Manage System Access and Security

This section contains the following topics:

Manage Certificates

What is a Certificate?

A certificate is an electronic document that identifies an individual, a server, a company, or another entity, and associates that entity with a public key. When a certificate is created with a public key, a matching private key is also generated. In TLS, the public key is used to encrypt data being sent to the entity and the private key is used to decrypt. A certificate is signed by an issuer or a "parent" certificate (Certificate Authority) - i.e. signed by the parent's private key. Certificates can also be self-signed. In a TLS exchange, a hierarchy of certificates is used to verify the validity of the certificate's issuer. This hierarchy is called a trust-chain and consists of 3 types of entities: a root CA certificate (self-signed), possibly multiple levels of intermediate CA certificates, and a server (or client) certificate (end-entity). The intermediate certificates act as a "link of trust" linking the server certificates to the CA's root certificate and providing additional layers of security. Starting from the root certificate's private key, the private key for each certificate in the trust chain signs and issues the next certificate in the chain until finally signing an end entity certificate. The end-entity certificate is the last certificate in the chain and is used as a client or server certificate. For more details about these protocols, see X.509 Certificates, on page 71 and HTTPS, on page 71.

How are Certificates Used in Crosswork?

Communication between Crosswork applications and devices as well as between various Crosswork components are secured using the TLS protocol. TLS uses X.509 certificates to securely authenticate devices and encrypt data to ensure its integrity from source to destination. Crosswork uses a mix of generated and client uploaded certificates. Uploaded certificates can be purchased from Certificate authorities (CA) or can be self-signed.

For example, the Cisco Crosswork VM-hosted web server and the client browser-based user interface communicate with each other using Crosswork generated X.509 certificates exchanged over TLS.

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 UI (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates. The following figure displays the default certificates provided by Cisco Crosswork.

Figure 1: Certificate Management UI

Certificates   Selected 0 / Total 5 ↻ ⚙

Name		Expiration Date	Last Updated By	Last Update Time	Associations	Actions
Crosswork-Device-Syslog	ⓘ	05-SEP-2026 10:27:04 PM GMT+5:30	Crosswork	06-SEP-2021 10:27:04 PM GMT+5:30	Device Syslog Communication	...
Crosswork-Internal-Communication	ⓘ	05-SEP-2026 10:26:24 PM GMT+5:30	Crosswork	06-SEP-2021 10:26:24 PM GMT+5:30	Crosswork Internal TLS	...
Crosswork-ZTP-Device-SUDI	ⓘ	15-MAY-2029 01:55:42 AM GMT+5:30	Crosswork	06-SEP-2021 10:26:54 PM GMT+5:30	ZTP SUDI	...
Crosswork-ZTP-Owner	ⓘ	05-SEP-2026 10:26:50 PM GMT+5:30	Crosswork	06-SEP-2021 10:26:50 PM GMT+5:30	Secure ZTP Provisioning	...
Crosswork-Web-Cert	ⓘ	05-SEP-2026 10:26:04 PM GMT+5:30	Crosswork	06-SEP-2021 10:26:04 PM GMT+5:30	Crosswork Web Server	...

Certificate Types and Usage

The following figure shows how Crosswork uses certificates for various communication channels.

Figure 2: Certificates in Cisco Crosswork
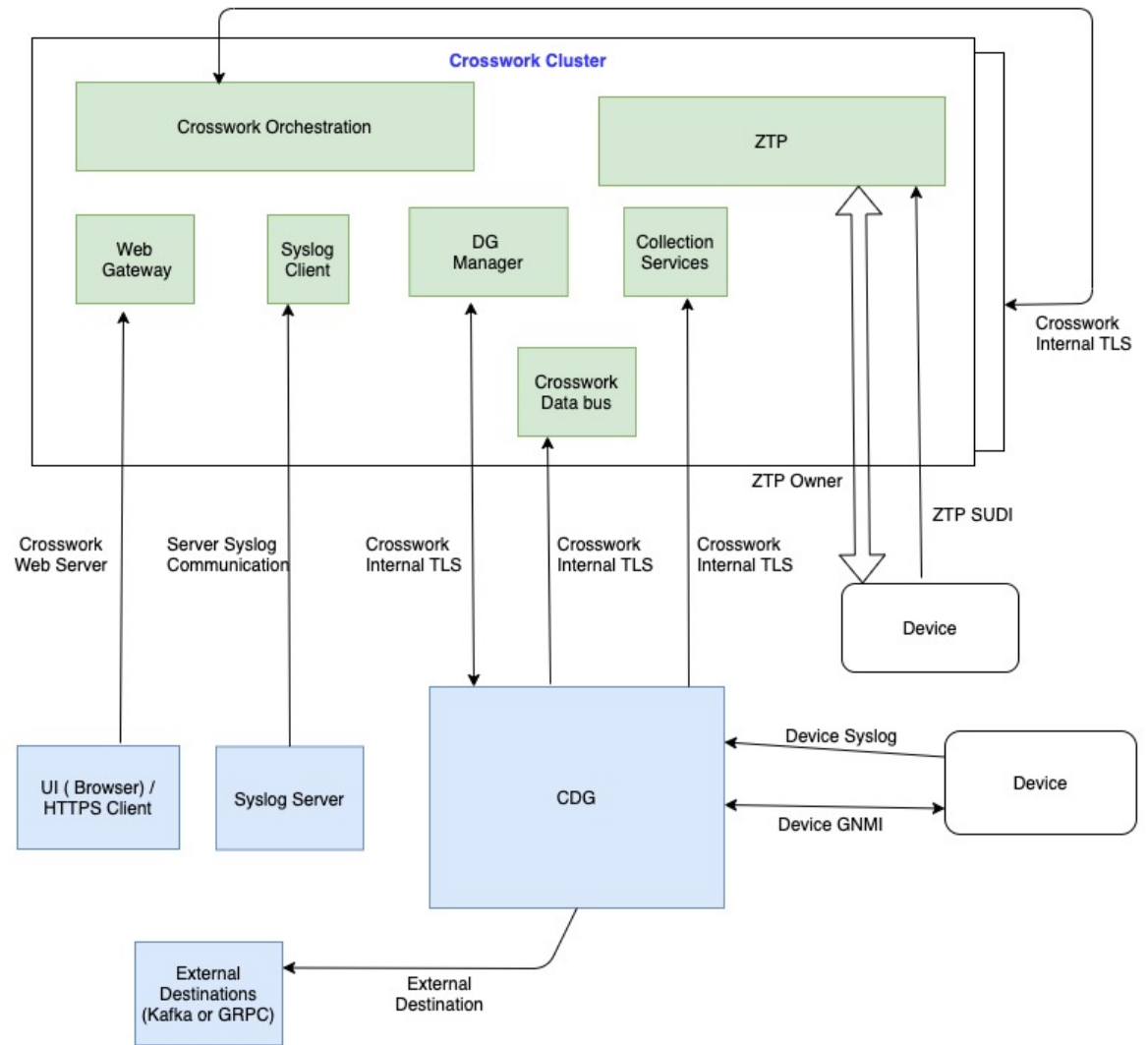
These certificates are classified into various roles with different properties depending on their use case as shown in the following table.

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork (CW) Internal TLS	CW-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. They are used for interprocess communications between Crosswork and Crosswork Data Gateway and communication between internal Crosswork components. • Allows mutual and server authentication.	Crosswork	• Crosswork Data Gateway • Crosswork	Download	5 years	—
CW Web Server	CW-Web-Certificate 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

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
ZTP SUDI	CW-ZTP-Device-SUDI	• A public Cisco certificate that is provided as part of Crosswork. • Provides ZTP protocol communication channel between the ZTP application and device. • Allows server authentication.	Crosswork ZTP	Device	• Upload • Download	100 days	30 days. This value is user-defined
Secure ZTP Provisioning	CW-ZTP-Owner	• Generated and provided by Crosswork. • Forwarded by ZTP to devices and used for second layer of encryption.	Crosswork ZTP	Device	• Upload • Download	5	30 days. This value is user-defined
Device Syslog	CW-Device-Syslog	• Generated and provided by Crosswork. • Provides Syslog telemetry communications between devices and Crosswork Data Gateway. • Allows server authentication.	Crosswork Data Gateway	Device	Download	5 years	—
Device gNMI Communication	—	Provides GNMI telemetry communications between devices and Crosswork Data Gateway.	Crosswork Data Gateway	Device	• Upload • Download	Not Applicable	30 days. This value is user-defined

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Server Syslog Communication	—	• Allows syslog events and logs from Crosswork to an external Syslog server. • Allows server authentication.	External Syslog Server	Crosswork	• Upload You can upload multiple certificates associated with different servers. • Download	—	30 days. This value is user-defined
External Destination	—	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a mutual-authentication.	External Destinations (Kafka or gRPC)	Crosswork Data Gateway	• Upload [1] • Download	—	30 days. This value is user-defined
External Destination Server Auth	—	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a server-based authentication.	External Crosswork Data Gateway Destinations (Kafka or gRPC)	Crosswork Data Gateway	• Upload [2] • Download	—	30 days. This value is user-defined
Secure LDAP Communication	—	Crosswork uses the trust chain of this certificate to authenticate the secure LDAP server.	Secure LDAP server	Crosswork	• Upload • Download	—	30 days. This value is user-defined
Application External Destination	—	Exports telemetry data from Crosswork to an external Kafka destination.	External Kafka Destinations	Crosswork	Upload	—	30 days. This value is user-defined

[1] You can upload multiple certificates associated with different destinations.

[2] You can upload multiple certificates associated with different destinations.

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 a New Certificate

You can add certificates for the following roles:

- **External Destination**: Certificates uploaded for this role are used to secure communication between Crosswork Data Gateway and external destinations like Kafka servers. To enable mutual authentication, the user uploads a **CA Certificate Trustchain** that will be common to both Crosswork Data Gateway and the external server. This trust chain contains a root CA certificate and any number of optional intermediate CA certificates. The last intermediate certificate in the chain and its corresponding private key is uploaded separately in the UI using **Intermediate key**, **Intermediate certificate**, and optionally **Passphrase** (if one was used for generating the intermediate key). Crosswork internally creates a client certificate using this intermediate key for the Crosswork Data Gateways that connects to the external destination. The destination (for example: Kafka) server certificate trust needs to be derived from the same root CA certificate.

  You can upload certificates to the **External Destination** role, the authentication type must be opted as **Mutual-Auth** on the **Add Destination** page. For more information about the authentication types, see Add or Edit a Data Destination.

- **Server Syslog Communication**: The user uploads the trust chain of the Syslog server certificate. This trust chain is used by Crosswork to authenticate the Syslog server. Once this trust chain is uploaded and propagated within Crosswork, the user can add the syslog server (**Administration** > **Settings** > **Syslog Server Configuration**) and associate the certificate to enable TLS. For more information, see Configure a Syslog Server, on page 74.

- **Devices gNMI communication**: The user uploads a bundle of trust chains used by Crosswork Data Gateway to authenticate the devices connecting to it. This trust chain and the device gNMI certificate must also be configured on the device. The trust chain file that is uploaded can contain multiple hierarchies of trust certificates as needed to allow all the devices in the network to connect. For more information, see Configure gNMI Certificate.

- **Secure LDAP Communication**: The user uploads 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 61) and associate the certificate.

- **External Destination Server Auth**: The user uploads the root CA certificate. This certificate is used to establish a secure communication between Crosswork Data Gateway and external destinations like Kafka servers.

  You can upload the certificates to the **External Destination Server Auth** role only when the authentication type is set to **Server-Auth**. For more information about the authentication types, see Add or Edit a Data Destination.

- **Application External Destination**: The user can upload the application certificates to ensure secure transfer of telemetry data to an external Kafka destination. The Kafka channel is safeguarded through mutual TLS, and the TLS Manager is responsible for managing the certificates used by external Kafka.

Note Cisco Crosswork 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.

If you prefer to upload your own ZTP and web certificates (instead of using the default certificates provided within Cisco Crosswork), use the Edit function (see Edit Certificates, on page 8).

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.

- A data destination must be configured prior to adding a new certificate for an external destination. For more information, see Add or Edit a Data Destination.

- Ensure there are no collection jobs configured for destinations when adding or updating a certificate with multiple destinations.

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. For more information, see Certificate Types and Usage, on page 2.

> **Note**   You can select available destinations (Kafka/gRPC) while adding or updating an **External Destination** certificate.

