

Manage Administrative Tasks

This chapter contains the following topics:

- Manage certificates, on page 1
- Manage users, on page 8
- Set up user authentication (TACACS+, LDAP, and RADIUS), on page 16
- Monitor system and application health, on page 29
- Manage backups, on page 33
- View system and network alarms, on page 39
- View audit log, on page 40
- Set the pre-login disclaimer, on page 40
- Manage maintenance mode settings, on page 41
- Update network access configuration, on page 42
- Update collector capability, on page 42
- Configure aging, on page 43
- Configure purging of archived plan files, on page 44
- Configure static routes, on page 44

Manage certificates

What is a certificate?

A certificate is an electronic document that identifies an entity such as a person, server, or company and links it to a public key. When a certificate is created, both a public key and a matching private key are generated. In the TLS protocol, the public key encrypts data, while the private key decrypts it.

Certificates are signed by an issuer, often a Certificate Authority (CA), which acts as a "parent" certificate. This process can also be self-signed. In a TLS exchange, a trust chain of certificates verifies the issuer's validity. This chain includes three types of entities: a self-signed root CA certificate, possibly several intermediate CA certificates, and an end-entity certificate. Intermediate certificates connect the server certificates to the root CA, adding security. Starting with the root certificate's private key, each certificate in the chain signs and issues the next one, ending with the end-entity certificate used for server or client authentication.

Certificates in Cisco Crosswork Planning

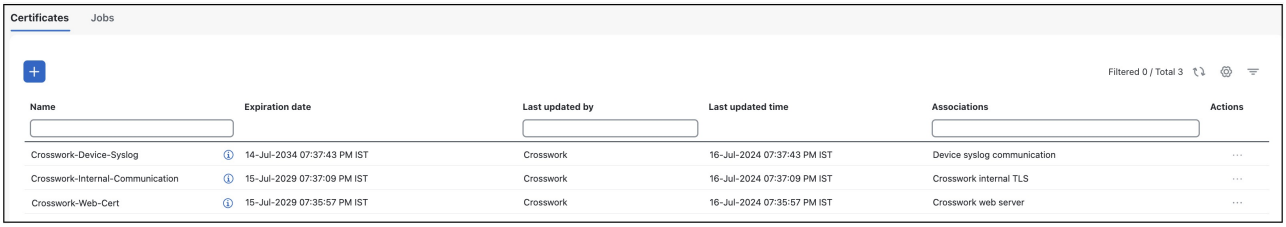
Cisco Crosswork Planning uses the TLS protocol for secure communication between devices and components. TLS utilizes X.509 certificates to authenticate devices and encrypt data, ensuring its integrity. The system

employs a combination of generated certificates and those uploaded by clients. Uploaded certificates might be purchased from Certificate Authorities or be self-signed. For instance, the system's VM-hosted web server and the client browser interface use the system-generated X.509 certificates exchanged over TLS for secure communication.

The Crosswork Cert Manager is a proxy for multiple microservices and services within the distributed framework and manages all the Crosswork certificates. The Certificate Management page (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates.

Figure 1: Certificate management page, on page 2 displays the default certificates provided by Cisco Crosswork Planning.

Figure 1: Certificate management page



Certificate types and usage

These certificates are classified into various roles with different properties depending on their use case as shown in the following table.

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork Internal TLS	Crosswork-Internal-Communication	• Generated and provided by Crosswork. • This trust-chain is available in the UI (including the server and client leaf certificates) and is created by Crosswork during initialization. • Allows mutual and server authentication.	Crosswork	Crosswork	Download	5 years	—

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork Web Server	Crosswork-Web-Cert Server Authentication	• Generated and provided by Crosswork. • Provides communication between the user browser and Crosswork. • Allows server authentication.	Crosswork Web Server	User Browser or API Client	• Upload • Download	5 years	30 days to 5 years
Crosswork Device Syslog	Crosswork-Device-Syslog	• Generated and provided by Crosswork. • Allows server authentication.		Device	Download	5 years	—

There are two category roles in Crosswork:

- Roles which allow you to upload or download trust chains only.
- Roles that allow upload or download of both the trust chain and an intermediate certificate and key.

Add new certificates

You can add certificates for the following role:

- **Secure LDAP communication**: You upload the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork, the user can add the LDAP server (see Manage LDAP servers, on page 19) and associate the certificate.

Note Cisco Crosswork Planning does not receive a web certificate directly. It accepts an intermediate CA and intermediate Key to create a new web certificate, and apply it to the Web Gateway.

Before you begin

- For information on certificate types and usage, see Certificate types and usage, on page 2.
- All certificates that are uploaded must be in Privacy Enhanced Mail (PEM) format. Note where these certificates are in the system so that you can navigate to them easily.

- Trust chain files that are uploaded may contain the entire hierarchy (root CA and intermediate certificates) in the same file. In some cases, multiple chains are also allowed in the same file.
- Intermediate Keys need to be either PKCS1 or PKCS8 format.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management** and click .

Step 2 Enter a unique name for the certificate.

Step 3 From the **Certificate Role** drop-down menu, select the purpose for which the certificate is to be used.

Note
Only the **Secure LDAP communication** option is applicable for Cisco Crosswork Planning.

Step 4 Click **Browse**, and navigate to the certificate trustchain.

Step 5 Click **Save**.

Note
Once uploaded, the Crosswork Cert manager accepts, validates, and generates the server certificate. Upon successful validation, an alarm ("Crosswork Web Server Restart") indicates that the certificate is about to be applied. The Certificate Management UI then logs out automatically and applies the certificate to the Web Gateway. The new certificate can be checked by clicking the lock <Not Secure>/<secure> icon next to the https://<crosswork_ip>:30603.

Edit certificates

You can edit a certificate to add or remove connection destinations, upload, and replace expired or misconfigured certificates. User provided certificates and web certificates can be edited. Other system certificates that are provided by Cisco Crosswork cannot be modified and will not be available for selection.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**.

Step 2 To update a certificate:

a) Under the **Actions** column, click ••• on the certificate that you want to modify, and select **Update certificate**.

b) Fill in the appropriate values for the fields based on the certificate you wish to update. Click the ⓘ icon next to the field for more information.

c) Click **Save** to save the changes.

Step 3 To enable the client certificate authentication of a web certificate:

a) Under the **Actions** column, click ••• on the Crosswork web certificate that you want to modify, and select **Configure client certificate authentication**.

The **Configure Client Authentication** page is displayed.

b) Check the **Enable** checkbox.

The **Certificate schema** and **OCSP** settings are displayed.

The **OCSP** settings are enabled by default, but you can disable it if desired. If enabled, you can check the certificate revocation status using the Online Certificate Status Protocol (OCSP).

c) Choose the **Certificate schema** value.

- **Automatic**—Searches for the user principal name (UPN) in the alternate subject name area. If a UPN is not found, the system will use the common name value. This is the default selection.
- **Manual**—Searches for the username in the subject area based on the user identity source and the specified regular expression.

d) (Optional) Choose the **OCSP** value:

- **Automatic**—Extracts the responder URL from the certificate and uses it to perform OCSP validation.
- **Manual**—You must provide the OCSP responder URL.

e) Click **Save** to save the changes.

Step 4 To update certificate and configure client authentication in a single step:

a) Click ••• on the Crosswork web certificate that you want to modify, and select **Update certificate & configure client certificate authentication**.

The **Update Certificate and Configure Client Authentication** page is displayed.

Note
Choosing the combined option to update the certificate and configure client authentication minimizes downtime during the Crosswork server restart, as it occurs only once instead of twice if these actions are performed separately.

b) Provide the data as per the instructions in step 2 and step 3.

c) Click **Save** to save the changes.

Download certificates

Follow these steps to download certificates.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**.

Step 2 Click ⓘ for the certificate you want to download.

Step 3 To separately download the root certificate and the intermediate certificate, click ⬆ next to the certificate. To download the certificates at once, click **Export all**.

Update web certificate using certificate signing request

Cisco Crosswork Planning enables the updating of web certificates by importing an intermediate Certificate Authority (CA) certificate. Starting with version 7.0.1, it also supports updating web certificates through a Certificate Signing Request (CSR).

This approach allows you to obtain a certificate signed by an Enterprise or Commercial CA without exposing the private key outside of Cisco Crosswork Planning.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- This process requires the Crosswork server to be restarted, which will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**

Step 2 Click ••• on the web certificate (`Crosswork-Web-Cert`) and select **Update certificate**.

The **Certificate Update Method** page is displayed.

Step 3 Create a CSR to submit to the Certificate Authority.

a) Select **Create a certificate signing request (CSR)** radio button and click **Update certificate**.

The **Certificate Signing Request (CSR)** page is displayed.

b) Click **Create CSR**.

The **Create Certificate Signing Request (CSR)** page is displayed.

