



# Manage System Access and Security

This section contains the following topics:

- [Manage Certificates, on page 1](#)
- [Manage Licenses, on page 11](#)
- [Manage Users, on page 16](#)
- [Set Up User Authentication \(TACACS+ and LDAP\), on page 31](#)
- [Security Hardening Overview, on page 35](#)
- [Configure System Settings, on page 38](#)

## 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 36](#) and [HTTPS, on page 35](#).

### 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.



Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork (CW) Internal TLS	CW- Internal-Communication	<ul style="list-style-type: none"> <li>Generated and provided by Crosswork.</li> <li>This trust-chain is available in the UI (including the server and client leaf certificates) and are created by Crosswork during initialization. They are used for interprocess communications between Crosswork and CDG as well as communication between internal Crosswork components.</li> <li>Allows mutual and server authentication.</li> </ul>	CW	<ul style="list-style-type: none"> <li>CDG</li> <li>CW</li> </ul>	Download	5 years	—
CW Web Server	CW-Web-Certificate Server Authentication	<ul style="list-style-type: none"> <li>Generated and provided by Crosswork.</li> <li>Provides communication between the user browser and Crosswork.</li> <li>Allows server authentication.</li> </ul>	CW Web Server	User Browser or API Client	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul>	5 years	30 day - 5 years

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
ZTP SUDI	CW-ZTP-Device-SUDI	<ul style="list-style-type: none"> <li>• A public Cisco certificate that is provided as part of Crosswork.</li> <li>• Provides ZTP protocol communication channel between the ZTP application and device.</li> <li>• Allows server authentication.</li> </ul>	CW ZTP	Device	<ul style="list-style-type: none"> <li>• Upload</li> <li>• Download</li> </ul>	100 days	30 day - User defined
Secure ZTP Provisioning	CW-ZTP-Owner	<ul style="list-style-type: none"> <li>• Generated and provided by Crosswork.</li> <li>• Forwarded by ZTP to devices and used for second layer of encryption.</li> </ul>	CW ZTP	Device	<ul style="list-style-type: none"> <li>• Upload</li> <li>• Download</li> </ul>	5	30 day - User defined
Device Syslog	CW-Device-Syslog	<ul style="list-style-type: none"> <li>• Generated and provided by Crosswork.</li> <li>• Provides Syslog telemetry communications between devices and CDG.</li> <li>• Allows server authentication.</li> </ul>	CDG	Device	Download	5 years	—
Device gNMI Communication	—	Provides GNMI telemetry communications between devices and CDG.	CDG	Device	<ul style="list-style-type: none"> <li>• Upload</li> <li>• Download</li> </ul>	Not Applicable	30 day - User defined

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Server Syslog	Not Applicable	<ul style="list-style-type: none"> <li>Allows syslog events and logs from Crosswork to an external Syslog server.</li> <li>Allows server authentication.</li> </ul>	External Syslog Server	Crosswork	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul> <p><b>Note</b></p>	— You can upload multiple certificates associated with different servers.	30 - User defined
External Destination	—	Exports telemetry data from CDG to external destinations (Kafka or GRPC).	External Destinations (Kafka or GRPC)	CDG	<ul style="list-style-type: none"> <li>Upload</li> <li>Download</li> </ul> <p><b>Note</b></p>	— You can upload multiple certificates associated with different destinations.	30 - User defined

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 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 CDG and external destinations like Kafka servers. To enable mutual authentication, the user uploads a **CA Certificate Trustchain** that will be common to both CDG 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 will internally create a client certificate using this intermediate key for the CDGs that will connect to the external destination. The destination (for example: Kafka) server certificate trust needs to be derived from the same root CA certificate.
- **Syslog Server 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 38](#).

- **Devices gNMI communication:** The user uploads a bundle of trust chains used by CDG 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 33](#)) and associate the certificate.



---


**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 ([Zero Touch Provisioning Concepts](#)) and web certificates (instead of using the default certificates provided within Cisco Crosswork), use the Edit function (see [Edit Certificates](#)).