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

Step 5   In the case of an **External Destination** certificate, you must select one or more destinations and provide the CA certificate trustchain, intermediate certificate, and intermediate key. The passphrase field is optional and is used to create the intermediate key (if applicable).

Step 6   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, ZTP 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.

You can also "remove" a certificate by following this procedure to replace the certificate or by disabling security (disable **Enable Secure Communication** option) for any assigned destinations (see Add or Edit a Data Destination). Permanently deleting a certificate from the Cisco Crosswork system is not supported.

Step 1 From the main menu, choose **Administration** > **Certificate Management**. and check the certificate that you want to modify.

Step 2 Click ⋯ on the certificate that you want to modify and select **Update Certificate**.

Step 3 Update the necessary options.

Note While updating a CW Web Server Certificate, provide relevant values for the following fields:

- **Crosswork Web CA**: Trust chain file (in PEM format) containing the root CA certificate and zero or more intermediate certificates.

- **Crosswork Web Intermediate**: An intermediate CA certificate signed with the root CA certificate.

- **Crosswork Web Intermediate Key**: The key associated with the intermediate CA certificate.

- **Crosswork Web Passphrase**: This is an optional field.

Upon successful validation, the Certificate Management UI logs out automatically and applies the certificate to the Web Gateway.

Step 4 Click **Save**.

Download Certificates

To export certificates, do the following:

Step 1 From the main menu, choose **Administration** > **Certificate Management**.
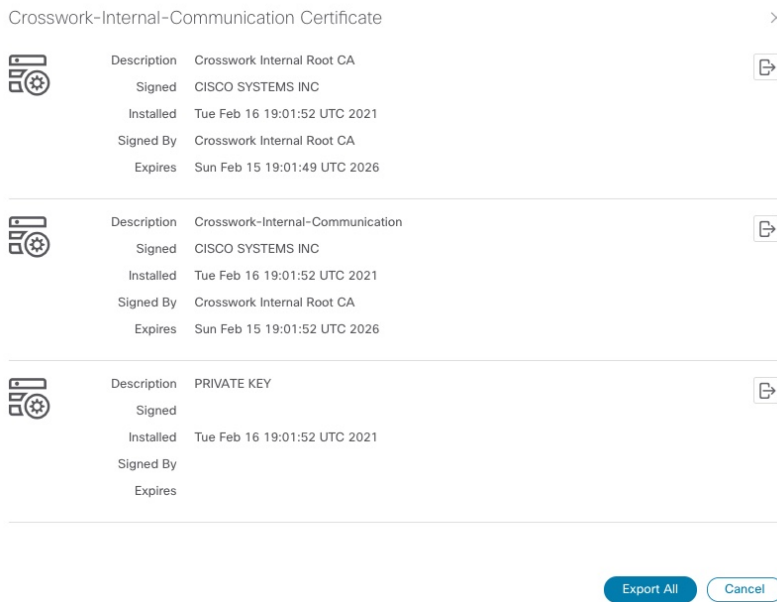
Step 2 Click ⓘ for the certificate you want to download.

Figure 3: Export Certificates

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

Renew Certificates

Kubernetes Certificate Renewal

Certificates are valid for one year before they expire. After renewing the certificates, ensure that the pods are healthy before resuming other operations.

Note When renewing certificates before expiry, it is recommended to perform this activity during a maintenance window as the cluster is in an operational state.

To renew a certificate, perform the following:

Before you begin

• Create a plain text file on your local machine (for example, `password.txt`) that contains the SSH login password for the server.

• Keep the management IP addresses readily available for the hybrid and worker nodes in your cluster.

Step 1   Create a backup of your Crosswork Network Controller.

Step 2   Log in to one of your hybrid nodes.

Step 3   Run the following command:

Attention   The command below has line breaks inserted for display purposes. Please remove these line breaks before executing it.

```
renew_k8s_cert --hybrid=hybridNodeMgmtIP1,hybridNodeMgmtIP2,hybridNodeMgmtIP3
--worker=workerNodeMgmtIP1,workerNodeMgmtIP2,workerNodeMgmtIP3 --user=<ssh-username>
--passwdfile=<passfile-path>
```

Replace the parameters with the management IP addresses of the nodes in your cluster.

- `hybridNodeMgmtIP`: Management IP of the hybrid node.

- `workerNodeMgmtIP`: Management IP of the worker node. You can add this parameter according to the number of worker nodes in your cluster. If no worker nodes are available, you can skip this parameter.

- `ssh-username`: The SSH username

- `passfile-path`: The path for the plain text file that contains the SSH login password.

Here are some examples:

- Example for a 6-node cluster:

```
renew_k8s_cert --hybrid=10.10.10.101,10.10.10.102,10.10.10.103
--worker=10.10.10.104,10.10.10.105,10.10.10.106 --user=cw-admin
--passwdfile=/home/cw-admin/password.txt
```

- Example for a 3-node cluster:

```
renew_k8s_cert --hybrid=10.10.10.101,10.10.10.102,10.10.10.103  --user=cw-admin
--passwdfile=/home/cw-admin/password.txt
```

- Example for the single VM deployment:

```
renew_k8s_cert --hybrid=10.10.10.101  --user=cw-admin --passwdfile=/home/cw-admin/password.txt
```

Automatic Renewal of Internal Certificates

Crosswork CA generates TLS certificate chains, including root, intermediate CA, and leaf certificates, for day 0 deployments (Geo HA and non-Geo HA). The leaf certificates are valid for 2 years, while root and intermediate CA certificates are valid for 5 years. Customers with Crosswork deployments lasting beyond 2 years will face certificate expiry, disrupting TLS communication and impacting cluster operations. Auto-renewal applies to all Crosswork certificates generated internally, including NATS, Kafka, and any application-specific internal certificates.

The renewal alert is generated only when the expiry period is less than 60 days. When an internal certificate is expiring and renewed, all internal certificates of that type will be renewed. For example, when a leaf certificate is renewed, the process will also renew all other leaf certificates.

☞

Important **For Geo HA deployment:**

- In the case of a Geo HA deployment, the certificate renewal is triggered in the active AZ cluster. Internally, the TLS manager determines if the cluster has Geo redundancy enabled or disabled and decides whether the certificate renewal must be performed on one cluster or both Geo HA clusters. Once the renewal job is completed on the active cluster, the job will automatically run in the standby cluster after a delay of a few minutes. The job progress is displayed on the standby cluster along with alarm events.

The certificate renewal process can cause a downtime of approximately 30 minutes to 1 hour. It is recommended to perform this activity during a maintenance window to avoid disrupting cluster operations.

To renew an internal certificate, perform the following:

Step 1 From the main menu, choose **Administration** > **Certificate Management**. The **Certificate Management** window is displayed. If an internal certificate is about to be expired, a prompt is displayed for certificate renewal.

Note Alerts about certificate expiry are displayed on the Crosswork dashboard when you log in. These alerts will be generated at various stages of the certificate expiry, with increasing severity as the expiry date approaches.
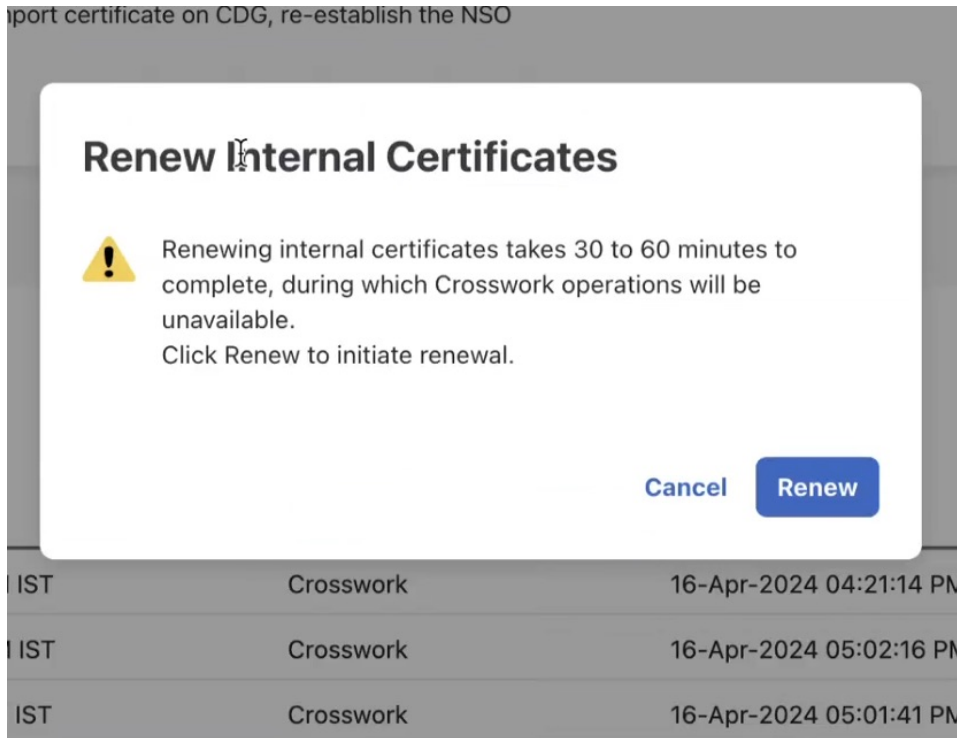
Figure 4: Renew Internal Certificate prompt

Step 2 Click **Renew Internal Certificate**. A confirmation popup is displayed. Click **Renew** to confirm.

Figure 5: Renewal Confirmation Prompt

This action invokes the REST API (/v2/cert/renew) and initiates the certificate expiry check. A notification about the new renewal job is displayed on the **Certificate Management** window.

Figure 6: Renewal Job Notification
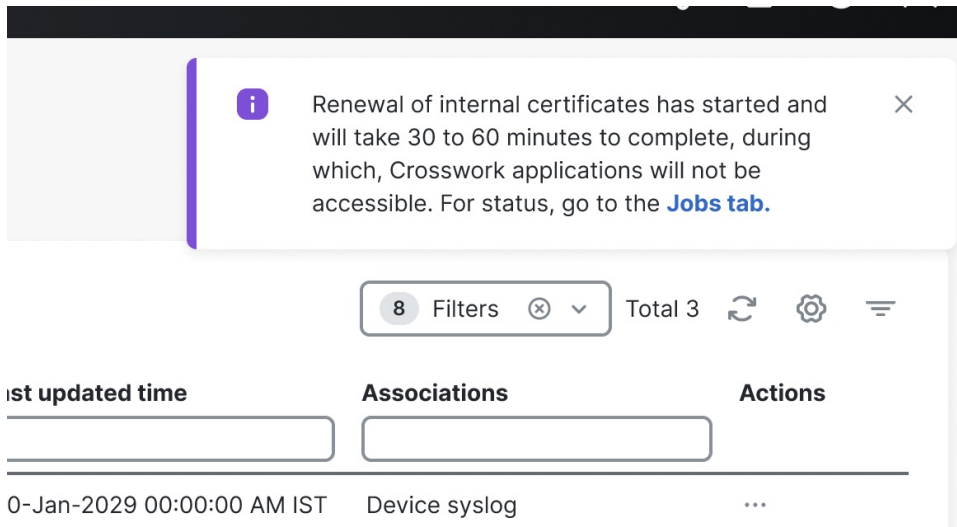
You can view progress of the renewal job from the **Jobs** tab. Once the job is complete, an Info alarm event is raised about the successful completion. You must manually clear this alarm to acknowledge the event. Any error during the process will result in job failure; however, the job can be triggered again as the API is idempotent.

Step 3   **In case of Geo HA deployment**: After successfully completing the certificate renewal, run an on-demand or periodic sync across the active and standby clusters to ensure that asynchronous replication is re-established over a secure channel.

Step 4   Once the renewal job is completed, perform the following steps to ensure TLS communication is maintained between Crosswork and other external components:

a) **Crosswork with Crosswork Data Gateway**: Re-import the newly recreated `controller.pem` signing certificate on Crosswork Data Gateway as `dg-admin` user. For more information, see Import Certificate. This action prevents the deletion of Data Gateway instances, avoids the detachment and re-attachment of devices, and ensures the continuation of collection and other offload operations.