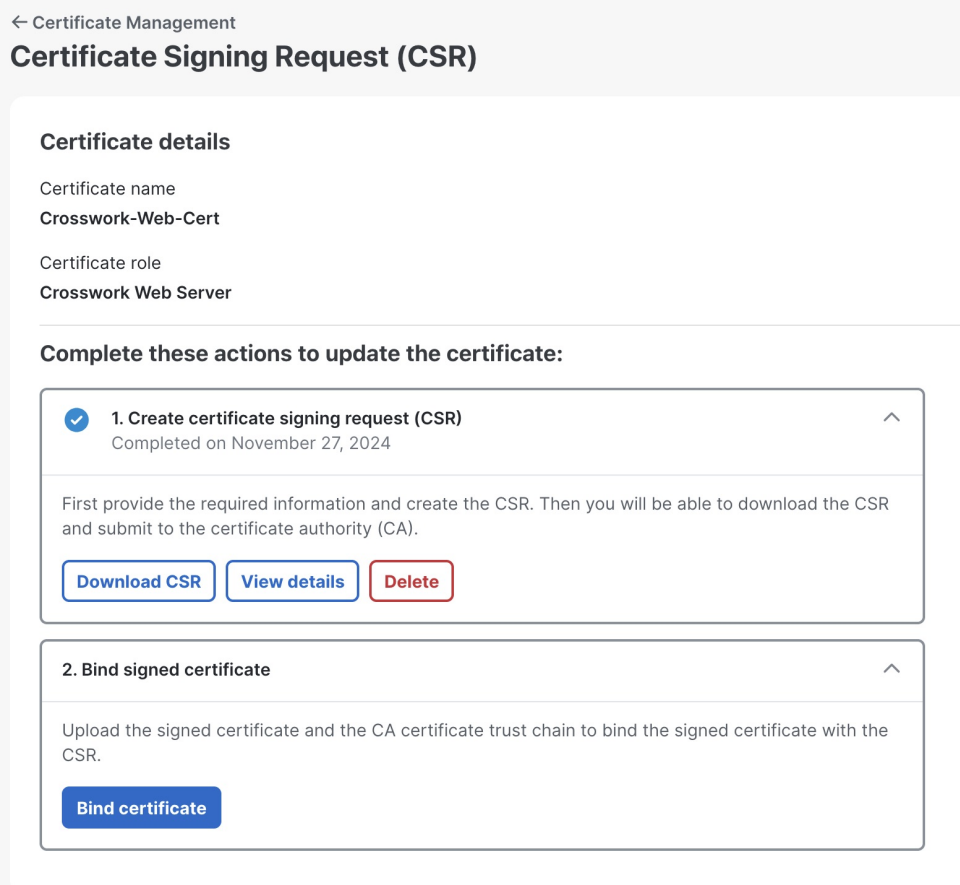
c) Provide relevant values for the fields provided. Click the ⓘ icon next to the field for more information. The mandatory fields are:

- **Common name (CN):** By default, this is the fully qualified domain name (FQDN) of the server, but it can be any unique name that identifies the server. The length should not exceed 64 characters.
- **IP address:** This is the Crosswork VIP address utilized in this deployment. Additional IP addresses should only be added if necessary for certificate validation.
- **Key Type:** The options are RSA and ECDSA. By default, RSA is selected.
- **Key Size (in bits):** The options are 2048, 3072, and 4096. By default, 2048 is selected.
- **Key Digest:** The options are SHA-256, SHA-384, SHA-224, and SHA-512. By default, SHA-256 is selected.

d) Click **Create CSR** to complete the action.

Step 4 After generating the CSR, click **Download** to download it and use the CSR to get a signed certificate from your CA.

Figure 2: Certificate Signing Request (CSR) page

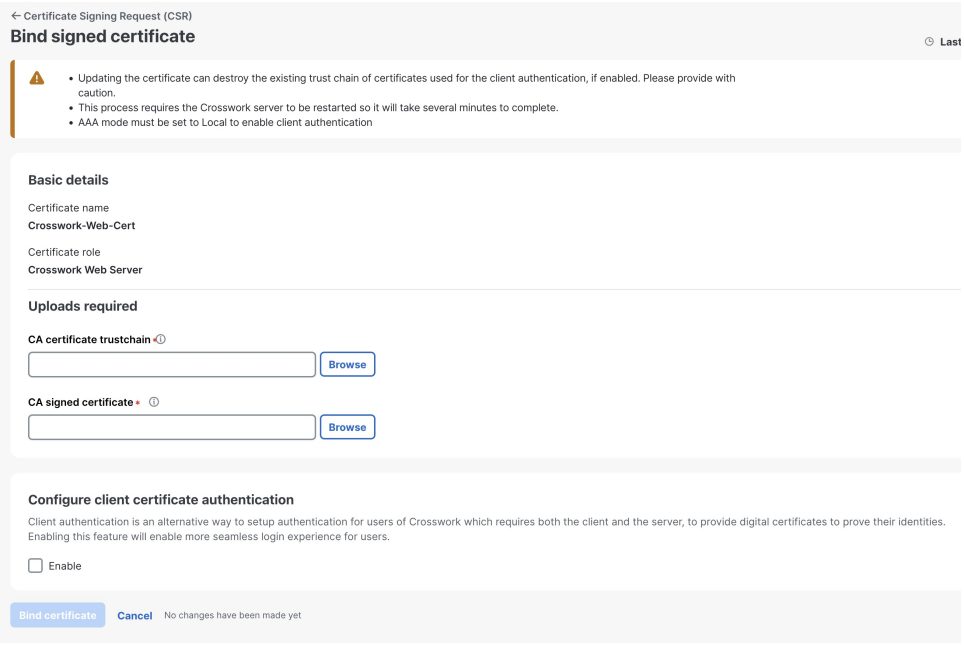


Step 5 Upload the CA-signed certificate and CA certificate trustchain to bind the certificate.

a) In the **Certificate Signing Request (CSR)** window, click **Bind certificate**.

The **Bind signed certificate** window is displayed.

Figure 3: Bind signed certificate



b) Upload the relevant data for the fields provided. Click the ⓘ icon next to the field for more information.

- **CA certificate trustchain:** This is the certificate trust chain for the web server certificate obtained from the CA.
- **CA signed certificate:** This is the final signed certificate for the web server obtained from the CA.

c) (Optional) Click the **Enable** checkbox to configure client certificate authentication.

d) Click **Bind certificate** to complete the operation.

After the bind action is completed, the web certificate is updated, and Tyk will restart with the new web certificate.

Manage users

As a best practice, administrators should create separate accounts for all users. Prepare a list of the people who will use Cisco Crosswork Planning. Decide on their user names and preliminary passwords, and create user profiles for them. During the creation of a user account, you assign a user role to determine the functionality to which the user will have access. If you will be using user roles other than "admin", create the user roles before you add your users (see Create user roles, on page 11).

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To add a new user:

a) Click  and enter the required user details.
b) Click **Save**.

Step 3 To edit a user:

a) Click the checkbox next to the User and click .
b) After making changes, click **Save**.

Step 4 To delete a user:

a) Click the checkbox next to the User and click .
b) In the **Confirm Deletion** window, click **Delete**.

Step 5 To view the audit log for a user:

a) Click the ••• icon under the **Actions** column, and select **Audit log**.

The **Audit Log** window is displayed for the selected user name. For more information, see View audit log, on page 40.

Administrative users created during installation

During installation, Cisco Crosswork Planning creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **`cw-admin`**, and the default password **`admin`**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Crosswork server.
2. The **Cisco Crosswork administrator**, with the username **`admin`** and the default password **`admin`**. Product administrators use this ID to log in to and configure the user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used.

User roles, functional categories and permissions

The **Roles** window lets users with the appropriate privileges define custom user roles. As with the default *admin* role, a custom user role consists of:

- A unique name, such as “Operator” or “admin”.
- One or more selected, named functional categories, which control whether or not a user with that role has access to the APIs needed to perform specific Cisco Crosswork functions controlled by that API.
- One or more selected permissions, which control the scope of what a user with that role can do in the functional category.

For a user role to have access to a functional category, that category and its underlying API must show as selected on the **Roles** page for that role. If the user role shows a functional category as unselected, then users with this role assigned will have no access to that functional area at all.

Some functional categories group multiple APIs under one category name. For example: The “AAA” category controls access to the Password Change, Remote Authentication Servers Integration, and Users and Role Management APIs. With this type of category, you can deny access to some of the APIs by leaving them unselected, while providing access to other APIs under the category by selecting them . For example: If you want to create an “Operator” role who is able to change his own password, but not see or change the settings for your installation’s integration with remote AAA servers, or create new users and roles, you would select the “AAA” category name, but uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” checkboxes.

For each role with a selected category, the **Roles** page also lets you define permissions to each underlying functional API:

- **Read** permission lets the user see and interact with the objects controlled by that API, but not change or delete them.
- **Write** permission lets the user see and change the objects controlled by that API, but not delete them.
- **Delete** permission gives the user role delete privileges over the objects controlled by that API. It is useful to remember that delete permission does not override basic limitations set by the Crosswork platform and it applications.

Although you can mix permissions as you wish:

- If you select an API for user access, you must provide at least “Read” permission to that API.
- When you select an API for user access, Cisco Crosswork assumes that you want the user to have all permissions on that API, and will select all three permissions for you, automatically.
- If you uncheck all of the permissions, including “Read”, Cisco Crosswork will assume that you want to deny access to the API, and unselect it for you.

Best Practices:

Cisco recommends that you follow these best practices when creating custom user roles:

- Restrict **Delete** permissions in roles for *admin* users with explicit administrative responsibility for maintenance and management of the Crosswork deployment as a whole.
- Roles for developers working with all the Cisco Crosswork APIs will need the same permissions as *admin* users.
- Apply at least **Read** and **Write** permissions in roles for users who are actively engaged in managing the network using Cisco Crosswork.
- Give read-only access to roles for users who only need to see the data to help their work as system architects or planners.

The following table describes some sample custom user roles you should consider creating:

Table 1: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager	All	Read, Write

Role	Description	Categories/API	Privileges
Monitor	Monitors alerts only	Cisco Crosswork Planning Design and Collector	Read only
API Integrator	All	All	All

Note Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions.

