IP addresses as required.

To add a DNS server, select **Add provider IP address** and enter the IP address. Select **Add**.

4. Under **Search domains**, add, edit, or remove DNS search domains as required.

To add a search domain, select **Add search domain** and enter the domain name. Select **Add**.

5. Select **Save** to save the DNS settings.

Configure NTP

NTP settings are initially configured during system bringup. Update the NTP configuration if the time servers or authentication settings used by Crosswork AI change.

You can configure one or more NTP servers and optionally use authentication.

To configure or update NTP:

1. Choose **Administration > System Settings**.
2. Under **NTP**, select **Edit**.
3. If the NTP server requires authentication, add the authentication key:
 - a. Under **ID authentication**, select **Add key**.
 - b. Enter the key ID and key.
 - c. For **Authentication type**, choose **MD5**, **SHA1**, or **AES128CMAC**.
 - d. Enable **Trusted** if the key should be configured as trusted.
 - e. Select **Add**.
4. To add a new NTP server, select **Add NTP host name**. To edit an existing NTP server, choose **Edit** from the corresponding ... menu.
5. Enter the NTP server hostname or IP address.
6. If you configured authentication, choose the corresponding **Key ID**.
7. Enable **Preferred** if this server should be the preferred NTP server.
8. Select **Add**.
9. Select **Save** to save the settings.

Configure an external proxy

Configure an external proxy when the Crosswork AI VM cannot directly reach required external services from the management network. For example, the external proxy can provide the connectivity required for the Crosswork AI LLM proxy to reach an external LLM provider.

If the VM has direct connectivity to the required external services, an external proxy is not required.

External proxy settings are typically configured during initial system bringup. For information about the initial configuration, refer to **Configure an external proxy** in the Crosswork AI Getting Started guide.

To configure or update an external proxy:

1. Choose **Administration > System Settings**.
2. Under **Proxy configuration**, select **Edit**.
3. Select **Add** to configure a new proxy, or select the edit icon for an existing proxy.
4. For **Type**, choose **HTTP**, **HTTPS**, or **HTTP and HTTPS**.

5. Enter the proxy server URL or IP address and port.
6. For **Authentication**, select one of the following:
 - **None** if the proxy does not require authentication.
 - **Credentials** if the proxy requires authentication, and enter the username and password.
7. Under **Ignored hosts**, add or edit any domains or IP addresses that should bypass the proxy.
8. Select **Save**.

After you save the proxy settings, Crosswork AI restarts the LLM proxy service. Wait for the restart to complete before configuring or verifying LLM provider connectivity.

Configure the pre-login disclaimer

Configure a pre-login disclaimer to display an authorized-use, security, or other required notice before users sign in to Crosswork AI.

To configure or update the pre-login disclaimer:

1. Choose **Administration > System Settings**.
2. Under **Pre-login disclaimer notification**, select **Edit**.
3. Enter the message that you want to display to users before sign-in.
4. Select **Save** to save the message.