Note   This action is also performed as part of the Crosswork Data Gateway day-N enablement as well.

b) **Crosswork Data Gateway - Device Syslog**: If device syslog root and intermediate certificates are renewed, users must manually export and reconfigure these certificates on all devices. For internally generated Crosswork CA certificates, export the new device syslog root and intermediate CA certificates and configure them as CA trustpoints on IOS XR/XE devices. For more information, see the IOS XE and IOS XR instructions in Syslog Collection Job.

if there is a renewal for device syslog root and intermediate certificates, users must manually export these certificates to the devices.

c) **External destination/Server Auth CA**: Re-upload the External Destination and Server Auth CA certificates to Crosswork.

d) **Cisco NSO**: Export the regenerated Crosswork Web server certificate from the Crosswork UI browser, configure it, and store it on the NSO server. For more information, see the Step 1b in the Configure Standalone NSO, on page 48 section.

Manage Licenses

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).

- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com). A **Cisco Smart Account** provides the repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage and track Cisco purchases. The **Cisco Smart Software Manager (CSSM)** enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you may create and manage multiple virtual accounts within your Smart Account to manage licenses. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab under the **Application Management** window. In the **Smart License** tab, you can register your Crosswork Network Controller application, edit the transport settings, renew the license, and de-register your application.

Important	All unmanaged devices are counted towards the device limits associated with Crosswork licenses. To prevent this, delete your unmanaged devices in the Crosswork UI.

Note	Licenses for lab systems are obtained through the same process as those for production environments. If you require a license for a lab beyond the 90-day trial period, please coordinate with your account team or a Cisco partner to have the appropriate license issued.

Tracked Node Counts for Crosswork Optimization Engine

For Crosswork Optimization Engine, the node count is reported in the following cases:

- After initial installation and startup of the following pods: Crosswork UI, RESTCONF, or any of the feature packs (Local Congestion Mitigation, Bandwidth on Demand, or Circuit Style Manager).

- Manually restarting the pods

- Daily at a fixed time (1:00 AM)

Configure Transport Settings

You can configure the transport settings to decide how Crosswork Network Controller communicates with the Cisco servers.

Note	Transport Settings cannot be changed while the Crosswork product is in Registered mode. You have to de-register to change them.

Step 1 In the **Smart License** tab, the Transport Settings display the current transport mode selected. To modify, click **View/Edit**.

The **Transport Settings** dialog box is displayed.

Figure 7: Transport Settings Dialog Box

Transport Settings   ✕

Configure how the product will communicate with Cisco. Note that this setting
is shared with smart transport, so any changes made here will apply to other
features using this service.

◉ Direct - product communicates directly with Cisco's licensing servers
    URL : https://smartreceiver.cisco.com/licservice/license

◯ On-prem Smart Software Manager

URL

◯ HTTP/HTTPS gateway - send data via an intermediate HTTP or HTTPS
    proxy

IP address

Port

Step 2   Select the relevant transport mode and make relevant entries in the fields provided.

- **Direct**: The application directly connects with Cisco Smart Software Manager (CSSM).

- **On-prem Smart Software Manager**: The application communicates via CSSM On-Prem, ensuring that all user
  communication remains on premises. For more information on the CSSM on-prem option, see the Smart Software
  Manager guide.

- **HTTP/HTTPS Gateway**: The application connects via an intermediate proxy server. This is applicable only for
  Direct mode.

Step 3   Click **Save**.

Register Crosswork Network Controller Application

To enable licensed features, the Crosswork Network Controller application must be registered to CSSM using
a registration ID token or a reserved license. Once registered, an Identity Certificate is saved securely in the
Smart Account and used for all ongoing communications. The certificate is valid for one year and will be
renewed automatically after six months to ensure continuous operation.

Note   For information on generating the registration token, please refer to the support resources provided in the
Smart Software Manager webpage.

Crosswork also supports registration of solution-based entitlements for Crosswork.

Step 1 From the main menu, select **Administration** > **Smart Licenses** to display the **Smart Licenses** tab.

The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 8: Smart Software Licensing Unregistered Example

Step 2 Click the **Select Crosswork Product** drop-down list and select your product. In you plan to register a specific application, select the application from the list.

- If you plan to register using a solution-based license, select **Crosswork Network Controller**.
- In you plan to register a specific application, select the application name from the list.

Important You can register an application using either a solution-based license or an application-specific license, but not both. If you attempt to register a product that is already licensed, the system will display an error and prompt you to deregister the previous license. Depending on the type of licensing you choose (solution-based or application-based), the respective entitlements will be displayed.

Step 3 In the **Smart Software Licensing** dialog box, click **Register**.

The Smart Software Licensing Product Registration dialog box is displayed. The **Register via token** radio button is selected by default.

Figure 9: Smart Software Licensing Product Registration Dialog Box

Smart Software Licensing Product Registration ✕

◉ Register via token   ◯ Register via reserved license

To register the product for Smart Software Licensing:

- Ensure you have connectivity to the URL specified in your transport settings. By default, this will require Internet access. See the online help registering to a on-prem Smart Software Manager.
- Paste the product instance registration token you generated from **Smart Software Manager** or your on-prem Smart Software Manager.

> ℹ️ After succesful registration, page may need to be refreshed to see the updated status.

Product instance registration token *

☑ Re-register this product instance if it is already registered

Step 4 In the **Product Instance Registration Token** field, enter the registration token generated from your Smart Account. Make sure the token ID is accurate and within validity period. For more information, see https://www.cisco.com/c/en_ in/products/software/smart-accounts/software-licensing.html.

Step 5 (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** check box.

   Note   After a backup restore, disaster recovery, or data migration operation, you must manually re-register the Cisco Crosswork VM to CSSM. This applies if the Cisco Crosswork VM was already registered at the time the backup was taken and is used in the restore operations.

Step 6 Click **Register**. It may take a few minutes to process the registration. If successful, the 'Product Registration completed successfully' message is displayed.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Note
- If you encounter a registration error (e.g., *"Communication send error"* or *"Invalid response from licensing cloud"*), please wait for some time and retry the registration. If the error persists after multiple attempts, please contact the Cisco Customer Experience team for assistance.

- If you encounter a communication timeout error during registration, click **OK** in the error dialog box, and the application will reattempt the registration.

- In some cases, after successful registration, you may need to manually refresh the page to see the updated status.

Manually Perform Licensing Actions

The renewal of registration and authorization are automatically enabled for Crosswork Network Controller, by default. However, in the event of a communication failure between the application and the Cisco server, these actions can be manually initiated. You can use the **Actions** drop-down button to manually renew, re-register and de-register the application.

Step 1   In the **Smart License** tab, click **Actions** drop-down button and select the relevant option for the following quick actions.

Figure 10: Actions drop-down menu
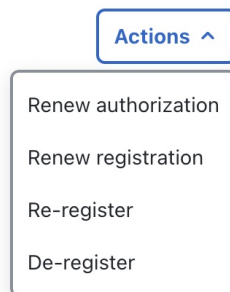
a) **Actions** > **Renew Authorization**: To renew the authorization manually if the automatic renewal service fails at the end of 30 days.
b) **Actions** > **Renew Registration**: To renew the registration manually if the automatic renewal service fails at the end of 6 months.
c) **Actions** > **Re-register**: Re-register the application, for example, on account of the expiry of registration tokens.
d) **Actions** > **De-register**: De-register the application, for example, when the transport settings need to be changed.

Note   Once de-registered, the application will be moved to **Evaluation** mode (if evaluation period is available), or **Evaluation Expired** mode. For more information, see License Authorization Statuses, on page 22.

Step 2   The selected action is executed successfully.

Register Cisco Crosswork Applications via Offline Reservation

Cisco Crosswork applications that use Smart Licensing share usage information to CSSM at regular intervals. If you do not want to connect with CSSM regularly, Cisco Smart Licensing provides an option of offline reservation.

There are two modes of offline reservation:

- Specific License Reservation (SLR)—In this mode, you can select the number of licenses of each entitlement that has to be reserved.

- Permanent License Reservation (PLR)—In this mode, there will be a single license that will make the entire product In Compliance.

Before you begin

Confirm that you have a Smart Account. If not, go to Smart Account Request and follow the instructions on the website.

Step 1 From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab.

Step 2 Click **Register**.

The Smart Software Licensing Product Registration dialog box is displayed.

Step 3 Select the **Register via Reserved License** option.

Figure 11: Smart Software Licensing Product Registration Dialog Box

Smart Software Licensing Product Registration   ✕

◯ Register via Token   ◉ Register via Reserved License

Reservation Code
Use this code to obtain a authorisation code from Cisco smart software manager.

Please click on generate

Copy   Generate

Paste Authorisation Code here
Please paste the authorisation code copied from Cisco smart software manager

Register   Cancel

Step 4 Click the **Generate** button under the Reservation Code section. Your Reservation Request Code is generated and populated in the text field. Copy this code using **Copy** button.

Step 5 Go to the Cisco Software Central website and select the appropriate virtual account.

Step 6 Click the **Licenses** tab, then click **License Reservation**. Paste the Reservation Request Code that you generated in Step 4 and click **Next**.

Step 7   In the Select Licenses page, select the **Reserve a specific license** radio button, reserve the necessary licenses from the list, and click **Next**.

Step 8   In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using the **Copy to Clipboard** button.

Step 9   Navigate back to the Smart Software Licensing Product Registration page on the Cisco Crosswork UI. Paste the Authorization Code in the text field under the **Paste Authorisation Code here** section.

Step 10   Click **Register**. It may take a few minutes to process the registration.

           The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Update Offline Reservation

           Use the **Update Reservation** option to update the license counts reserved via offline reservation.

Step 1   From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2   Go to the Cisco Software Central website and select the appropriate virtual account.

Step 3   Click the name of the product instance that matches your Product Instance Name.

Step 4   Click the **Actions** drop-down button and choose **Update Reservation**.

Step 5   In the Select Licenses page, select the **Reserve a specific license** radio button, update the count of the necessary licenses from the list and click **Next**.

Step 6   In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using **Copy to Clipboard** button.

Step 7   Navigate back to the Smart License page on the Cisco Crosswork UI. Click the **Actions** drop-down button and choose **Update Reservation**. Paste the Authorization Code that you generated in Step 6 and click **Update**.

           A Confirmation Code is generated. You can find this under the Smart Software Licensing Status section. Copy this code.

Step 8   Navigate back to the Cisco Software Central website. Click the required product instance name.

Step 9   Click the **Actions** drop-down button and choose **Enter Confirmation Code**.

Step 10   Enter/paste the Reservation Confirmation Code that was generated in Step 7 and click **OK**.

           The license count will be updated on the Smart License page of the Cisco Crosswork UI.

Disable Offline Reservation

           Use the **Disable Reservation** option to release the reserved licenses. Once the licenses are released, the application will be moved to **Evaluation** mode (if evaluation period is available), or **Evaluation Expired** mode. For more information, see License Authorization Statuses, on page 22.

Step 1   From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2   Click the **Actions** drop-down button and choose **Disable Reservation**.

Step 3 In the Confirm Disable Reservation window, click **Confirm**.

A Release Code (Reservation Return Code) is generated. Copy this code using the **Copy** button.

Step 4 Navigate to the Cisco Software Central website and select the appropriate virtual account.

Step 5 Click the name of the product instance that matches your Product Instance Name.

Step 6 Click the **Actions** drop-down button and choose **Remove**.

Step 7 In the Remove Reservation pop-up, paste the Reservation Return Code that you generated in Step 3 and click **Remove Reservation**.

The Registration Status will be updated to Un Rgistered state on the Smart License page of the Cisco Crosswork UI.

License Authorization Statuses

Based on the registration status of your Crosswork Network Controller application, you can see the following License Authorization Statuses.

Table 1: License Authorization Statuses

Registration Status	License Authorization Status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which the licensed features of the application can be freely used. This state is initiated when you use the application for the first time.
	Evaluation Expired	The application has not been successfully registered at the end of the evaluation period. During this state, the application features are disabled, and you must register to continue using the application.
	Registered Expired	The application is unable to contact the CSSM before the expiration of Identity Certificates and has returned to the unregistered state. The application resumes the remaining evaluation period, if available. At this stage, new registration ID token is required to reregister the application.
Registered	Authorized (In Compliance)	The application has been fully authorized to use the reserved licensed features. The authorization is automatically renewed every 30 days.
	Out of Compliance	The associated Virtual Account does not have enough licenses to reserve for the application's current feature use. You must renew the entitlement/usage limit registered with the token to continue using the application.
	Authorization Expired	The application is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

Authorization Status Response

This section explains the actions or message enforced by Crosswork in case of "Out of Compliance" or "Evaluation Expired" status.