Create user roles

Local users with administrator privileges can create new users as needed (see Manage users, on page 8).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

The local **admin** role enables access to all functionality. It is created during installation and cannot be changed or deleted. However, its privileges can be assigned to new local users. Only local users can create or update user roles; TACACS, RADIUS and LDAP users cannot.

Follow these steps to create a new user role.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

The **Roles** window has a **Roles** table on the left side and a corresponding **Global API Permissions** tab on the right side which shows the grouping of user permissions for the selected role.

Step 2 On the **Roles** table, click  to display a new role entry in the table.

Step 3 Enter a unique name for the new role.

Step 4 To define the user role's privilege settings, select the **Global API Permissions** tab and perform the following:

a) Check the check box for every API that users with this role can access. The APIs are grouped logically based on their corresponding application.

b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 5 Click **Save** to create the new role.

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (see Edit user roles, on page 12).

Clone user roles

Cloning an existing user role is the same as creating a new user role, except that you need not set privileges for it. If you like, you can let the cloned user role inherit all the privileges of the original user role.

Cloning user roles is a handy way to create and assign many new user roles quickly. Following the steps below, you can clone an existing role multiple times. Defining the cloned user role's privileges is an optional step; you are only required to give the cloned role a new name. If you like, you can assign it a name that indicates the role you want a group of users to perform. You can then edit the user IDs of that group of users to assign them their new role (see Manage users, on page 8). Later, you can edit the roles themselves to give users the privileges you want (see Edit user roles, on page 12).

Note Some API permissions are predefined in the system admin role and remain unchanged in the cloned role. For example, the system admin role includes the default **Read** and **Write** permissions for the **Alarms & Events** API. These permissions are not configurable for both, original, and cloned admin roles.

Follow these steps to clone user roles.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click an existing role.

Step 3 Click to create a new duplicate entry in the **Roles** table with all the permissions of the original role.

Step 4 Enter a unique name for the cloned role.

Step 5 (Optional) Define the role's settings:

a) Check the check box for every API that the cloned role can access.

b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Edit user roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

Follow these steps to edit user roles.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click and select on an existing role from the left side table. The **Global API Permissions** tab on the right side displays the permission settings for the selected role.

Step 3 Define the role's settings:

a) Check the check box for every API that the role can access.

b) For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write**, and **Delete** permissions pre-selected.

Step 4 When you are finished, click **Save**.

Delete user roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

Follow these steps to delete user roles.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click on the role you want to delete.

Step 3 Click .

Step 4 Click **Delete** to confirm that you want to delete the user role.

Global API permissions

The **Roles** window lets users with the appropriate privileges define custom user roles.

The following table is an overview of the various **Global API Permissions** in Cisco Crosswork Planning.

Table 2: Global API permission categories

Category	Global API permissions	Description
AAA	Password Change APIs	Provides permission to manage passwords. The READ and WRITE permissions are automatically enabled by default. The DELETE permission is not applicable to the password change operation. You cannot delete a password, you can only change it.
	Remote Authentication Servers Integration APIs	Provides permission to manage remote authentication server configurations in Cisco Crosswork Planning. You must have READ permission to view/read configuration, and WRITE permission to add/update the configuration of any external authentication server (for example, LDAP, TACACS) into Cisco Crosswork Planning. The Delete permissions are not applicable for these APIs.
	Users and Roles Management APIs	Provides permission to manage users, roles, sessions, and password policies. Supported operations include "Create new user/role", "Update user/role", "Delete a user/role", "Update task details for a user/role", "Session management (Idle-timeout, max session)", "update password policy", "get password tooltip help text", "get active sessions", and so on. The READ permission allows you to view the content, the WRITE permission allows you to create and update, and the DELETE permission allows you to delete a user or role.
Administrative Operations	Diagnostic Information APIs	
Alarms and Events	Alarms and Events APIs	Allows you to manage system alarms. **Note** The alarms and events associated with the Cisco Crosswork Planning applications are not supported.
Crosswork Planning		

Category	Global API permissions	Description
Platform	Platform APIs	The READ permission allows you to fetch the server status, Cisco Crosswork Planning node information, application health status, collection job status, certificate information, backup and restore job status, and so on. The WRITE permission allows you to • Enable/disable the xFTP server • Manage node information (set the login banner, restart a microservice, and so on) • Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, and so on) • Perform normal/data-only backup and restore operations. • Manage applications (activate, deactivate, uninstall, add package, and so on) The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.
	View APIs	Views Management in Cisco Crosswork Planning Design. The READ permission allows you to see views, the WRITE permission allows you to create/update views, and the DELETE permission will enable delete capabilities.

Manage active sessions

As an administrator, you can monitor and manage the active sessions in the Cisco Crosswork Planning UI, and perform the following actions:

- Terminate a user session
- View user audit log

Attention

- Non-admin users with permission to terminate can terminate their own sessions.
- Non-admin users with read-only permission can only collect the audit log for their sessions.
- Non-admin users without read permissions can't view the Active sessions window.

Procedure

Step 1 From the main menu, choose the **Administration** > **Users and Roles** > **Active sessions** tab.

The Active sessions tab displays all the active sessions in the Cisco Crosswork Planning with details such as user name, login time, and login method.

Note
The **Source IP** column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork Planning. This option is available in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.

Step 2 To terminate a user session, click the ••• icon under the **Actions** column, and select **Terminate**. A dialog box is displayed to confirm your action. Select **Terminate** to terminate the session.

Attention
- You are recommended to use caution while terminating a session. A user whose session is terminated will not receive any prior warning and will lose any unsaved work.
- Any user whose session is terminated will see the following error message: `"Your session has ended. Log into the system again to continue"`.

Step 3 To view audit log for a user, click the ••• icon under the **Actions** column, and select **Audit log**.

The Audit Log window is displayed for the selected user name. For more information on the Audit Logs, see View audit log, on page 40.

Set up user authentication (TACACS+, LDAP, and RADIUS)

In addition to supporting local users, Cisco Crosswork Planning supports TACACS+, LDAP, and RADIUS users through integration with the TACACS+, LDAP, and RADIUS servers.



Caution Please note that any operation you do following the instructions in this section will affect all new logins to the Crosswork user interface. To minimize session interruption, Cisco recommends that you perform all your external server authentication changes and submit them in a single session.

The integration process has these steps:

- Configure the TACACS+, LDAP, and RADIUS servers.
- Create the roles that are referenced by the TACACS+, LDAP, and RADIUS users.
- Configure AAA settings.
- You can also enable Single Sign-on (SSO) for authentication of TACACS+, LDAP, and RADIUS users. For more information, see Enable Single Sign-on (SSO), on page 27.

Note

- The AAA server page works in bulk update mode wherein all the servers are updated in a single request. It is advised to give write permission for "Remote Authentication Servers Integration API" only to users who have the relevant authorization to delete the servers.
- A user with only Read and Write permissions (without 'Delete' permission) can delete the AAA server details from Cisco Crosswork since delete operations are part of 'Write' permissions. For more information, see Create user roles, on page 11.
- While making changes to AAA servers (create/edit/delete), you are recommended to wait for few minutes between each change. Frequent AAA changes without adequate intervals can result in external login failures.

Manage TACACS+ servers

Cisco Crosswork Planning supports the use of TACACS+ servers to authenticate users.

You can integrate Crosswork with a standalone server (open TACACS+) or with an application such as Cisco ISE (Identity Service Engine) to authenticate using the TACACS+ protocols.

Before you begin

- Configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the TACACS+ server (standalone or Cisco ISE), before configuring the AAA server in Cisco Crosswork Planning. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **TACACS+** tab. From this window, you can add, edit, and delete a new TACACS+ server.

Step 2 **To add a new TACACS+ server**:

a) Click the + icon.

b) Enter the required TACACS+ server information.

Table 3: TACACS+ field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS name	Enter the DNS name (if DNS name is selected). Only IPv4 DNS name is supported.

Field	Description
Port	The default TACACS+ port number is 49.
Shared secret format	Shared secret for the active TACACS+ server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active TACACS+ server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the TACACS+ server.
Service	Enter value of the service that you are attempting to gain access to. For example, "`raccess`". This field is verified only for standalone TACACS+. In case of Cisco ISE, you can enter a junk value. Do not leave the field blank.
Policy ID	Enter the user role that you created in the TACACS+ server. **Note** If you try to log in to Cisco Crosswork Planning as a TACACS+ user before creating the required user role, you will get the error message: "`Key not authorized: no matching policy`". If this occurs, close the browser. Log in as a local admin user and create the missing user roles in the TACACS+ server, and log in back to Cisco Crosswork Planning using the TACACS+ user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the (ISE/Standalone) TACACS+ server attributes. These values can be one or more comma-separated entries. In the TACACS+ context, the Device Access Group attribute is typically a custom or authorization attribute that the TACACS+ server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for TACACS+: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

See the example at the end of this topic for more details.

c) After you enter all the relevant details, click **Add**.

d) Click **Save all changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save changes** to confirm.

Step 3 **To edit a TACACS+ server**:

a) Click the check box next to the TACACS+ server and click .
b) After making changes, click **Update**.

Step 4 **To delete a TACACS+ server**:

a) Click the check box next to the TACACS+ server and click . The Delete *server-IP-address* dialog box opens.
b) Click **Delete** to confirm.

Manage LDAP servers

Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. Cisco Crosswork Planning supports the use of LDAP servers (OpenLDAP, Active Directory, and secure LDAP) to authenticate users. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

To use secure LDAP protocol, you must add **Secure LDAP Communication** certificate before adding the LDAP server. For more details on adding certificates, see Add new certificates, on page 3.