#### 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](#).

- 
- 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 [Manage Certificates, on page 1](#).
- 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") will indicate that the certificate is about to be applied. The Certificate Management UI then logs out automatically and applies the certificate to the Web Gateway. The new certificate can be checked by clicking the lock <Not Secure>/<secure> icon next to the `https://<crosswork_ip>:30603`.

## Edit Certificates


You can edit a certificate to add or remove connection destinations, upload, and replace expired or misconfigured certificates. User provided certificates and ZTP 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.



**Note** For information about ZTP certificates, see [Assemble and Load ZTP Assets](#).

**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

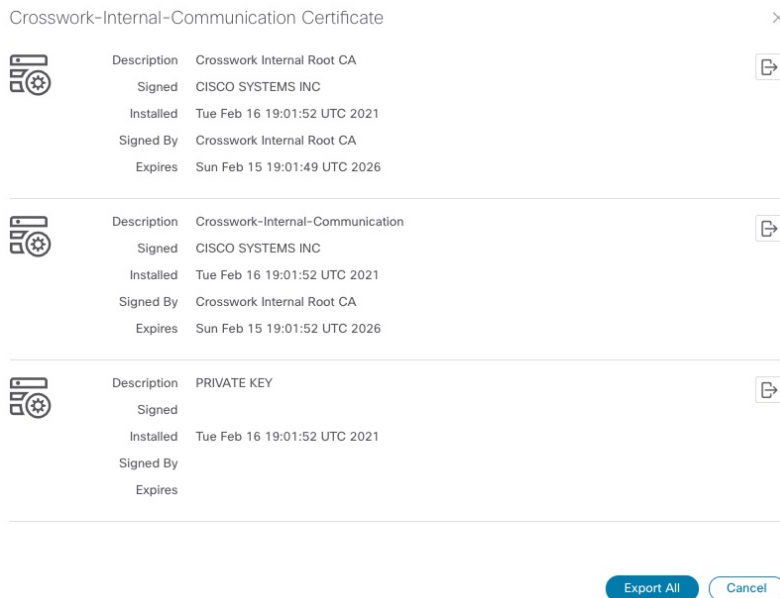
To export certificates, do the following:



**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

Certificates are valid for 1 year before they expire. The below procedure needs to be executed sequentially on each node (hybrid and worker) in the cluster. After renewing the certificates in one node, ensure that the pods are healthy before proceeding to the next node.



**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:

**Step 1** In the node, run command to move to root user.

```
sudo -i
```

You will be prompted to enter your password. Enter the `cw-admin` user password.

**Step 2** Verify if the certificate date has expired.

```
kubeadm alpha certs check-expiration
```

The following image is a sample of the output:

**Figure 4: Certificate expiration sample output**

```
root@10-90-147-67-hybrid:~# kubeadm alpha certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -oyaml'
```

CERTIFICATE	EXPIRES	RESIDUAL TIME	CERTIFICATE AUTHORITY	EXTERNALLY MANAGED
admin.conf	May 16, 2023 21:31 UTC	343d		no
apiserver	May 16, 2023 21:31 UTC	343d	ca	no
apiserver-etcd-client	May 16, 2023 21:31 UTC	343d	etcd-ca	no
apiserver-kubelet-client	May 16, 2023 21:31 UTC	343d	ca	no
controller-manager.conf	May 16, 2023 21:31 UTC	343d		no
etcd-healthcheck-client	May 16, 2023 21:31 UTC	343d	etcd-ca	no
etcd-peer	May 16, 2023 21:31 UTC	343d	etcd-ca	no
etcd-server	May 16, 2023 21:31 UTC	343d	etcd-ca	no
front-proxy-client	May 16, 2023 21:31 UTC	343d	front-proxy-ca	no
scheduler.conf	May 16, 2023 21:31 UTC	343d		no

CERTIFICATE AUTHORITY	EXPIRES	RESIDUAL TIME	EXTERNALLY MANAGED
ca	May 13, 2032 21:31 UTC	9y	no
etcd-ca	May 13, 2032 21:31 UTC	9y	no
front-proxy-ca	May 13, 2032 21:31 UTC	9y	no

```
root@10-90-147-67-hybrid:~#
```