The behavior is covered for Right-to-Use (RTU) and Right-to-Manage (RTM) licenses.

Table 2: Out of compliance status action for registered systems

Registration Status	License Authorization Status	Solution or Product	Enforced Action or Message
Registered	Out of Compliance	Crosswork Network Controller (solution)	No action taken.
		Crosswork Optimization Engine	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Active Topology	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Service Health	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Change Automation	RTU: No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Health Insights	RTU: No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork External Collection	No action taken.
		Element Management Functions	RTM: No action taken (in case of normal token-based registration).

Table 3: Evaluation expired status action for unregistered systems

Registration Status	License Authorization Status	Solution or Product	Enforced Action or Message
Unregistered	Evaluation Expired	Crosswork Network Controller (solution)	All UI screens are disabled, and only the Smart Licensing window is displayed. Users can continue to use Crosswork Network Controller only after completing the registration.
		Crosswork Optimization Engine	Only READ operations are allowed. Create, update, and delete operations are restricted.
		Crosswork Active Topology	No action taken. No impact on provisioning UI (NSO) workflows.
		Crosswork Service Health	Monitoring cannot be enabled or resumed. An error message ("License evaluation expired or reservation exceeded, Service Health functionality disabled") is displayed.
		Crosswork Change Automation	RTU: Playbook execution is not allowed. A major alarm is raised.
		Crosswork Health Insights	RTU: Health Insights usage is not allowed. A message is logged with license state indicating that "License is expired".

RTM: Critical alarm is raised. |
| | | Crosswork External Collection | RTM: Collection Job creation, Template Collection Job creation, and Bulk template collection operation requests are rejected. |
| | | Element Management Functions | RTM: ZTP API operations are not allowed. An error message is displayed ("Your License Evaluation Period has expired or there are no Reserved Licenses"). |

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. 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 27).

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.

When you are configuring Device Access Groups for your users, select the **Device Access Group** listed in the right pane to assign it to the new user you are creating.

Note 1. By default users associated with ALL-ACCESS Device Access Group are provided access to ALL devices.

2. You must associate at least one Device Access Group to a user.

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 on the Audit Logs, see View Audit Log.

Step 6 (Optional) To view NACM rules for a user:

a) Click the ⋯ icon under the **Actions** column, and select **Generate NACM Rules**.

The **NACM Rules** window is displayed for the selected user name.

If you have an NSO service configured on your Crosswork Network Controller, you can generate NACM rules by clicking the ⋯ icon under the **Actions** column for a user and selecting **Generate NACM Rules**. This rule list for the device level NACM control will integrate Crosswork Network Controller with the NSO workflow. Note that for every unique combination of Device Access Group that is associated with a user, there is–

- A NACM group associated with the user.

- A corresponding NACM rule list associated with the user.

The rule will allow access to devices in selected Device Access Groups and deny access to other devices. You can copy the XML rules file and add it in your NSO NACM Rule configuration setup. The options available under the NSO Actions tab, located in Device **Management > Network Devices**, will also be restricted based on the Device Access Groups permissions of the user.

You also view the Crosswork Audit log and the NSO commit logs to track and verify the activities of users using the NACM rules, ensuring traceability.

Administrative Users Created During Installation

During installation, Crosswork 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. You can also change the Cisco Crosswork administrator password using the following methods:

- Log in as the admin user and edit the admin user password .

- Enter the following command: `admin(config)#` **`username admin`** *`<password>`*

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 4: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager, triggers Playbooks in response to KPI alerts	All	Read, Write
Monitor	Monitors alerts only	Health Insights, Inventory, Topology	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. Using Zero Touch Provisioning features requires access to all ZTP APIs.

Create User Roles

Step 1 From the main menu, choose **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 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 28).

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 24). Later, you can edit the roles themselves to give users the privileges you want (see Edit User Roles, on page 28).

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

Step 2 Click on 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.

Step 1 From the main menu, choose **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.

Step 1   From the main menu, choose **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:

Table 5: 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 Crosswork. You must have READ permission to view/read configuration, and WRITE permission to add/update the configuration of any external authentication server (e.g. LDAP, TACACS) into Crosswork. 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", etc. 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.
Alarms **Attention** The Alarm APIs are deprecated in the Crosswork 6.0 release.	Alarms APIs	Allows you to manage alarms. The READ permission allows you to get events/alarms according to request criteria, get the list of Syslog destinations, and get the list of trap destinations. The WRITE permission allows you to set a response for when an alarm is raised or acknowledged, create/raise an event, update the event info manifest, and add notes to alarms. The DELETE permission allows you to delete REST destinations, Syslog destinations and trap destinations.

Category	Global API Permissions	Description
Automated Assurance DSS Instance	Data Store Service Administrator Settings	Allows Administrators to view Datastore storage info (READ permission) and run diagnostic tests for external storage (WRITE permission).
	Data Store Service API	Allows you to use external storage for longer retention, and to manage external datastore used by Service Assurance for archiving service metrics data. The READ permission allows you to get storage provider information, check storage stats, etc. The WRITE permission allows you to sync the local CW datastore with the external storage and run diagnostics. The DELETE permission allows you to delete an external storage provider.

Category	Global API Permissions	Description
Crosswork Network Controller	CAT FP Deployment Manager APIs	Allows you to manage function pack upload and deployment. The READ permission enables you to get the list of packages, files, and deployment information. The WRITE permission allows you to upload/deploy/un-deploy a package/function pack/file. The DELETE permission is not applicable for these APIs.
	CAT Inventory RESTCONF APIs	North Bound Interface (NBI) RESTCONF interface for the CAT services inventory data (from CAT to external consumers). The READ permission allows you to fetch the services information from CAT, while the WRITE permission allows you to invoke operations APIs to retrieve the service information from CAT. The DELETE permission is not applicable for these APIs.
	CAT ISTP REST APIs	System use only. The READ/WRITE permissions are mandatory for CAT UI/ISTP to function. The DELETE permission is not applicable for these APIs.
	CAT Service Overlay APIs	Primarily used to investigate issues in the overlay. Only READ permission is applicable.
	CAT UI APIs	Mandatory APIs that enable CAT UI to fetch all NSO services and resources. The READ permission allows you to fetch and display all service information, while WRITE permission allows you to commit service assurance information. The DELETE permission is not applicable for these APIs.
	NSO Connector APIs	Allows you to perform services resync, full-resync, change log-level and return service HA status. The READ permission allows you to check the service status, while WRITE permission is required for all other operations. The DELETE permission is not applicable for these APIs.
	OAM Service APIs	Not Applicable

Category	Global API Permissions	Description
Change Automation	Administration APIs	Provides administrative control to manage job scheduling, manage override credentials, and configuration of user roles for playbook executions.
		The READ permission allows you to check the status and fetch the information, while the WRITE permission allows you to make changes. The DELETE permission is not applicable for these APIs.
	Application APIs	Allows you to manage the Change Automation tasks (for example, schedule playbook executions, execute playbooks, update playbook jobs, check playbook executions status, check playbook job-set details, list supported YANG modules, etc.)
		The READ permission allows you to view the applicable information (for example, check the job status, fetch job details, etc.), while the WRITE permission is required for playbook job scheduling/execution. The DELETE permission is not applicable for these APIs.
	Playbook APIs	Allows you to manage playbooks.
		The READ permission allows you to retrieve playbooks, params, and policy specs.
		The WRITE permission allows you to import/export, and generate playbooks.
		The DELETE permission enables you to delete playbooks.
	Play APIs	Allows you to manage plays.
		The READ permission allows you to fetch or view plays, while the WRITE permission allows you to create, update or import a play. The DELETE permission allows you to delete a play.
Collection Infra	Collection APIs	Permissions for APIs to manage collection jobs.
		Based on the READ/WRITE/DELETE permissions, you can view collection jobs, create/update new collection jobs (external), or delete existing collection jobs. System collection jobs (data collection setup internally for Crosswork consumption) cannot be modified irrespective of these permissions (permitted for Administrators only), but users with the READ permission will be able to view the details of all collection jobs including system collection jobs.
		For most users, READ-only permissions would be enough as it enables them to view Collection jobs detail (request and status) and actual data collection status/metrics per device/sensor path level.
	Data Gateway Manager APIs	Permissions to perform CRUD operations on Destinations, Data Gateways, Custom Packages, etc.
		The READ permission allows you to view the data, while the WRITE permission allows you to add/update/delete the data.

Category	Global API Permissions	Description
Crosswork Optimization Engine	OPTIMA Analytics API	Allows you to manage analytics in Crosswork Optimization Engine. The READ permission allows you to view/export historical data, while WRITE permission enables you to change the Traffic Engineering Dashboard settings.
	Optimization Engine UI APIs	Allows you to manage SR policies, RSVP tunnels, LCM, BWoPT, BWoD, Traffic Engineering settings, and Preview policies. The READ permission allows you to view deployed policies, settings, routes, LCM domain config/data, service overlay data, path queries, dashboard metrics, etc. The WRITE permission allows you to configure LCM, BWoD, BWopt, deploy policies, preview Crosswork Optimization Engine-managed policies, etc. The DELETE permission allows you to delete SR policies, RSVP tunnels, remove affinity mapping, and delete LCM domains.
Crosswork Optimization Engine v2	Optimization Engine RESTCONF API v2	Allows you to customize the RESTCONF interface permissions in Crosswork Optimization Engine. The READ permission enables you to fetch L2 and L3 topology details, and Segment Routing Policy details. The WRITE permission allows you to fetch policy routes, provision/modify/delete/preview SR policies, and manage LCM configuration. The DELETE permission is not applicable for these APIs.
Data Gateway Global Settings	Data Gateway Global Parameters API	There are certain parameters in the data gateway, which can be changed globally across all gateways in a Deployment. The READ permission allows you to view the data, while the WRITE permission is required to reset/update the data.
	Data Gateway Global Resources Reset API	Allows you to reset updates done to the Global Parameters. The READ permission allows you to view the data, while the WRITE permission resets the data.
	Data Gateway Global Resources Update API	Allows you to update the Global Parameters. The READ permission allows you to view the data, while the WRITE permission updates the data.

Category	Global API Permissions	Description
Data Gateway Troubleshooting	Data Gateway Reboot API	Reboots a data gateway. The WRITE permission allows you to reboot the data gateway.
	Data Gateway Showtech API	Generates and downloads showtech logs for a data gateway. The READ permission allows you to view showtech, while WRITE permission generates showtech. Write Permission allows u to generate showtech
Health Insights	Health Insights APIs	Allows you to manage Heath Insights KPIs. The READ permission allows you to view all KPIs, KPI profiles, job details, alerts, etc. The WRITE permission allows you to create or update KPIs and KPI profiles, enable/disable KPI profiles, link KPIs to playbooks, etc. The DELETE permission allows you to delete custom KPIs and KPI profiles.
ICON Server	ICON Server APIs	Allows you to update the collection setting for interface/IP data collection intended for topology and optimization use cases.

Category	Global API Permissions	Description
Inventory	Inventory APIs	Allows you to manage inventory.
		The READ permission allows you to
		• Fetch the list of nodes, the node credentials, and the count of nodes in the database.
		• Retrieve the list of HA pools, data gateway enrollments, virtual data gateways, and inventory job information.
		• Retrieve the list of policies, providers, and tags.
		The WRITE permission allows you to
		• Update device mapping to virtual data gateway pool.
		• Lock/unlock the requested nodes.
		• Remove tag associations from nodes. Does not support partial un-assignment.
		• Update input data to a set of devices.
		• Set API endpoint for provider onboarding.
		The DELETE permission allows you to
		• Perform bulk deletion of credential profiles and nodes.
		• Upload CSV for delete operations.
		• Delete HA pools, Data Gateway enrollments, and virtual data gateways.
		• Delete policies, providers, and tags.

Category	Global API Permissions	Description
Platform	Platform APIs	The READ permission allows you to fetch the server status, cluster node information, application health status, collection job status, certificate information, backup and restore job status, etc. The WRITE permission allows you to • Enable/disable the xFTP server • Manage cluster (set the login banner, restart a microservice, etc.) • Rebalance cluster resources • Manage nodes (export cluster inventory, add VM, apply VM configuration, remove VM from a cluster, etc.) • Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, etc.) • Perform normal/data-only backup and restore operations. • Manage applications (activate, deactivate, uninstall, add package, etc.) The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.
	Distributed Cache APIs	The READ permission allows you to fetch cache statistics for troubleshooting.
	Grouping APIs	Grouping management and Topology groups selection tree. The READ permission allows you to view topology UI, while the WRITE permission allows you to create/update groups. The DELETE permission is needed to delete groups from the Grouping Management page. **Note** When READ access is removed for Grouping APIs, in addition to being blocked out of the Grouping window, the users will also be unable to access the Traffic Engineering, VPN Services, and Topology Services windows.
	View APIs	Views Management in Topology. 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.