Before you begin

- Configure the relevant parameters (Bind DN, Policy baseDN, Policy ID, and so on) in the LDAP server before configuring the AAA server in Cisco Crosswork Planning.

Procedure

Step 1 From the main menu, choose the **Administration** > **AAA** > **Servers** > **LDAP** tab. Using this window, you can add, edit, and delete a new LDAP server.

Step 2 **To add a new LDAP server**:

a) Click the icon.
b) Enter the required LDAP server details.

Table 4: LDAP field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
Name	Name of the LDAP handler.
IP address/ Host name	LDAP server IP address or host name

Field	Description
Secure connection	Enable the **Secure Connection** toggle button if you want to connect to the LDAP server via the SSL communication. When enabled, select the secure LDAP certificate from the **Certificate** drop-down list. **Note** The secure LDAP certificate must be added in the Certificate Management screen prior to configuring the secure LDAP server. This field is disabled by default.
Port	The default LDAP port number is 389. If Secure Connection SSL is enabled, the default LDAP port number is 636.
Bind DN	Enter the login access details to the database. Bind DN allows user to log in to the LDAP server.
Bind credential / Confirm bind credential	Username and password to login to the LDAP server.
Base DN	Base DN is the starting point used by the LDAP server to search for user authentication within your directory.
User filter	The filter for user search.
DN format	The format used to identify the user in base DN.
Principal l ID	This value represents the UID attribute in the LDAP server user profile under which a particular username is organized.
Policy baseDN	This value represents the role mapping for user roles within your directory.
Policy map attribute	This helps in identifying the user under the policy base DN. This value maps to the `userFilter` parameter in your LDAP server attributes.
Policy ID	The **Policy ID** field corresponds to the user role that you created in the LDAP server. **Note** If you try to log in to Cisco Crosswork Planning as an LDAP user before creating the required user role, you will get the error message: `"Login failed, policy not found. Please contact the Network Administrator for assistance."`. To avoid this error, ensure to create the relevant user roles in the LDAP server, before setting up a new LDAP server in Cisco Crosswork Planning.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the LDAP server attributes. These values can be one or more comma-separated entries. In the LDAP context, the Device Access Group attribute is typically a custom or authorization attribute that the LDAP server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.

Field	Description
Connection timeout	Enter the timeout value. Maximum timeout is 30 seconds.

See the example at the end of this topic for more details.

c) Click **Add**.
d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Step 3 **To edit an LDAP server**:

a) Select the LDAP server and click .
b) After making changes, click **Update**.

Step 4 **To delete an LDAP server**:

a) Select the LDAP server and click .
b) Click **Delete** to confirm.

Example

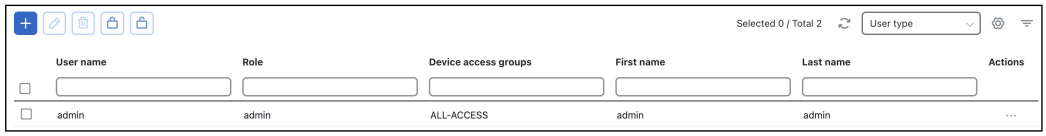
This example shows the parameters that are entered for secure LDAP configuration in Cisco Crosswork Planning. The relevant parameters are configured in the LDAP server.

These are some of the key points:

User settings in the Cisco Crosswork Planning UI

In this example, the existing default user role **admin** is used. You can find this setting on the **Administration** > **Users and Roles** > **Users** page.

- The user name, user role, first name, and last name are set to `admin`.
- The device access group is configured in the LDAP server as `description='ALL-ACCESS'`.



LDAP server details

This section describes the user's LDAP server configuration details.

1. System base DN: ou=system
2. The admin user ‘admin’ has these attributes:
   a. DN: uid=admin,ou=system
   b. password: secret
3. Users group with DN: ou=users,ou=system

4. The admin user John belongs to the ‘users’ group and has these attributes:
   a. DN: uid=john,ou=users,ou=system
   b. password: john
   c. mail: John@test.com
   d. display name: John
   e. description: ALL-ACCESS



Important The description must be equal to the **Device access groups** value for the 'admin' user in Cisco Crosswork Planning (see User settings in the Cisco Crosswork Planning UI, on page 21).

5. The group ‘CpAdmins’ has these attributes:
   a. DN: cn=CpAdmins,ou=groups,ou=system
   b. uniqueMember=uid=john,ou=users,ou=system

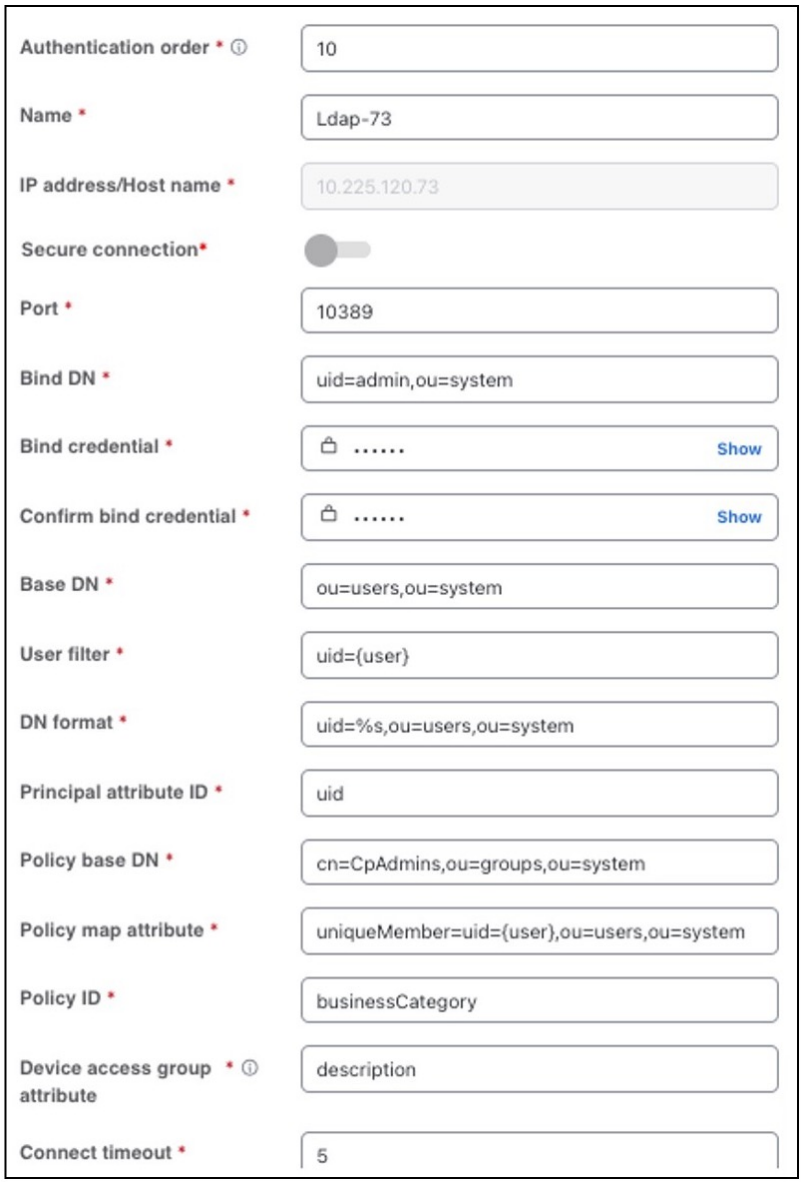
      This indicates the user’s group membership. This value must match with admin user’s DN (see Section 4(a)).
   c. businessCategory: admin

      This indicates the role that needs to be assigned to all users belonging to this group. This value must match with the **Role** value for the admin user in Cisco Crosswork Planning (see User settings in the Cisco Crosswork Planning UI, on page 21).

Corresponding LDAP configuration in the UI

This section describes the corresponding LDAP configuration in the Cisco Crosswork Planning UI.

Figure 4: LDAP configuration in the Cisco Crosswork Planning UI



Parameter	Value
Authentication order	10 (default)
Name	Ldap-73 Custom name for the LDAP configuration of a server.
IP Address/Host name	10.225.120.73 LDAP server IP address.

Parameter	Value
Port	10389 LDAP server port.
Bind DN	uid=admin,ou=system Admin user DN, as described in Section 2(a).
Bind credential	secret Admin user password, as described in Section 2(b).
Confirm bind credential	secret Admin user password, as described in Section 2(b).
Base DN	ou=users,ou=system The user's group DN for *authentication* from where the users must be searched, as described in Section 3.
User filter	uid={user} User search filter attribute 'uid', as described in Section 4.
DN format	uid=%s,ou=users,ou=system User's DN format, as described in Section 4.
Principal attribute ID	uid As described in Section 4.
Policy base DN	cn=CpAdmins,ou=groups,ou=system The group that has the role mapping attribute (admin) and under which the users will have group membership, as described in Section 5(a).
Policy map attribute	uniqueMember=uid={user},ou=users,ou=system The user's group membership attribute under the 'CpAdmins' user group (Policy base DN), as described in Section 5(b).
Policy ID	businessCategory The user role attribute (admin) under the 'CpAdmins' group (Policy base DN), as described in Section 5(c). This value must match with the CpAdmins group's attribute having 'admin' value.
Device access group attribute	description The device group attribute under the user DN, as described in Section 4(e). This value must match with the user DN attribute having value 'ALL-ACCESS'.