**Step 3** Make a backup of the certificates and conf files.

```
mkdir $HOME/Old-K8-Certs
mkdir $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/pki/*.* $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/*.conf $HOME/Old-K8-Certs
~#
```

**Step 4** Run command to renew the certificate.

```
kubeadm alpha certs renew all
```

**Step 5** Repeat step 2 to verify the creation of new certificates.

**Step 6** Run command to restart the kubelet.

```
systemctl stop kubelet
```

**Note** The restart occurs on all the nodes and the refreshed certificates do not take effect until the `kubelet` and `kube-apiserver` are restarted. It is recommended to stop any operations from the applications from running when the restart occurs.

After stopping `kubelet`, find the following processes (using `ps -eaf | grep <process name>`):

```
kube-apiserver
controller-manager
kube-scheduler
```

Kill them (using `kill -9 <pid>`). After killing the above processes, perform the following to restart the `kubelet`:

```
systemctl daemon-reload
systemctl start kubelet
```

The node will first move to `degraded` state, and then to `down` state.

**Note** The syslog may continue to show traffic even after the node has moved to `down` state.

```
10-90-147-67-hybrid kernel: [1897091.695393] ll header: 00000000: ff ff ff ff ff ff fa 51
56 a2 9c 7c 08 0
10-90-147-67-hybrid kernel: [1897091.695414] IPv4: martian source 169.254.1.1 from
10.244.215.17, on dev calieff0340c649
10-90-147-67-hybrid kernel: [1897091.695416] ll header: 00000000: ff ff ff ff ff ff 72 e8
75 10 bb 64 08 06
```

**Important** Check the status of the `kubelet` using the command `systemctl status kubelet`.

- If the status shows `running`, repeat steps 1 to 6 on the other two nodes. Check the status by executing steps 7 and 8.
- If the status is not `running`, execute step 9 on all three nodes. Repeat steps 1 to 6 and step 9 on the other two nodes. Check the status by executing steps 7 and 8.

**Step 7** Verify if all the pods are healthy and running.

```
kubectl get nodes
kubectl get pods -A -o wide
```

It also verifies the running pods on the hybrid node that you have restarted.

**Step 8** Verify if the certificate has been renewed.

**Step 9** If the issue is still seen, change the conf file.

```
sudo kubeadm alpha kubeconfig user --org system:nodes --client-name system:node:$(hostname) >
/etc/kubernetes/kubelet.conf
```

Check the status of the `kubelet` using the command `systemctl status kubelet`.

Repeat the above steps for each node in your cluster.

---

## 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](https://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](https://cisco.com/go/licensingguide).

From the main menu, select **Administration > Smart Licensing Registration** to display the **Smart Software Licensing** window. Using this window, you can register your Cisco Crosswork application, edit the transport settings, renew the license, and de-register your application.

### Prerequisites for Smart Licensing Registration

You should have:

- A Cisco Smart Account.
- Purchased licenses for the Cisco Crosswork application.

## Configure Transport Settings

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

- **Direct:** The application directly connects with Cisco Smart Software Manager (CSSM).
- **Transport Gateway:** The application communicates via a Transport Gateway or CSSM on-prem, which replicates the cloud-based user experience but keeps all communication on premises.



---

**Note** 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.



---

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

---

---

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

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

Transport Settings ×

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

Direct - product communicates directly with Cisco's licensing servers  
URL :

Transport Gateway - proxy data via Transport Gateway or 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.

**Step 3** Click **Save**.

## Register Cisco Crosswork Application

To enable licensed features, the Cisco Crosswork application must be registered to CSSM using a registration ID token. 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.