Category	Global API Permissions	Description
Topology	Geo APIs	Provides geo service for offline maps. The READ permission allows you to use Geo Map in offline mode, the WRITE allows you to upload Geo Map files, and DELETE permission allows you to delete the map files in settings.
	Topology APIs	Allows you to manage topology pages, settings, or any other pages that uses the Topology visualization framework. The READ permission is mandatory for topology visualization. The WRITE permission enables you to update topology settings, and the DELETE permission allows you to delete a topological link if it goes down.
Proxy	Crosswork Proxy APIs	Permissions to manages Crosswork proxy APIs for NSO Restconf NBI. The READ permission allows all GET request for NSO REST conf NBI, the WRITE permission allows POST/PUT/PATCH operation, and the DELETE permission enables all delete APIs.
SWIM	SWIM NB API	Allows you to upload images to the SWIM repository, distribute them to devices and install them. The READ permission allows you to list all images from the SWIM repository, view image information from a device, and check the details of any SWIM job. The WRITE permission allows you to upload/distribute and perform all install-related operations. The DELETE permission allows you to delete copied images from a device. You require WRITE/DELETE permission to execute software install/uninstall playbooks in Change Automation.

Category	Global API Permissions	Description
Service Health	Archiver APIs	The READ permission allows you to • Check if Historical Data exists for a given service. • Get the Historical Timeline series for a given service. • Get a Service Graph for a selected timestamp of the service. • Get Service-Metric data The WRITE/DELETE permissions are not applicable for these APIs.
	Assurance Graph Manager APIs	The READ permission allows you to • Fetch details of a service. • Get the impacted list of services. • Retrieve the list of matching sub-services (transport or device only). The WRITE/DELETE permissions are not applicable for these APIs.
	Heuristic Package Manager APIs	Permissions for Heuristic package management and to manage plugins and config profiles for Service Assurance. The READ permission allows you to export heuristic packages, query for heuristic package details (Rules, Profiles, SubServices, Metrics, Plugins), and query for assurance options. The WRITE permission allows you to import heuristic packages and perform all create/update operations. The DELETE permission allows you to perform delete operations (for example, delete the RuleClass, MetricClass, etc.)

Category	Global API Permissions	Description
Zero Touch Provisioning	CW Config Service APIs	The READ permission allows you to • List all day-0 configuration files stored in the ZTP config repository. • Fetch count of day-0 configuration files stored in the ZTP config repository. • Download the day-0 configuration file from the ZTP config repository. • List all device family/device versions and device platforms based on information associated with day-0 config files stored in the CW ZTP repository. The WRITE permission allows you to • Upload the day-0 config file or script to the ZTP config repository. • List/update relevant metadata associated with specific day-0 config files stored in the ZTP config repository The DELETE permission allows you to delete config files and scripts uploaded in the ZTP config repository.
	CW Image Service APIs	The READ permission allows you to • List all device image files stored in the ZTP image repository. • List all device platform/family names associated with image files stored in the CW ZTP repository. • Download the device image file by ID. The WRITE permission allows you to update relevant metadata associated with specific image files stored in the ZTP image repository. The DELETE permission allows you to delete image files uploaded in the ZTP image repository
	CW ZTP Service APIs	Allows you to manage the ZTP devices and profiles - add/update/delete into Crosswork. The READ permission enables you to fetch ZTP devices, serial number/OVs, profiles, sample data CSV, list ZTP devices, profiles, and export ZTP devices and metadata. The WRITE permission allows you to add ZTP devices, serial numbers/OVs, profiles and add/update the ZTP device's attributes. The DELETE permission allows you to delete ZTP devices, profiles, serial numbers/ownership vouchers.

Category	Global API Permissions	Description
CW-CLMS	Common Licensing Management Service (CLMS) APIs	Permissions for APIs to manage license registration in Crosswork. The READ permission enables you to view Smart Licensing settings, registration status, and license usage while the WRITE permission is required to change any Smart Licensing setting such as register, re-register, de-register, renew a license etc.

Manage Active Sessions

As an administrator, you can monitor and manage the active sessions in the Cisco Crosswork 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.

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

The **Active Sessions** tab displays all the active sessions in the Cisco Crosswork with details such as user name, source IP, 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. 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 Session**. 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.

Manage WebSocket Subscriptions

If you have subscribed to WebSocket subscriptions using **Basic Authentication** or **JWT** based authentication to authenticate and establish your connections, you can view these subscriptions in the Crosswork UI. The types of subscriptions that are supported are-

- Inventory

- Alarm

- Service Notification

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

Step 2 Click the **WebSocket subscriptions** tab.

It displays details such as **Subscription ID**, **Topic**, **Subscribed By** , **Subscription Time** and **Source IP.**

Crosswork Network Controller

Users and Roles

Dashboard

Users   Roles   Active sessions   **WebSocket subscr**

Topology

Device Management

☐	**Subscription ID**	**Topic**
☐	24458	inventory
☐	23858	alarm

Alerts

Administration

Note   • The **Source IP** column appears when you check the **Enable source IP for auditing** check box. This option is available in the Source IP section of the **Administration** > **AAA** > **Settings** page.

You can also choose to delete a subscription by using the **Delete** icon on this page.

Manage Device Access Groups

Crosswork offers access control based on user roles, with read/write/delete permissions for specific APIs grouped by functional areas.

While this centralizes access control, it does not extend to device-level access. To manage device access for users, Device Access Groups can be used to logically group devices. Non-admin users assigned to the system-level task of Device Access Groups management can create and manage these groups.

APIs, Tasks and Device Access Groups- Know the Difference

Device Access Groups are not directly related to API access control or task-based access control. Here's a breakdown of their differences and roles:

- **APIs**: Control read/write/delete access levels to the APIs but do not control the UI access of a user. Permissions for APIs are defined and enforced at the API level, allowing administrators to specify what actions a user can perform.

- **Tasks**: Control access to certain functionalities by combining a set of APIs. Enabling a specific task also enables the corresponding APIs required for that task.

- **Device Access Groups**: Serve as an extra security layer to control access to specific devices or resources within Crosswork, beyond API and task-based access controls. They are used to logically group devices for user management.

Administrators have full control over building user roles and permissions, including defining Device Access Groups. Device Access Groups become relevant only after a user has passed the initial API-based and/or task-based access controls set by an administrator. Once these initial access levels are granted, Device Access Groups provide additional control over which devices a user can have WRITE permissions for provisioning.

Administrators can configure Device Access Groups according to specific requirements, adding an extra layer of control and customization for access management within Crosswork.

How do Device Access Groups work?

When a user is associated with one or more Device Access Groups, they can make configuration changes and provision services on the devices within those groups. A Crosswork user with an administrator role or a mapped Device Access Groups management task can:

- Create and manage Device Access Groups.

- Assign users to specific Device Access Groups.

- Define and control which devices users can access and modify.

- Ensure that users have the appropriate permissions to perform their tasks on designated devices.

☞

Important   Device Access Groups control device-level WRITE or Provisioning and Crosswork flows that trigger such operations. They do not affect WRITE or EDIT operations within Crosswork itself.

You can restrict users to specific tasks based on their role's permissions, ensuring only authorized individuals have access and control over their actions within the system. Crosswork's role-based access control synchronizes

with NSO and Device Access Groups to streamline device configurations, using JWT tokens for authentication and authorization in RESTCONF and JSON-RPC API workflows. However, reverse synchronization is not possible; changes in NSO are not reflected in Crosswork Device Access Groups (for detailed information on the prerquisites for setting up NSO, see Configure NSO Servers, on page 47). External LDAP, TACACS, and RADIUS servers support Device Access Groups integration. For server configuration details, refer to the specific field description tables for each server in Set Up User Authentication (TACACS+, LDAP, and RADIUS), on page 55.

Create Device Access Groups

To enable seamless device-level granular Role-Based Access Control across Crosswork applications and integrated NSO, create a Device Access Group that will allow for centralized management of device access permissions, ensuring consistent role based access implementation across the system. Only users belonging to a role that has the "Device Access Group Management" task enabled have the ability to perform Create, Read, Update and Delete operations on the Device Access Groups.

Step 1   From the main menu, choose **Administration** > **Device Access Groups**.

Step 2   Click the [...] icon next to ALL-ACCESS, then click **Add Sub-Group.**
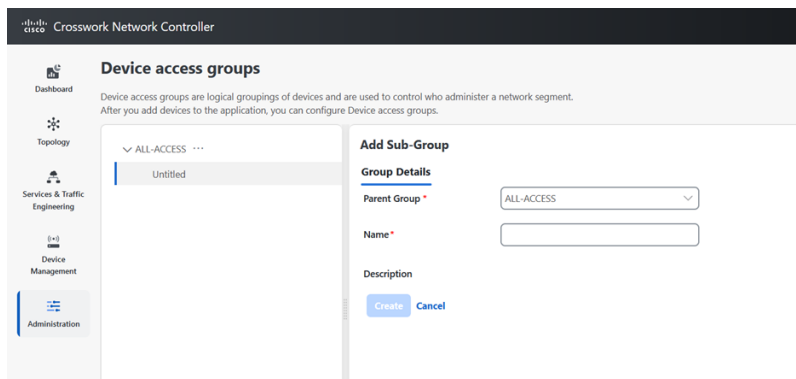
Step 3   Add the name and description of the sub-group under **Group Details**.

Step 4   Click **Create.**

When you add a devices to a Device Access Group, you can view the **Devices** tab next to **Group Details**.

Step 5   Click on **Add Devices**.

Step 6   Select the devices you want to add and click **Save**.

You can also filter the devices that you want to add using the **Filter By** options for **Host Name, Product Type and Node IP**. The devices are added under Device Access Groups as well as updated in the NSO site.

Step 7   Click **Save**.

Edit Device Access Groups

You can add or remove a device from an existing Device Access Group.

> ⚠️
>
> **Attention** The delete group check is only relevant for local users defined in Crosswork and does not apply to users managed by external AAA servers.

Step 1 From the main menu, choose **Administration** > **Device Access Groups**.

Step 2 Click the Device Access Group that you want to edit and then click **Edit Group**.

You can add more devices by clicking **Add Devices** or remove them by clicking **Remove Devices**.

Step 3 Click **Save**.

> **Note** You cannot delete a Device Access Group if a user is exclusively associated with it. However, if all users associated with the Device Access Group also belong to other Device Access Groups, you can delete it.
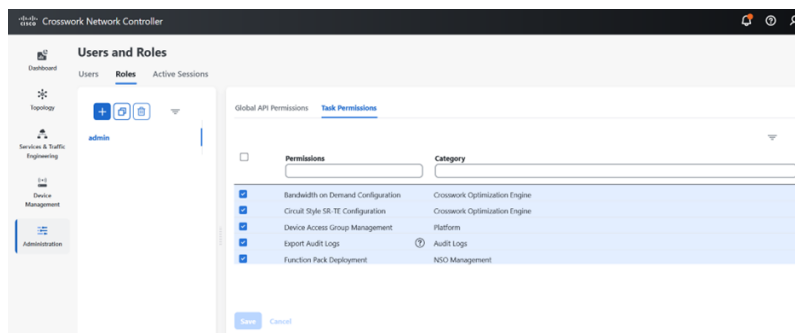

Assign Task permissions

You can assign the tasks that you have created to a specific role. You can enable or disable these tasks based on the permissions you want to give for a role. The task permissions are defined by the Global APIs, which allow you to assign **Read/Write/Delete** permissions for that specific task.

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

Step 2 Click **Task Permissions** to view a list of all the available tasks for your application.

Figure 12: Users and Roles Window

Step 3 Select the task for which you want to assign permissions. Under the **Global API Permissions** tab, you can also view the specific **Read/Write/Delete** permissions that are automatically enabled for the selected task.

Step 4 Click **Save**.

Associate a User with a Device Access Group

Once you have created a user, you can associate that user with a specific Device Access Group. You can then assign task permissions for this user, which lets you restrict or allow certain tasks for them.