Manage RADIUS servers

Crosswork supports the use of RADIUS (Remote Authentication Dial-In User Service) servers to authenticate users. You can also integrate Crosswork with an application such as Cisco ISE (Identity Service Engine) to authenticate using the RADIUS protocols.

Before you begin

- Similar to TACACS+ server, you must configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the RADIUS server before configuring the AAA server in Cisco Crosswork Planning. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **RADIUS** tab. From this window, you can add, edit, and delete a new RADIUS server.

Step 2 **To add a new RADIUS server**:

a) Click the + icon.

b) Enter the required RADIUS server information.

Table 5: RADIUS field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the RADIUS server (if IP address is selected).
DNS name	Only IPv4 DNS name is supported (if DNS name is selected).
Port	The default RADIUS port number is 1645.
Shared secret format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active RADIUS server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Cisco Crosswork Planning to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the RADIUS server.
Service	Enter value of the service that you are attempting to gain access to. For example, "`raccess`".

Field	Description
Policy ID	The **Policy Id** field corresponds to the user role that you created in the RADIUS server. **Note** If you try to login to Cisco Crosswork Planning as a RADIUS user before creating the required user role, you will get the error message: `"Key not authorized: no matching policy"`. If this occurs, close the browser. Log in as a local admin user and create the missing user roles in the RADIUS server, and log in back to Cisco Crosswork Planning using the RADIUS user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the RADIUS server attributes. These values can be one or more comma-separated entries. In the RADIUS context, the Device Access Group attribute is typically a custom or authorization attribute that the RADIUS server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy ID to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for RADIUS: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

As RADIUS configuration is very similar to TACACS+, please refer to the detailed example in the Manage TACACS+ servers, on page 17 for more information.

c) After you enter all the relevant details, click **Add**.
d) Click **Save all changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save changes** to confirm.

Step 3 **To edit a RADIUS server**:

a) Click the checkbox next to the RADIUS server and click .
b) After making changes, click **Update**.

Step 4 **To delete a RADIUS server**:

a) Click the checkbox next to the RADIUS server and click . The Delete *server-IP-address* dialog box opens.
b) Click **Delete** to confirm.

Enable Single Sign-on (SSO)

Single Sign-on (SSO) is an authentication method that allows you to log in with a single ID and password to any of several related, yet independent, software systems. It allows you to log in once and access the services without reentering authentication factors. Cisco Crosswork acts as Identity Provider (IDP) and provides authentication support for the relying service providers. You can also enable SSO for authentication of TACACS+, LDAP, and RADIUS users.

Crosswork supports SSO cross-launch to enable easier navigation with the service provider. Once configured, the URL can be launched using the launch icon ( ) located at the top right corner of the window.

Attention

- When Crosswork is re-installed or migrated, you must ensure that the latest IDP metadata from Crosswork is updated to the service provider applications. Failing to do this will result in authentication failure due to mismatched metadata information.
- First-time login users cannot switch to using a different username before mandatorily changing the password. The only workaround is for the administrator to terminate the session.

Note The Cisco Crosswork Planning login page is not rendered when the Central Authentication Service (CAS) pod is restarting or not running.

Before you begin

Ensure that the **Enable source IP for auditing** check box is selected in the **Administration** > **AAA** > **Settings** page.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **SSO**. The **Identity Provider** window is displayed. Using this window, you can add, edit settings, and delete service providers.

Step 2 **To add a new service provider**:

a) Click the icon.

b) In the **Service Provider** window, enter the values in the following fields:

- **Name**: Enter the name of the service provider entity.

  Note
  If a URL is provided, the **Service name** column entry in the **Identity Provider** window becomes a hyperlink.

- **Evaluation Order**: Enter a unique number which indicates the order in which the service definition should be considered.
- **Metadata**: Click the field, or click **Browse** to navigate to the metadata XML document that describes a SAML client deployment. You can also enter the service provider URL here for cross-launch.

Step 3 Click **Add** to finish adding the service provider.

Step 4 Click **Save all changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save changes** to confirm.

After the settings are saved, when you log into the integrated service provider application for the first time, the application gets redirected to the Cisco Crosswork server. After providing the Crosswork credentials, the service provider application logs in automatically. For all the subsequent application logins, you do not have to enter any authentication details.

Step 5 **To edit a service provider:**

a) Click the check box next to the service provider and click . You can update the Evaluation Order and Metadata values as required.
b) After making changes, click **Update**.

Step 6 **To delete a service provider**:

a) Click the check box next to the service provider and click .
b) Click **Delete** to confirm.

Configure AAA settings

Users with relevant AAA permissions can configure the AAA settings.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **Settings**.

Step 2 Select the relevant setting for **Fallback to Local**. By default, Cisco Crosswork Planning prefers external authentication servers over local database authentication.

Note
Admin users are always authenticated locally.

Step 3 Select the relevant value for the **Logout all idle users after** field. Any user who remains idle beyond the specified limit will be automatically logged out.

Note
The default timeout value is 30 minutes. If the timeout value is adjusted, the page will refresh to apply the change.

Step 4 Enter relevant values in the **Number of parallel sessions** and **Number of parallel sessions per user** fields.

Note
Crosswork supports between 5 to 200 parallel sessions for concurrent users. If the number of parallel sessions is exceeded, an error is displayed while logging in to Crosswork.

Note
Crosswork supports 50 simultaneous NBI sessions up to 400 sessions.

Step 5 Check the **Enable source IP for auditing** check box to log the IP address of the user (source IP) for auditing and accounting. This check box is disabled by default. Once you enable this option and relogin to Cisco Crosswork Planning, you will see the **Source IP** column on the **Audit Log** and **Active Sessions** pages.

Step 6 Select the relevant settings for the **Local password policy**. Certain password settings are enabled by default and cannot be disabled (for example, Change password on first login).

Note
Any changes in the password policy are enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

Note
Local password policy allows administrators to configure the number of unsuccessful login attempts a user can make before they are locked out of Cisco Crosswork Planning, and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

Monitor system and application health

The Cisco Crosswork Platform is built on an architecture consisting of microservices. Due to the nature of these microservices, there are dependencies across various services within the Crosswork system. The system and applications are considered Healthy if all services are up and running. If one or more services are down, then the health is considered Degraded. If all services are down, then the health status is Down.

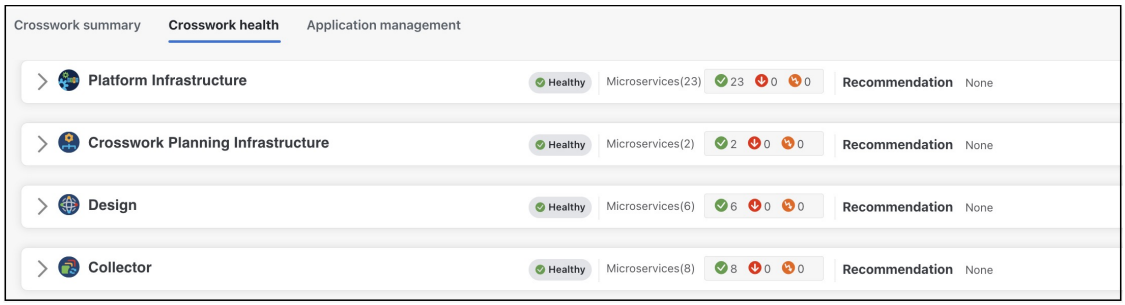
From the main menu, choose **Administration** > **Crosswork Manager** to access the **Crosswork summary** and **Crosswork health** windows. Each window provides various views to monitor system and application health. It also supplies tools and information that, with support and guidance from your Cisco Customer Experience account team, you can use to identify, diagnose, and fix issues with the Cisco Crosswork, Platform Infrastructure, and installed applications.

While both windows can give you access to the same type of information, the purpose of each summary and view is different.

Monitor platform infrastructure and application health

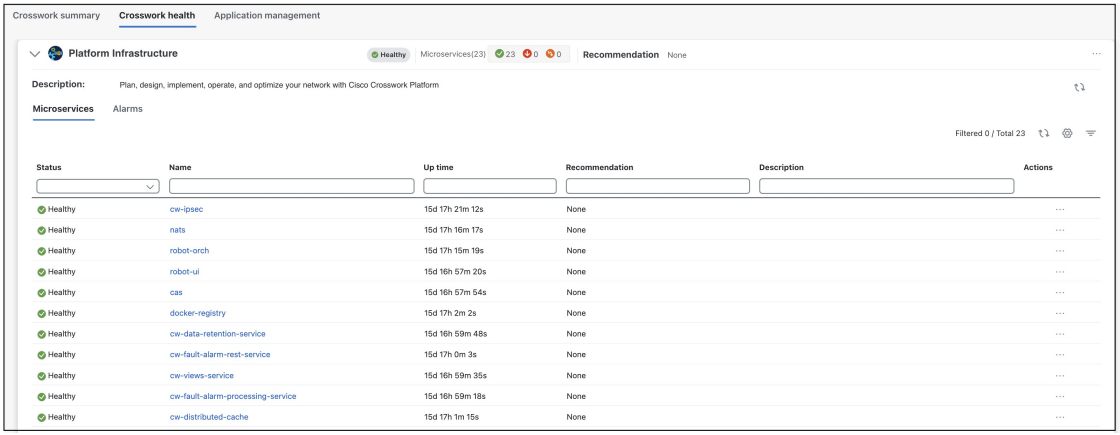
The **Crosswork health** window (**Administration** > **Crosswork Manager** > **Crosswork health** tab) provides health summaries for the Cisco Crosswork Platform Infrastructure and installed applications with the addition of microservice status details.

Figure 5: Crosswork health tab



Within this window, expand an application row to view Microservice and Alarm information.

Figure 6: Microservices tab



From the **Microservices** tab:

- View the list of microservices and, if applicable, associated microservices by clicking on the microservice name.
- Click ••• to restart or obtain Showtech data and logs per microservice.

Note Showtech logs must be collected separately for each application.

From the **Alarms** tab, you can:

- Filter the active alarms.
- Click the alarm description to drill down on alarm details.
- Change status of the alarms (Acknowledge, Unacknowledge, Clear).
- Add notes to alarms.
- View list of events in the product.
- View the correlated alarm for each event.

Check system health example

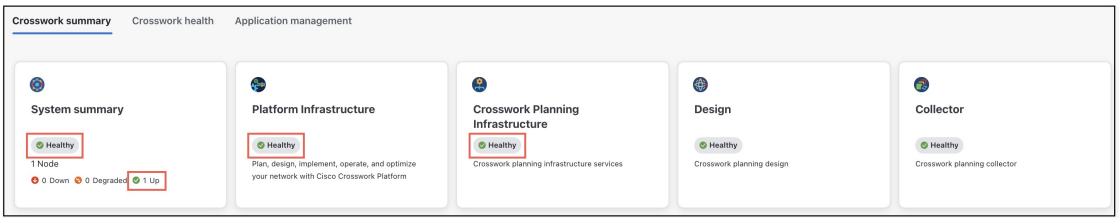
In this example, we navigate through the various windows and what areas should be checked for a healthy Crosswork system.

Procedure

Step 1 Check overall system health.

a) From the main menu, choose the **Administration** > **Crosswork Manager** > **Crosswork summary** tab.
b) Check that all the nodes are in Operational state (Up) and that the System Summary, Platform Infrastructure, and Crosswork Planning Infrastructure are Healthy.

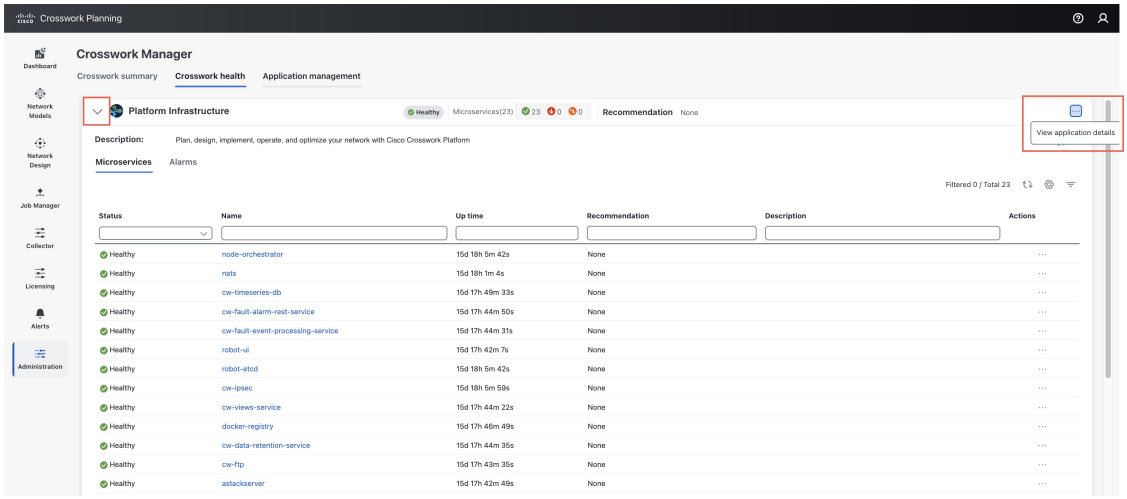
Figure 7: Crosswork summary tab



Step 2 Check and view detailed information about the microservices that are running as part of the Crosswork Platform Infrastructure.

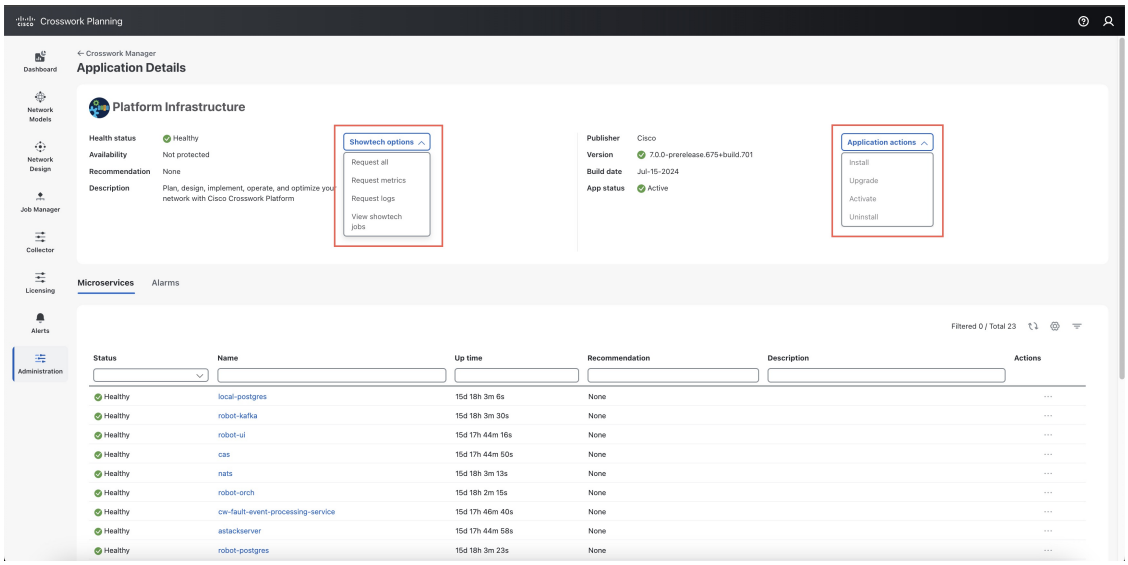
a) Click the **Crosswork health** tab.
b) Expand the Crosswork Platform Infrastructure row, click ***, and select **View application details**.

Figure 8: Crosswork health tab



c) From the Application Details page, you can check and review microservice details, restart microservices, and collect showtech information. You can also perform installation-related tasks from this window.

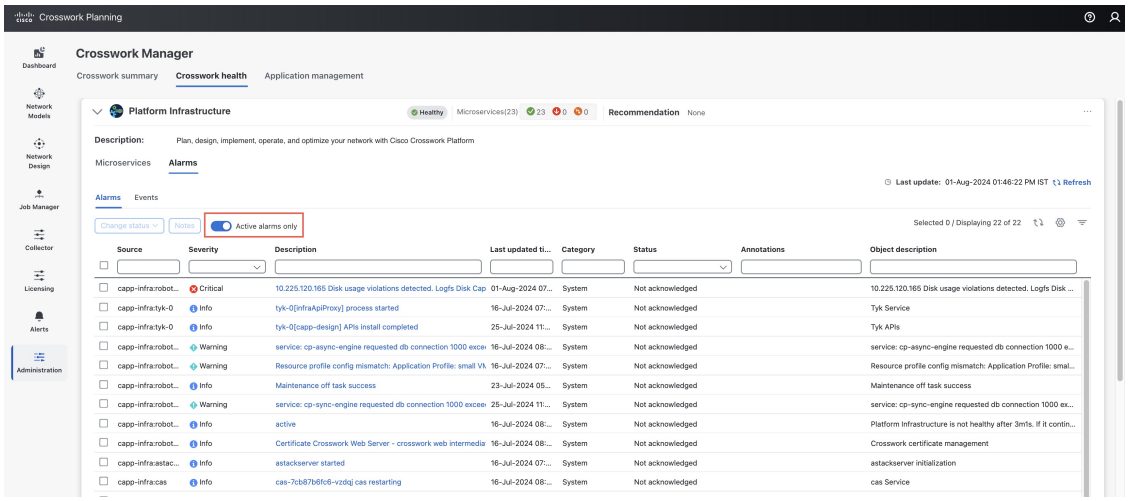
Figure 9: Application Details page



Step 3 Check and view the alarms and events related to the microservices.

a) Click the **Alarms** tab. The list only displays Crosswork Platform Infrastructure alarms. You can further filter the list by viewing only active alarms.

Figure 10: Alarms tab

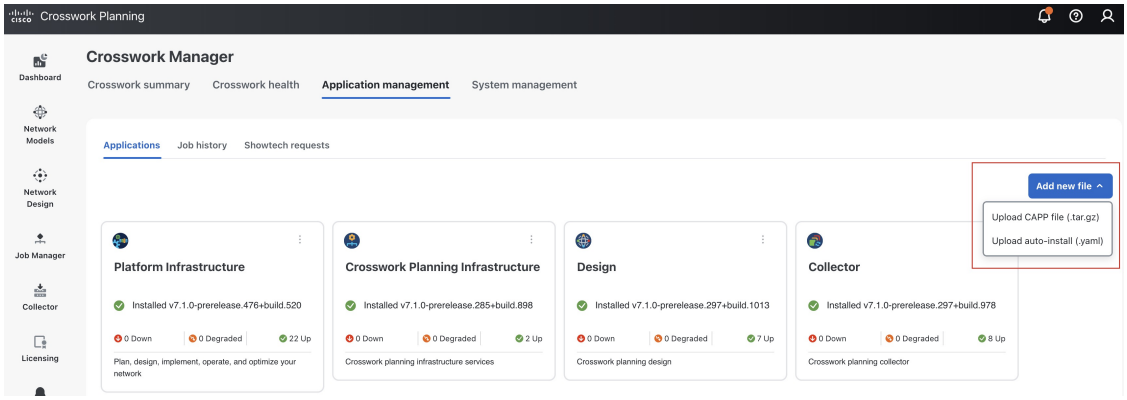


b) Click the **Events** tab. The list displays all Crosswork Platform Infrastructure events, and their correlated alarms.