Step 1 Create a role with **read/ write/ delete** API permissions and assign the set of specific tasks that need to be enabled within each role. Refer to the section, User Roles, Functional Categories and Permissions, on page 26 for more details.

Step 2 Assign this role and one or more Device Access Group to a user. Refer to the section, Manage Users, on page 24 for more details.

When the user logs in, the user can only perform operations allowed by the tasks on devices belonging to the associated Device Access Groups. Based on task permissions and Device Access Group privileges, a restricted read-only Device Access Group user has the following capabilities while provisioning policies on BWoD, LCM, CSM, DLM, DGM and CAT. Such a user can-

- Preview and dry run policies but cannot provision or commit changes for the policies.

- View Services and Traffic Engineering configuration pages but cannot edit or import files.

- Perform Path Query operations.

- View Services and Traffic Engineering configuration pages but cannot edit or import files.

- Create VPN services.

- View the devices that are associated with a failed service, along with the detailed error message but cannot take actions on the errors.

Correspondingly, a Device Access Group user with all the **read/ write/ delete** permissions has the following capabilities. Such a user can-

- Perform all the tasks listed for a restricted read-only Device Access Group user.

- Provision policies for which they have been granted access to. For instance, if a user wants to create an RSVP-TE policy on a Tunnel, they will be able to do so only if they have been granted access to the head-end node. However, note that access to the end-points and hops is not checked for Device Access Group control.

- View the devices that are associated with a failed service, along with the detailed error message. Additionally, users with all privileges can take actions on errors such as Check-Sync, Sync-To, and Compare-Config at the node level.

- Run and execute Playbooks.

Note To restrict device access in Crosswork for read-only users, the administrators must create an empty Device Access Group (for example, NO_DEVICE_ACCESS) without any devices, and assign it while creating read-only user profiles (or user profiles associated with read-only roles).

Configure NSO Servers

The integration of authentication and authorization between Crosswork and NSO for RESTCONF and JSON-RPC API workflows is facilitated through the use of JWT. To enable role-based access control and seamless synchronization between Crosswork and NSO refer to the prerequisite steps listed under the following sections:

Note • Only administrators are allowed to make modifications to tasks.

• If any changes are made to NACM settings, the user must log out and then log back in. This is necessary to regenerate the JWT.

• When a user with limited device access tries to edit a service or upload an XML file in the Provisioning UI, the **commit** button is enabled. However, it throws an error when the user clicks the **commit** button.

Configure Standalone NSO

Follow the steps below to configure a standalone NSO server to sync role-based access control functions with Crosswork.

Step 1 Enable `cisco-cfp-jwt-auth`.

a) **Update the ncs.conf file:** Open the `ncs.conf`` file in the NSO directory. Add the following configuration under the <aaa> section.

```
 <aaa>
    <package-authentication>
     <enabled>true</enabled>
     <packages>
       <package>cisco-cfp-jwt-auth</package>
     </packages>
    </package-authentication>
</aaa>
- Make sure to restart ncs for the configuration in ncs.conf to take effect:
   /etc/init.d/ncs restart
```

Note Make sure to restart NCS for the configuration in the `ncs.conf` file to take effect. If you do not want to use this feature, change 'package-authentication' to 'false' in '`ncs.conf` in the AAA section under the NCS configuration file and restart NCS. This disables the package authentication for '`cisco-cfp-jwt-auth`'.

b) Copy the certificate file from Crosswork to the NSO VM. To get the certificate from Crosswork to NSO VM, follow these steps:

1. Open the Chrome browser and navigate to the Crosswork website for which you want to import the certificate.

2. Click the padlock icon in the address bar to view the site information and then click **Certificate is not Valid** > **View Certificate**.

Figure 13: View Certificate Window
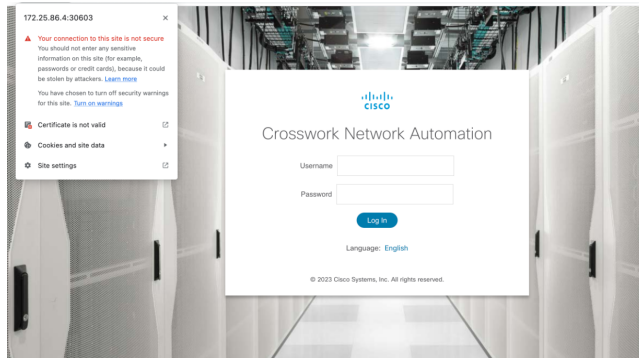
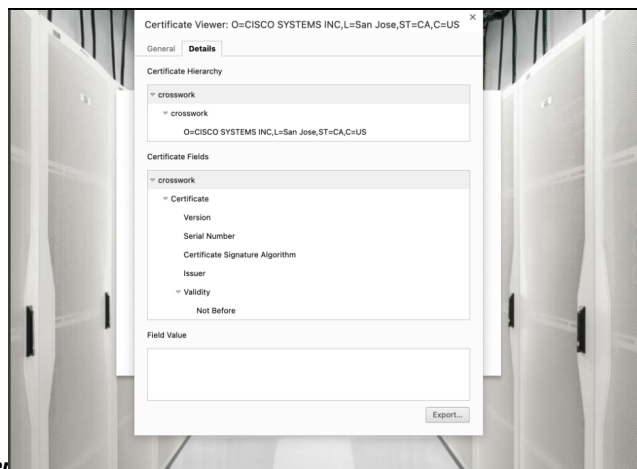3. In the **Certificate Viewer** window, go to the **Details** tab.

Figure 14: Details for Certificate Viewer

4. Click **Crosswork** under **Certificate Hierarchy**.

5. Click the **Export** button and choose a file name and location to save the certificate. Choose the **Base64-encoded ASCII, single certificate** option and save it with the extrension **.pem**. For example: crosswork.pem.

Note   In case you encounter issues saving the file in the .pem format, an alternative is to save it as a .cer file. Once saved, proceed to use this .cer file during the bootstrap configuration process. Make sure to reference the file path of the .cer file in all subsequent steps that require it.

Figure 15: Save the Certificate Window
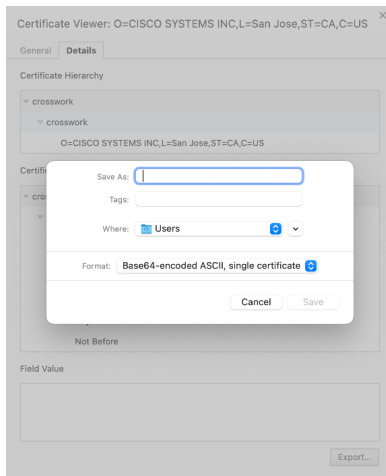
6. Copy the .**pem** file to NSO VM.

   Note   Make sure that the value of the **pem-key-path** parameter and the filename are the same on the primary and secondary host.

c) **Configure Bootstrap:** To configure the Bootstrap authentication package, perform the following steps:

   Login to NSO VM and load the cw-jwt-auth.xml file using the **merge** operation.

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <jwt-auth xmlns="http://cisco.com/ns/nso/cfp/cisco-cfp-jwt-auth">
    <ip-address>172.20.100.42</ip-address>
    <port>30603</port>
    <pem-key-path>/home/nso/crosswork.pem</pem-key-path>
  </jwt-auth>
</config>
```

   OR

   Log in to `ncs_cli` and enter config mode.

```
set jwt-auth cnc-host <Crosswork IP>
set jwt-auth port 30603
set jwt-auth pem-key-path /home/nso/crosswork.pem
commit
```

Step 2   Enable service level NACM.

Before creating a Rule-list, create the NACM group manually and update the user as needed when the same group applies to more that one user.

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

Step 3   Create NACM Groups and Rule list.

a) **For admin users:** Follow the steps below to create NACM groups and Rule-list for admin users.

1. **User Association:** If a NSO user is an admin user, they will automatically be part of the "ncsadmin" group, which grants them all access by default. However, if the admin user does not add this user to the "CNC#ALL-ACCESS" group, the functionalities will still work properly. If the NSO user has a different name, such as "cisco", then you must add the user to the "CNC#ALL-ACCESS" group.

   Note that user creation is not required at this point.

2. **Create Device group:** When a Device Access Group gets created in Crosswork, an equivalent device-group is created in NSO.

   Note that the ALL-ACCESS Device Access Group is not created by default, and is not needed for an admin user. If you want, you can create it manually using the following command, where **group-name** is the name of the group you create.

   ```
   ncs_cli -u admin
   configure
   set devices device-group "group-name" device-name [ device-host-name1, device-host-name2]
   commit dry-run
   commit
   ```

   You can also copy this from Crosswork by navigating to **Administration** > **Users and Roles** > **Users** > **Generate NACM Rules**.

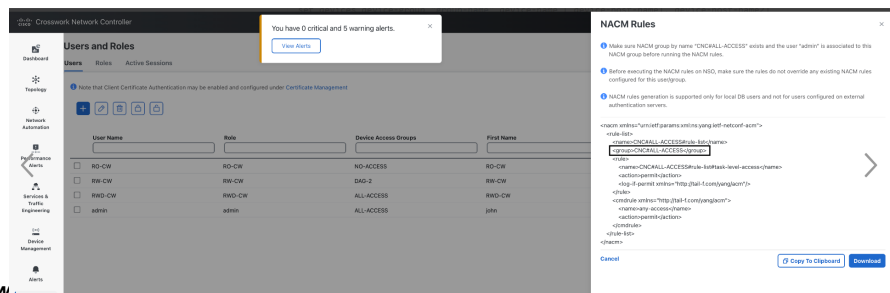*Figure16:GenerateNACMRulesWindow*

3. Create a NACM group manually and update the user as needed when the same group applies to more that one user. Make sure to do this before you create the Rule-list.

   ```
   ncs_cli -u admin
   configure
   set nacm groups group "CNC#ALL-ACCESS" user-name admin
   commit dry-run
   commit
   ```

4. **Create NACM Rule list:** When a User with a Role and Device Access Group is set in Crosswork, the UI displays an option to generate the NACM rules under each user. You can either copy these rules and apply them to NSO using the **commit manager** or copy the xml to the file <sample-nacm.xml> and load it using the **merge** operation. Note that for admin users only the task level access and cmd-rule are required.

   ```
   <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
       <rule-list>
           <name>CNC#ALL-ACCESS#rule-list</name>
           <group>CNC#ALL-ACCESS</group>
           <rule>
               <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
               <action>permit</action>
               <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
           </rule>
           <cmdrule xmlns="http://tail-f.com/yang/acm">
               <name>any-access</name>
   ```

```
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

b) **For non-admin users:** Follow the steps below to create NACM groups and Rule-list for non- admin users.

In the code sample below, we have used RW-CW as an example for non-admin user and DAG-2 as a Device Access Group name.

1. **Create NACM Group:** See the code sample below:

```
ncs_cli -u admin
configure
set nacm groups group "CNC#DAG-2" user-name RW-CW
commit dry-run
commit
```

You can copy the Group name from Crosswork using the **Generate NACM Rules** option.

2. **Create NACM Rule list:** You can copy the Rule list from Crosswork using **Generate NACM Rules** option. Here is a sample-

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <rule-list>
        <name>CNC#DAG-2#rule-list</name>
        <group>CNC#DAG-2</group>
        <rule>
            <name>CNC#DAG-2#rule-list#allow-DAG-2</name>
            <device-group
xmlns="http://tail-f.com/yang/ncs-acm/device-group-authorization">DAG-2</device-group>
            <access-operations>create read update delete exec</access-operations>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <rule>
            <name>CNC#DAG-2#rule-list#deny-others</name>
            <path>/devices</path>
            <access-operations>create update delete exec</access-operations>
            <action>deny</action>
        </rule>
        <rule>
            <name>CNC#DAG-2#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

You can push these rules to NSO via commit manager or copy them to a xml file (For example: sample-nacm.xml) and then add it on NSO with these commands:

Load sample-nacm.xml

```
ncs_cli -u admin
configure
```

```
load merge /home/nso/sample-nacm.xml
commit
```

Configure LSA NSO

Follow the steps below to configure a LSA NSO server to sync role-based access control functions with Crosswork.

Step 1 Enable local authentication in the `ncs.conf` file under the AAA section on all the NSO RFS nodes. (If you are using the CFS node, you can skip this step)

```
<local-authentication>
      <enabled>true</enabled>
</local-authentication>
```

Restart NSO by running the command `sudo /etc/init.d/ncs restart` on each RFS node.