Step 4 View which Crosswork applications are installed.

a) From the main menu, choose **Administration** > **Crosswork Manager** > **Application management** tab and click **Applications**. This page displays all applications that have been installed. You can also click **Add new file** to install more applications by uploading another application bundle or an auto-install file.

Figure 11: Application management window



Step 5 View the status of jobs.

a) Click the **Job History** tab. This window provides the information regarding the status of jobs and the sequence of events that have been executed as part of the job process.

Manage backups

Backup and restore overview

Cisco Crosswork Planning's backup and restore features help prevent data loss and preserve your installed applications and settings.

Cisco Crosswork Planning offers multiple menu options to backup and restore your data.

From the main menu, click **Administration** > **Backup and Restore** to access the **Backup and Restore** window.

Table 6: Backup and restore options

Menu option	Description
Actions > Data backup (See Manage backup and restore, on page 34 for details)	Preserves the Cisco Crosswork Planning configuration data. The backup file can be used with the data disaster restore (Restore Cisco Crosswork Planning after a disaster, on page 37) to recover from a serious outage.
Actions > Data disaster restore (See Restore Cisco Crosswork Planning after a disaster, on page 37 for details)	Restores the Cisco Crosswork Planning configuration data after a natural or human-caused disaster has required you to rebuild a Cisco Crosswork Planning server.

Menu option	Description
Actions > Data migration (see Migrate data using backup and restore, on page 38 for details)	Migrates data from an older version of Cisco Crosswork Planning to a newer version.

Manage backup and restore

This section explains how to perform a data backup and restore operation from the Cisco Crosswork Planning UI.

Attention

- Building a target machine for the backup is out of scope for this document. The operator is expected to have the server in place, to know the credentials for the server, and to have a target directory with adequate space for the backups in place.
- Cisco Crosswork Planning does not manage the backups. It is up to the operator to periodically delete old backups from the target server to make room for future backups.
- The backup process depends on having SCP access to a server with sufficient amount of storage space. The storage required for each backup will vary based on the applications in the Cisco Crosswork Planning server and the scale requirements.
- The time taken for the backup or restore processes will vary based on the type of backup and the applications in the Cisco Crosswork Planning server.

When creating or restoring backups for Cisco Crosswork Planning, follow these guidelines:

- Configure a destination SCP server for storing backup files during your first login. This is a one-time setup and must be completed before taking backups or initiating restore operations.
- Perform backup or restore operations during a scheduled maintenance window. You should not access the system during these operations. Backups will take the system offline for about 10 minutes, while restore operations can be lengthy and pause other applications, affecting data-collection jobs.
- Use the same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- Use the dashboard to monitor the progress of backup or restore processes. Avoid using the system during these processes to prevent errors or incorrect content.
- Only one backup or restore operation can run at a time.
- Ensure both Cisco Crosswork Planning and the SCP server are in the same IP environment (for example, both using IPv6).
- Delete older backups to save space on the backup server, though they may still appear in the job list.
- Operators making frequent changes should back up more often (possibly daily), while others might back up weekly or before major system upgrades.

- By default, backups are not allowed if the system is not considered healthy, but this can be overridden for troubleshooting purposes.
- If using collector agents, manually restart them, as they may remain in a stopped state after the backup and restore operation.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of the secure SCP server. Ensure that the server has sufficient storage available.
- A file path on the SCP server, to use as the destination for your backup files.
- User credentials for an account with file read and write permissions to the remote path on the destination SCP server.
- Made a note of the build version of the installed applications. Before performing the data restore, you must install the exact versions of those applications. Any mismatch in the build versions of the applications can result in data loss and failure of the data restore job.

Procedure

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** drawer panel. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create a backup:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data backup** to display the **Data Backup** drawer panel with the destination server details pre-filled.
c) Provide a relevant name for the backup in the **Job name** field.
d) If the VM or any of the applications are not in Healthy state, but you want to create the backup, check the **Force** check box.

Note
The **Force** option must be used only after consultation with the Cisco Customer Experience team.

e) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host name**, **Port**, **Username**, **Password** and **Server path/Location** fields to specify a different destination.

f) (Optional) Click **Verify backup readiness** to verify that Cisco Crosswork Planning has enough free resources to complete the backup. If the check is successful, Cisco Crosswork Planning displays a warning about the time-consuming nature of the operation. Click **OK** to continue.

If the verification is unsuccessful, contact the Cisco Customer Experience team for assistance.

g) Click **Backup** to start the backup operation. Cisco Crosswork Planning creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.

h) To view the progress of a backup job, enter the job details (such as Status or Job Type) in the search fields in the **Backup restore job sets** table. Then, click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job name, and Job type. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note
After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.

Note
If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

i) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note
Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task `uploadBackupToRemote`). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Step 3 **To restore from a backup file:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) In the **Backup and Restore Job Sets** table, select the data backup file to be used for the restore. The **Job Details** panel shows information about the selected backup file.
c) With the backup file selected, click the **Data Restore** button shown on the **Job Details** panel to start the restore operation. Cisco Crosswork Planning creates the corresponding restore job set and adds it to the job list.

To view the progress of the restore operation, click the link to the progress dashboard.

Recommendation: Post-restore actions

After the restore process completes, ensure these actions are performed to resume normal system operations:

Editing collections

After restoring the backup, navigate to the **Collector** > **Collections** page and perform the Edit collection operation on each listed collection. Save the collections without making any changes. This ensures that the configuration data is properly updated.

Restarting agents

The restore process only copies the database and file system data. Once the restore process completes, all agents will be in a stopped state, and you must restart them manually from the Cisco Crosswork Planning UI.

- Restart the NetFlow and SR-PCE agents using the **Start** option for the respective agent in the **Setup Agent** page (**Collector** > **Agents**). For more information, see Agent operations.
- Restart the traffic poller agent by disabling and then enabling the **Traffic collection** option on the Traffic collector configuration page. For more information, see Collect traffic statistics.

Executing schedulers

- If using a "Run now" scheduler, execute the scheduler manually.
- If the scheduler has a CRON job configured, then the scheduler triggers automatically based on the CRON job configuration.

Restore Cisco Crosswork Planning after a disaster

A disaster recovery is a restore operation that you use after a natural or human-caused disaster has destroyed a Cisco Crosswork Planning server. You must deploy a new server first, following the instructions in *Cisco Crosswork Planning 7.1 Installation Guide*.

To perform a disaster recovery:

Before you begin

- Obtain the full name of the backup file you want to use in your disaster recovery from the SCP backup server. Typically, this will be the most recent backup file you have created. Cisco Crosswork Planning backup file names typically follow this format:

  `backup_`*`JobName_CWVersion_TimeStamp`*`.tar.gz`

  Where:

  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the Cisco Crosswork Planning platform version of the backed-up system.
  - *TimeStamp* is the date and time when Cisco Crosswork Planning created the backup file.

  For example: `backup_Wednesday_4-0_2021-02-31-12-00.tar.gz`.

- Install the exact versions of the applications that were present in your old Cisco Crosswork Planning server when the data backup was made. Any version mismatch can lead to data loss and restore job failure.
- Use the same Cisco Crosswork Planning software image that was used when creating the backup. You cannot restore the cluster using a backup created with a different software version.
- Keep your backups up-to-date to ensure you can recover the system's true state as it existed before the disaster. If you have installed new applications or patches since your last backup, take another backup.
- If the disaster recovery fails, contact Cisco Customer Experience.
- Smart Licensing registration for Crosswork applications are not restored during a disaster restore operation, and must be registered again.

Procedure

Step 1 From the main menu of the newly deployed Cisco Crosswork Planning server, choose **Administration** > **Backup and Restore**.

Step 2 Click **Actions** > **Data disaster restore** to display the **Data Disaster Restore** dialog box with the remote server details pre-filled.

Step 3 In the **Backup file name** field, enter the file name of the backup from which you want to restore.

Step 4 Click **Start restore** to initiate the recovery operation.

To view the progress of the operation, click the link to the progress dashboard.

Migrate data using backup and restore

Using data migration backup and restore is a prerequisite when upgrading your Cisco Crosswork Planning installation to a new software version, or moving your existing data to a new installation.

Follow these guidelines whenever you create a data migration backup:

- Ensure that you have configured a destination SCP server to store the data migration files. This configuration is a one-time activity.
- Both the Cisco Crosswork Planning and the SCP server must be in the same IP environment. For example, if Cisco Crosswork Planning is communicating over IPv6, so must the backup server.
- We recommend that you create a data migration backup only when upgrading your Cisco Crosswork Planning installation, and that you do so during a scheduled upgrade window only. Users shouldn't attempt to access Cisco Crosswork Planning while the data migration backup or restore operations are running.

Before you begin

Ensure that you have

- the hostname or IP address and the port number of a secure destination SCP server
- a file path on the SCP server, to use as the destination for your data migration backup files, and
- user credentials for an account with file read and write permissions to the remote path on the destination SCP server.