Step 2 **Enable cisco-cfp-jwt-auth:** Refer to the same steps to enable `cisco-cfp-jwt-auth` as described in the section, Configure Standalone NSO, on page 48.

Make sure that the value of the **pem-key-path** parameter and the filename are the same on the primary and secondary host.

Step 3 Enable service level NACM.

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

You must enable this on both the CFS and RFS nodes.

Step 4 Create NACM Groups and Rule list. (This is applicable for both admin users and non admin-users)

a) **Associate Users:** To enhance security with LSA role-based authentication in NSO, we recommend that you remove the "auth-group default" map if NSO is exclusively used with Crosswork. However, if there are non-Crosswork NSO users, they must use the default map. In this case, every Crosswork user must have an entry in the "auth-group umap" to ensure the Role-Based Access Control flow functions correctly.

b) Define a Crosswork user under "aaa:aaa" as an authentication user on every RFS node. This configuration enables communication between CFS and RFS for this user. Note that the username must match the username used in Crosswork, but the password can differ.

c) Add every Crosswork user as a "umap" entry under the device authentication group in the CFS. This ensures proper functionality and enforces Role-Based Access Control for users in Crosswork. This also allows the CFS to pass user requests to the RFS node as the corresponding user. If you want a role-based access for a user, you must create the umap entry in the CFS auth-group. Otherwise, the default map applies, which breaks the role-based access workflow.

d) Define a generic NACM group and NACM rule with all permissions on the CFS, to enable access to RFS nodes for all users. This grants access to RFS for all users. Additionally, when creating any user in Crosswork, add that user to the "CNC#ALL-ACCESS" NACM group in CFS. This ensures that the user has the necessary access privileges and permissions to perform actions within Crosswork.

```
group "CNC#ALL-ACCESS" {
      user-name [ RW-CW admin rw-user ];
   }
```

You can copy the NACM rules from Crosswork.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <!--NACM rules for NSO - CFS-->
    <rule-list>
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <!--NACM rules for NSO - RFS-->
    <rule-list>
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

Step 5   **Create Device group:** Add the Device Access Groups and NACM rules on the RFS node. By defining NACM rules for a user, access to devices can be granted based on the specific rules that you configure for that user. Note that Device Access Group creation is automatically handled by Crosswork, so you do not need any additional steps for Device Access Group creation on NSO.

Note   If you have Geo-HA set up, and encounter the 503 error, follow the steps below to resolve it.

Add the following configurations exclusively to the **/etc/environment** file within the CFS node:

a) Open the file `sudo vi /etc/environment`.

b) Add the following lines:

```
https_proxy="http://proxy.esl.cisco.com:80"
http_proxy="http://proxy.esl.cisco.com:80"
```

c) Define exceptions with the line:

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,<az1 mgmt vip>,<az2
 mgmt vip>,<fqdn of CW geo-mgmt VIP>"
```

For example:

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,
192.168.6.50,192.168.5.50,geomanagement.cw.cisco,cw.cisco"
```

d) Source the file: `source /etc/environment`

e) Reboot the CFS nodes for the proxy settings to take effect.

Set Up User Authentication (TACACS+, LDAP, and RADIUS)

In addition to supporting local users, Crosswork Network Controller supports TACACS+, LDAP, and RADIUS users through integration with the TACACS+, LDAP, and RADIUS servers. The integration process has the following 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 68.

- You can create and manage Device Access Groups for users on these servers. For more information, see Manage Device Access Groups, on page 44.

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 27.

- 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.

- Cisco Crosswork supports the configuration of up to 5 external 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.

Manage TACACS+ Servers

Crosswork 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

- Create Device Access Group to manage access to the AAA operations. For more information, see Create Device Access Groups, on page 45

- 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 Crosswork Network Controller. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

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 6: 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.
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.

Field	Description
Policy Id	Enter the user role that you created in the TACACS+ server. **Note** If you try to login to Crosswork Network Controller 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. Login as a local admin user and create the missing user roles in the TACACS+ server, and login back to Crosswork using the TACACS+ user credentials.
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in (ISE/Standalone) TACACS+ server attributes. These values can be one or more than one comma separated values.
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 checkbox next to the TACACS+ server and click ✎.

b) After making changes, click **Update**.

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

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

b) Click **Delete** to confirm.

Example

In this example, the TACACS+ parameters are configured in Cisco ISE. As a prerequisite, a Device Access Group has been created in Crosswork to manage the AAA operation access.

The relevant TACACS+ parameters are configured in Cisco ISE:

• User profile: `role0` (to be used in *Policy Id* field)

- Device Access Group Attribute: `DAG-CONFIGURE`

- Shared secret format: `ASCII`

Figure 17: Configure TACACS+ Profile Attributes in Cisco ISE

Figure 18: Configure TACACS+ Authentication Settings in Cisco ISE
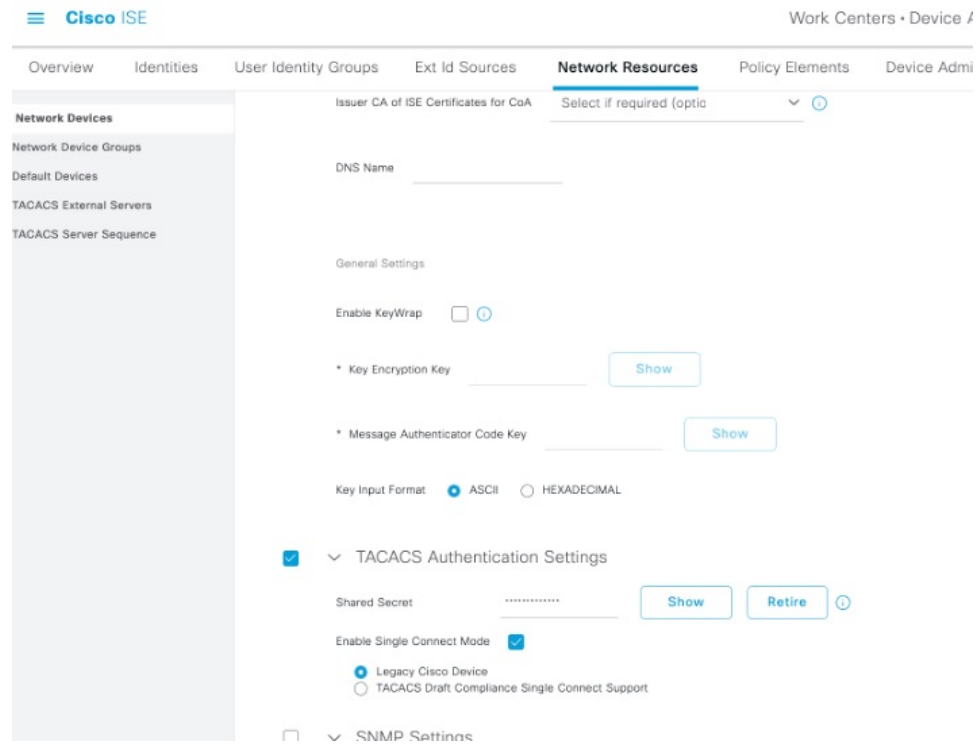
Now, the TACACS+ server is added in Crosswork UI:

Figure 19: Add TACACS+ Server

Here is the sample API payload for the above example:

```
{
    "tacacs":{
        "tacacs_servers":[
            {
                "priority":10,
                "host":"cw-qa-ise-1-ipv4",
                "dnsName":"",
                "port":49,
                "secretFormat":"ascii",
                "secret":"sample",
                "service":"raccess",
                "policy-id": "role0",
                "virtualDomain":"deviceAccessGroups"
                "timeout":30,
```

```
                  "retries":10,
                  "authType":"pap",
              }
          ]
       }
  }


  ------------------------------------------------------------------------------
  CROSSWORK                                    CISCO ISE
  VALUE
  ------------------------------------------------------------------------------
  Device Access Group Attribute=deviceAccessGroups    deviceAccessGroups=DAG-CONFIGURE
  DAG-CONFIGURE
  PolicyId=role0                               role0=ReadWrite
  ReadWrite
```

Manage LDAP Servers

Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. Crosswork 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 a New Certificate, on page 7.

Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see Create Device Access Groups, on page 45

- Configure the relevant parameters (bind DN, policy baseDN, policy id, device access group attribute, etc.) in the LDAP server before configuring the AAA server in Crosswork Network Controller.

Step 1   From the main menu, select **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 7: 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 login 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 Attribute 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 login to Crosswork Network Controller as a 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 Crosswork.
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in LDAP server attributes. These values can be one or more than one comma separated values.
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 a LDAP server**:

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

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

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

Example

The below example shows the parameters entered for secure LDAP configuration. As a prerequisite, a Device Access Group has been created and configured in Crosswork to manage the AAA operation access.

The relevant parameters are configured in the LDAP server. Here are some of the key points:

- The user role is `ldapa-user1` and it belongs to the user group `ldapAdmin`.

- The username is this example is `DSEENIVA`.

- The policy id is `sAMAccountName`.

- The `ldapUrl` parameter is a combination of address and port

- The parameters under the `ldap_attr_server` section are used for role mapping. The `baseDN` parameter maps to the *Policy baseDN* field and the `userFilter` parameter maps to the *Policy Map Attribute* field in the Crosswork UI.

- The device access group is configured in LDAP server as `'Description='ALL-ACCESS'`.

The user group and user role mapping configured in LDAP server:

Figure 20: Add LDAP Server
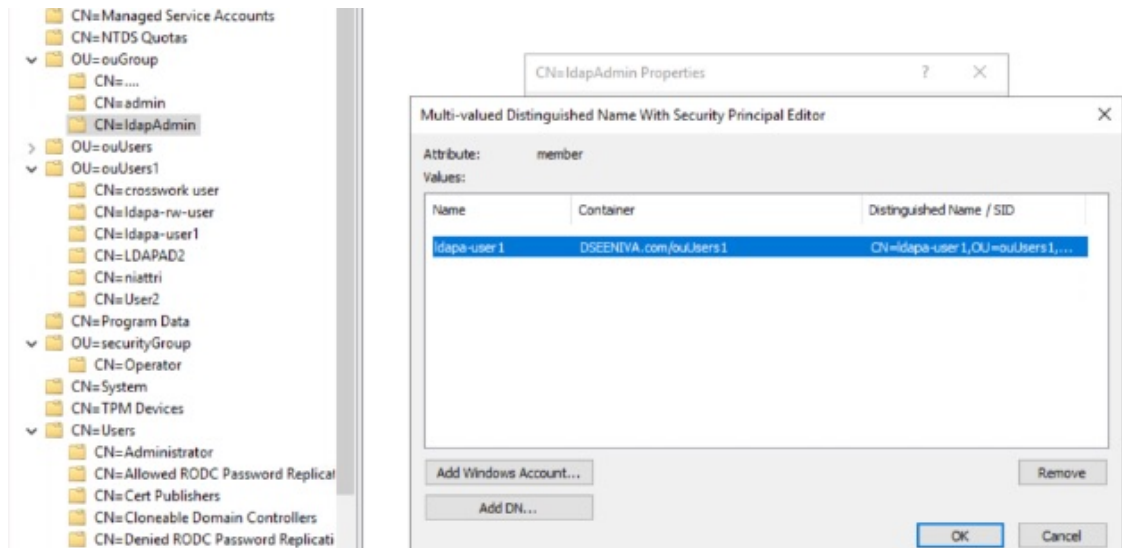
Here is the sample API payload for this example:

```
{    "ldap": {
    "ldap_servers": {
      "ldap_server": [{
          "type": "DIRECT",
          "bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "connectionStrategy": "",
          "useSsl": false,
          "useStartTls": false,
          "connectTimeout": 10,
          "baseDn": "OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "userFilter": "cn={user}",
          "subtreeSearch": true,
          "usePasswordPolicy": false,
          "dnFormat": "cn=%s,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "principalAttributeId": "cn",
          "policyId": "Description",
          "minPoolSize": 1,
          "maxPoolSize": 1,
          "validateOnCheckout": false,
          "validatePeriodically": true,
          "validatePeriod": 600,
          "idleTime": 5000,
          "prunePeriod": 5000,
          "blockWaitTime": 5000,
          "providerClass": "org.ldaptive.provider.unboundid.UnboundIDProvider",
          "allowMultipleDns": false,
          "order": 16,
          "trustStore": "ldaps",
          "name": "ldapsecure",
          "ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
          "bindCredential": "<>"
        }
      ],
      "ldap_attr_servers": {
        "ldap_attr_server": [
          {
            "baseDn": "OU=ouGroup,dc=DSEENIVA,dc=COM",
            "trustStore": "ldaps",
```

```
"ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
"bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
"bindCredential": "<>",
"userFilter": "member=cn={user},OU=ouUsers1,dc=DSEENIVA,dc=COM",
"failFast": false,
"attributes": {
"policy_id":"sAMAccountName"
}}]}}}}
```

Here is the corresponding LDAP configuration in the Crosswork UI:

Figure 21: Add LDAP Server

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

- Create Device Access Group to manage access to the AAA operations. For more information, see Create Device Access Groups, on page 45

- 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 Crosswork Network Controller. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

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 8: 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 TACACS+ 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 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 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 Crosswork Network Controller 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. Login as a local admin user and create the missing user roles in the RADIUS server, and login back to Crosswork using the RADIUS user credentials.
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in RADIUS server attributes. These values can be one or more than one comma separated values.
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 55 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.