Procedure

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Add Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create a backup:**

a) Log in as an administrator to the Cisco Crosswork Planning installation whose data you want to migrate to another installation.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data backup** to display the **Data Backup** dialog box with the destination server details prefilled.

d) Provide a relevant name for the backup in the **Job Name** field.
e) If you want to create the backup despite any microservice issues, check the **Force** check box.
f) Complete the remaining fields as needed.

   If you want to specify a different remote server upload destination: Edit the pre-filled **Host name**, **Port**, **Username**, **Password** and **Server path/Location** fields to specify a different destination.

g) Click **Backup** to start the backup operation. Cisco Crosswork Planning creates the corresponding backup job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.
h) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

   The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

i) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

   If the upload failed due to problems with the remote server, use the **Destination** button to specify a different remote server and path before clicking **Upload backup**.

Step 3 **Migrate the backup to the new installation:**

a) Log in as an administrator on the Cisco Crosswork Planning installation to which you want to migrate data from the backup.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data migration** to display the **Data Migration** dialog box with the remote server details pre-filled.
d) In the **Backup file name** field, enter the file name of the backup from which you want to restore.
e) Click **Start migration** to initiate the data migration. Cisco Crosswork Planning creates the corresponding migration job set and adds it to the job list.

   To view the progress of the data migration operation, click the link to the progress dashboard.

View system and network alarms

You can view alarms by navigating to one of the following:

- From the main menu, choose **Alerts** > **Alarms and Events**.
- For application specific alarms, choose **Administration** > **Crosswork Manager** > **Crosswork Health** tab. Expand one of the applications and select the **Alarms** tab.

  From the **Alarms** tab, you can:

  - Click the alarm description to drill down on alarm details.
  - Change the status of the alarms (Acknowledge, Unacknowledge, Clear). Select the alarm and select the required status from the **Change status** drop-down.
  - Add notes to alarms. Select the alarm and click the **Notes** button.

View audit log

The **Audit Log** window tracks the following AAA-related events:

- Create, update, and delete users
- Create, update, and delete roles
- User login activities - login, logout, login failure due to maximum active session limit, and account locked due to maximum login failures.
- Source IP - IP address of the machine from where the action was performed. This column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork Planning. This check box is available in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.
- Password modification by user

To view the audit log, perform the following steps:

Procedure

Step 1 From the main menu, choose **Administration** > **Audit Log**.

The Audit Log window is displayed.

Step 2 Click to filter the results based on your query.

Using the export icon ( ), you can export the log in the CSV format. When exporting the CSV, you have the option to use the default file name or enter a unique name.

Set the pre-login disclaimer

Many organizations require that their systems display a disclaimer message in a banner before users login. The banner reminds the authorized users of their obligations when using the system, or provides warnings to unauthorized users. You can enable such a banner for Cisco Crosswork Planning users, and customize the disclaimer message as needed.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings**.

Step 2 Under **Notifications**, click the **Pre-login disclaimer** option.

Step 3 To enable the disclaimer and customize the banner:

a) Check the **Enable** check box.

b) Customize the banner **Title**, the **Icon**, and the **Disclaimer text** as needed.

c) (Optional) Check the **Enable** check box under **Require user consent** to prompt the user to agree to the disclaimer before they log in.
d) (Optional) While editing the disclaimer, you can:
   - Click **Preview** to see how your changes look when displayed before the Crosswork login prompt.
   - Click **Discard changes** to revert to the last saved version of the banner.
   - Click **Reset to default** to revert to the original, default version of the banner.
e) When you are satisfied with your changes, click **Save** to save them and enable display of the custom disclaimer to all users.

Step 4 To turn off the disclaimer display, select **Administration** > **Settings** > **Pre-login disclaimer**, then uncheck the **Enable** check box.

Manage maintenance mode settings

The maintenance mode provides a means for shutting down the Cisco Crosswork Planning system temporarily. Cisco Crosswork Planning synchronizes all application data before the shutdown. It can take several minutes for the system to enter maintenance mode and to restart when maintenance mode is turned off. During these periods, you should not attempt to log in or use the Cisco Crosswork Planning applications.

Caution
- Make a backup of your Cisco Crosswork Planning system before enabling the maintenance mode.
- Notify other users that you intend to put the system in maintenance mode and give them a deadline to log out. The maintenance mode operation cannot be canceled once you initiate it.

Procedure

Step 1 To put Crosswork in maintenance mode:
a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.
b) Drag the **Turn on/off maintenance** slider to the right, or On position.
c) You will receive a warning message that the system is about to enter maintenance mode. Click **Continue** to confirm your choice.

Note
If you wish to reboot, wait for five minutes after system has entered maintenance mode in order to allow the Cisco Crosswork database to sync, before proceeding.

Step 2 To restart from maintenance mode:
a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.
b) Drag the **Turn on/off maintenance** slider to the left, or Off position.

Note

If a reboot or restore was performed when the system was previously put in maintenance mode, the system will boot up in the maintenance mode and you will be prompted with a pop-up window to toggle the maintenance mode off. If you do not see a prompt (even when the system was rebooted while in maintenance mode), you must toggle the maintenance mode on and off to allow the applications to function normally.

Update network access configuration

The **Network access configuration** section specifies the parameters used for network access through SNMP, Login, and the SAM interface. These parameters can be modified to meet your specific requirements. For example, you can update the SNMP timeout value according to your needs.

Caution Before you edit, be aware that your changes will be applied globally and will affect all collections, jobs, and plan files.

To edit the network access configuration, do the following:

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Collection settings** > **Network access configuration**.

Step 2 Click the **Edit** button. An alert window appears informing that modifying the configuration to disable the required service results in collection failure. If you are changing only the timeout and other parameters, click **Confirm**.

The page turns editable.

Step 3 Edit the file as per your requirement.

Step 4 Click **Save** to save the changes.

Download the network access configuration file:

To download the network access configuration file to your local machine, click .

Update collector capability

Each collector's data source and the tables/columns into which they are populating the data are available in the **Collector capability** page. In Cisco Crosswork Planning, you can update these configurations as per your requirement.

Caution Before you update, be aware that your changes will be applied globally and will affect all collections, jobs, and plan files.

The collector's table and column details are configured using the following format:

Collector.table.table-name=ALL/Column list

where ALL indicates that the collector populates all columns in that table. If the collector populates only a subset of columns, then it is specified as a list of column names separated by commas.

Follow these steps to update the default configurations.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Collection settings** > **Collector capability**.

Step 2 Click the **Edit** button.

The page turns editable.

Step 3 Edit the .txt file as per your requirement.

Step 4 Click **Save** to save the changes.

Download the collector capability configurations

To download the collector capability configurations to your local machine, click .

Reset to default configurations

To reset the configurations to the default values, click **Reset default config** button at the top right.

Configure aging

By default, when a circuit, port, node, or link disappears from a network, it is permanently removed and must be rediscovered. To configure how long Cisco Crosswork Planning retains these elements that have disappeared before they are permanently removed from the network, complete the following steps.

Caution Before you configure, be aware that your changes will be applied globally and will affect all collections, jobs, and plan files.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** > **Collection Settings** > **Purge delay**.

Step 2 Check the **Enable** check box to enable aging.

Step 3 Enter the values in the relevant fields:

- **L3 port**—Enter the time duration for which an L3 port must be kept in the network after it becomes inactive.
- **L3 node**—Enter the time duration for which an L3 node must be kept in the network after it becomes inactive.
- **L3 circuit**—Enter the time duration for which an L3 circuit must be kept in the network after it becomes inactive.

Note
The value of **L3 node** must be greater than or equal to **L3 port** which in turn must be greater than or equal to **L3 circuit**.

Configure purging of archived plan files

The archived plan files are periodically deleted in Cisco Crosswork Planning to conserve storage space. By default, the files are retained for 30 days.

Follow these steps to configure the retention period (in days) as per your requirement.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Collection settings** > **Archive purge**.

Step 2 In the **Archive retention** field, enter the number of days after which the files can be deleted.

For example, if you enter 40 in this field, the plan files older than 40 are deleted.

Step 3 Click **Save** to save the changes.



Note Uncheck the **Enable** check box to disable the purging of archived plan files. Be aware that if you disable it, storage space will eventually run out.

Configure static routes

Static routes are used to reach the devices in a different subset reachable via the data interface.



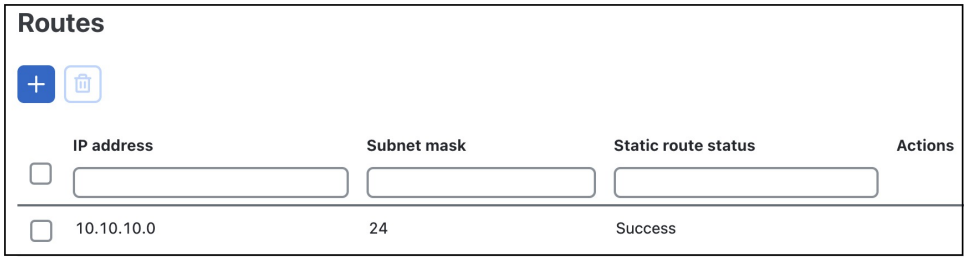
Note After static routes are applied, their corresponding entries will appear when you run the **ip rule list** command at the Crosswork shell prompt.

Add static routes

Follow these steps to add static routes.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Device connectivity management** > **Routes**.



Step 2 Click . The Add Route IP window appears.

Step 3 Enter the valid IPv4 or IPv6 subnet in CIDR format.

Step 4 Click **Add**.

Delete static routes

Follow these steps to delete static routes.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** > **Device connectivity management** > **Routes**.

Step 2 Select the static route you want to delete and click .

Step 3 Click **Delete** in the confirmation window.