Configure AAA Settings

Users with relevant AAA permissions can configure the AAA settings.

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

Step 2   Select the relevant setting for **Fallback to Local**. By default, Crosswork 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 a relevant value for the **Number of Parallel Sessions**.

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

Note   Crosswork supports 50 simultaneous NBI sessions up to 400 sessions (in Crosswork Network Controller version 4.1.x) and 500 sessions (in Crosswork Network Controller version 5.0.x).

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, 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 is 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 Crosswork , and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

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, 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.

When Crosswork is re-installed, 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.

✎

Note   The Cisco Crosswork 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 on the **Administration** > **AAA** > **Settings** page.

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.

Figure 22: Identity Provider window

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.

Security Hardening Overview

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

• Cisco Crosswork infrastructure

• Cisco Crosswork storage system (local or external)

Hardening Cisco Crosswork security requires completion of the following tasks:

• Shutting down insecure and unused ports

• Configuring network firewalls

• Hardening the Cisco Crosswork infrastructure, as needed

Although your primary source of information is your Cisco representative, who can provide server hardening guidance specific to your deployment, you can also follow the steps in this section to secure Cisco Crosswork.

Authentication Throttling

Cisco Crosswork throttles the login attempts after a failed login attempt to avoid password guessing and other related abuse scenarios. After a failed login attempt for a username, all authentication attempts for that username would be blocked for 3 seconds. The throttling is applicable to all supported authentication schemes such as TACACS, LDAP and the default local authentication.

Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco Crosswork product, you should have a good understanding of the following security concepts.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco Crosswork now supports TLS only.

Note TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

X.509 Certificates

X.509 certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.

2. Installing the identity certificate on the server.

3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.

- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL or x.509 certificate) to the client in order to verify its identity.

The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco Crosswork server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.

Note   A client might need to store multiple server certificates to enable interaction with multiple servers.

To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

Disable Insecure Ports and Services

As a general policy, any ports that are not needed should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco Crosswork. You can do this by listing the ports that are open and comparing it with a list of ports needed for Cisco Crosswork.

To view a list of all open listening ports:

Step 1   Log in as a Linux CLI admin user and enter the **netstat -aln** command.
The **netstat -aln** command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. The command returns output similar to the following:

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto  Recv-Q  Send-Q  Local Address            Foreign Address          State
tcp    0       0       0.0.0.0:111              0.0.0.0:*                LISTEN
tcp    0       0       127.0.0.1:8080           0.0.0.0:*                LISTEN
tcp    0       0       0.0.0.0:22               0.0.0.0:*                LISTEN
tcp    0       0       127.0.0.1:25             0.0.0.0:*                LISTEN
tcp    0       0       127.0.0.1:10248          0.0.0.0:*                LISTEN
tcp    0       0       127.0.0.1:10249          0.0.0.0:*                LISTEN
tcp    0       0       192.168.125.114:40764    192.168.125.114:2379     ESTABLISHED
tcp    0       0       192.168.125.114:48714    192.168.125.114:10250    CLOSE_WAIT
tcp    0       0       192.168.125.114:40798    192.168.125.114:2379     ESTABLISHED
tcp    0       0       127.0.0.1:33392          127.0.0.1:8080           TIME_WAIT
tcp    0       0       192.168.125.114:40814    192.168.125.114:2379     ESTABLISHED
tcp    0       0       192.168.125.114:40780    192.168.125.114:2379     ESTABLISHED
tcp    0       0       127.0.0.1:8080           127.0.0.1:44276          ESTABLISHED
tcp    0       0       192.168.125.114:40836    192.168.125.114:2379     ESTABLISHED
tcp    0       0       192.168.125.114:40768    192.168.125.114:2379     ESTABLISHED
tcp    0       0       127.0.0.1:59434          127.0.0.1:8080           ESTABLISHED
tcp    0       0       192.168.125.114:40818    192.168.125.114:2379     ESTABLISHED
tcp    0       0       192.168.125.114:22       192.168.125.1:45837      ESTABLISHED
tcp    0       0       127.0.0.1:8080           127.0.0.1:48174          ESTABLISHED
tcp    0       0       127.0.0.1:49150          127.0.0.1:8080           ESTABLISHED
tcp    0       0       192.168.125.114:40816    192.168.125.114:2379     ESTABLISHED
tcp    0       0       192.168.125.114:55444    192.168.125.114:2379     ESTABLISHED
```

Step 2   Check the *Crosswork Network Controller 7.0 Installation Guide* for the table of ports used by Cisco Crosswork, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product*.

Note   If you are not sure whether you should disable a port or service, contact the Cisco representative.

Step 3   If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork to operate.

Harden Your Storage

We recommend that you secure all storage elements that will participate in your Cisco Crosswork installation, such as the database, backup servers, and so on.

• If you are using external storage, contact the storage vendor and the Cisco representative.

• If you are using internal storage, contact the Cisco representative.

• If you ever uninstall or remove Cisco Crosswork, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted). Contact the Cisco representative for more information.

Configure System Settings

Administrator users can configure the following system settings:

Configure a Syslog Server

Crosswork allows external syslog consumers to:

- Register on Crosswork to receive system events, audit events, and internal collection jobs from the Syslog and Trap servers.

- Define and filter which kind of events should be forwarded as a syslog, per consumer.

- Define the rate at which syslogs are forwarded to the consumer.

> **Note** After the Syslog TLS server certificate is added, wait for 5-10 minutes before configuring the syslog server.

> **Attention** The APIs to configure a syslog server are deprecated in the Crosswork 6.0 release.

Before you begin

Ensure that you have uploaded the Syslog TLS server certificate. For more information, see Add a New Certificate, on page 7.

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

Step 2 Under **Server**, click the **Syslog Configuration** option.

Step 3 Click ➕.

Step 4 Enter Syslog configuration details. For more information, click ⓘ next to each option.

Use the **Criteria** option to define the scope and range of which kind of events should be forwarded as a syslog. For example: **(EventSeverity<2 or EventSeverity>=5) and OriginAppId=capp-infra and EventCategory=1**

The expression sends events as a syslog only if the event originates from the Infrastructure Platform, the category is the system, and the severity is either less than 2 or is equal or above 5.

Caution Expressions are freeform and not validated.

Step 5 Click **Save**.

Syslog Events

After the Syslog destination is configured, Crosswork generates events in the form of Syslogs and sends it to the Syslog destination. The events have the following format:

<pri><v> <stamp> <vip> <app> <PID> <Message ID> <Structure Data> <Message>

The following table lists the fields that are sent in syslogs.

Table 9: Syslog Event Fields and Description

Field	Description	Example

`Pri`	The priority of the event generated:
	
	`Priority = (8*facility + severity)`
	
	Where `facility` is the category of the event generated.
	
	The category of the event generated represented using an integer value:
	
	`System = 3, Network = 7, Audit = 13, Security = 4, External = 1`
	
	The alarm severity indicates the severity of the event using an integer value:
	
	`Critical=2, Major=3, Warning=4, Minor=5, Info=6,Clear=7`
		Event with the Category as System and Severity as Major, the PID = 8 * 3 + 3 = 27.

`v`	The version of the Syslog server.	NA
`Stamp`	The timestamp at which the event is created.	`Mar 28 15:2:22 10.56.58.188`
`VIP`	The Crosswork VIP address.	`10.56.58.188`
`App`	The event OriginServiceId and OriginAppId.	`orchestrator-capp-infra`
`PID`	The process ID.	NA
`Message ID`	The event ID.	`8586f9cf-d05d-4d94-ab62-27d7e808b5f6`
`Structured Data`	The event ObjectId and event type.	`robot-topo-svc-0`
`Message`	The description of the event.	`Restart of robot-topo-svc successful.`

Configure a Trap Server

Cisco Crosswork allows external trap consumers to:

- Register on Crosswork and receive system events and audit log as traps.

- Define and filter which kind of events should be forwarded as a traps, per consumer.

- Define the rate of which traps are forwarded to the consumer.

For more information on trap handling, see Enable Trap Handling.

⚠️

Attention The APIs to configure a trap server are deprecated in the Crosswork 6.0 release.

Follow the procedure below to manage Trap Servers from the Settings window:

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

Step 2 Under **Server**, click the **Trap servers** option.

Step 3 Click ➕ .

Step 4 Enter Trap server details. For more information, click ⓘ next to each option.

Use the **Criteria** option to define scope and range of which kind of events should be forwarded as a trap.

Click **Events and Alarms examples** for more information on the attributes used to raise an event.

Step 5 After entering all the relevant information, click **Add**.

Configure the Interface Data Collection

Crosswork Data Gateway collects the interface state and stats data such as name, type, and traffic counters from the devices through the SNMP or gNMI protocol. Crosswork Data Gateway starts the data collection when a device is onboarded and attached to the data gateway.

Follow the steps to configure interface data collection settings:

Before you begin

Create a tag and assign it to the device for which Crosswork collects the interface data. For information on how to create and assign a tag to the device, see Create Tags and Apply or Remove Device Tags.

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

Step 2 Under **Data Collection**, select **Interfaces**.

Figure 23: Interface Data Collection Window

Step 3 In the **Interface Data Collection** pane, select the appropriate method:

- SNMP: Crosswork collects the IF-MIB and IP-MIB data from the devices.

- gNMI: Crosswork collects the openconfig-interfaces data from the devices.

- Both: Depending on the device's capability, select SNMP and gNMI protocol to discover the devices.

If you choose **Both** as the method, you must select the appropriate SNMP and gNMI device tags. If you choose **SNMP** or **gNMI** method, the device tags become optional.

Step 4 From the **Select {SNMP or gNMI} Device Tag** drop-down, select unique tags for SNMP and gNMI protocols.

The precreated tags associated to the device are listed. If you select **No Tag Selected** option, Crosswork starts the data collection for devices with system SNMP or gNMI tags.

Step 5 In the **Interface Collection Interval** field, specify the duration between the data collection requests. The default duration is 5 minutes.

Step 6 Click **Save**.

Set the Pre-Login Disclaimer

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

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

Step 2 Under **Notifications**, click the **Pre-Login Disclaimer** option.

Step 3 To enable the disclaimer and customize the banner:

a) Check the **Enabled** checkbox.

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

c) Optional: While editing the disclaimer, you can

Click **Preview** to see how your changes will look when displayed before the Crosswork login prompt.

Click **Discard Changes** to revert to the last saved version of the banner.

Click **Reset** to revert to the original, default version of the banner.

d) 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** > **System Settings** > **Pre-Login Disclaimer**, then uncheck the **Enabled** checkbox.

Manage File Server Settings

Cisco Crosswork provides secure file transfer services (FTP and SFTP) for Crosswork applications that need them. They are disabled by default.

Note This feature is currently only supported for the EPNM application. For more information about the enabling scenarios, please refer to the EPNM user documentation.

Step 1 To enable FTP server:
a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **File Servers**
b) Under FTP, select on the **Enable** radio button.
c) Click **Save** to save your settings.

Step 2 To enable SFTP server:
a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **File Servers**
b) Drag the **Enable Server Upload** slider to **On** position.

Caution SFTP supports upload option that allows write access to the Cisco Crosswork storage from the outside. You are recommended to use caution while enabling the upload, and it should be disabled as soon as it is no longer needed.

c) Click **Save** to save your settings.