**Step 1** From the main menu, select **Administration > Smart Licensing Registration** to display the **Smart Software Licensing** window. The registration status

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

Figure 5: Smart Software Licensing Unregistered Example

Last Refresh: Sun, Feb 14, 2021, 09:41:35 AM PST

Select Crosswork Product: Crosswork Platform Services

**i** You are currently running in Evaluation Mode. To register your Crosswork application with Cisco Smart Licensing:

- Ensure this product has access to the Internet or On Prem Smart Software Manager installed on your network. This might require you to [edit the Smart Call Home Transport Settings](#).
- Log in to your Smart Account in [Smart Software Manager](#) on your On Prem Smart Software Manager.
- Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

[Register](#) [Learn more about Smart Software Licensing](#)

Smart Software Licensing Status

Registration Status **Un Registered**

License Authorization Status **Evaluation Mode**(87 days remaining)

Product Instance Name UDI\_PID:CW\_INFRA;UDI\_SN:f150b4bf-3f2f-4c98-842f-9097acf06498;

Export-Controlled Functionality Not Allowed

Transport Settings [Direct View](#) / [Edit](#)

Smart Licensing Usage

License (Version)	Description	Count	Status
CW_EXTERNAL_COLLECT(1.0)			<b>Init</b>

**Step 2** In the **Smart Software Licensing** window, click **Register**.

The **Smart Software Licensing Product Registration** dialog box is displayed.

Smart Software Licensing Product Registration ×

To register the product for Smart Software Licensing:

- Ensure you have connectivity to the URL specified in your Smart Call Home 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.

**i** After successful 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

[Register](#) [Cancel](#)

**Step 3** 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](https://www.cisco.com/c/en_in/products/software/smart-accounts/software-licensing.html).

**Step 4** (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** checkbox.

**Note** After a backup restore or disaster restore operation, you must manually re-register the Cisco Crosswork VM to CSSM. This is applicable in case of a Cisco Crosswork VM that has been already registered while taking the backup which is used in the restore operations.

**Step 5** 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 (for example, "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.
  - 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, the page may need to be refreshed manually to see the updated status.

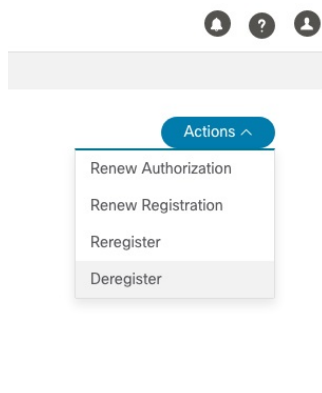
## Manually Perform Licensing Actions

The renewal of registration and authorization are automatically enabled for Cisco Crosswork, 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.



- Note** In the case of the Cisco Optimization Engine smart license, the node count is tracked during the initial onboarding of devices and during the registration and entitlement of the license. Any further changes to node count are synced with the Smart Licensing server after every 24 hours GMT. If you prefer not to wait, you can reregister the application license to update the node count immediately.

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



- Actions > Renew Authorization:** To renew the authorization manually if the automatic renewal service fails at the end of 30 days.
- 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 16](#).

**Step 2** The selected action is executed successfully.

## License Authorization Statuses

Based on the registration status of your Cisco Crosswork 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.

## 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 19](#)).

- 
- 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:
- Click  and enter the required user details.
  - Click **Save**.
- Step 3** To edit a user:
- Click the checkbox next to the User and click .
  - After making changes, click **Save**.
- Step 4** To delete a user:
- Click the checkbox next to the User and click .
  - In the **Confirm Deletion** window, click **Delete**.
- Step 5** 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](#).
- 

## 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 its 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 Cisco Crosswork data to help their work as system architects or planners.

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

**Table 2: 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

Local users with administrator privileges can create new users as needed (see [Manage Users, on page 16](#)).

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

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

Follow the steps below to create a new user role.

- 
- 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 **admin** table 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** Define the user role's privilege settings:
- Check the check box for every API that users with this role can access. The APIs are grouped logically based their corresponding application.
  - 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 20](#)).


---

## 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 16](#)). Later, you can edit the roles themselves to give users the privileges you want (see [Edit User Roles, on page 20](#)).

---

- 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** In the **Roles** table, click on an existing role to select it. The **Admin** table 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.
- 

## Role Permission Categories

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

The following table is an overview of the various role permission categories in Cisco Crosswork:

**Table 3: Role Permission Categories**

Category	Role Permission	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.

Category	Role Permission	Description
Alarms	Alarms APIs	<p>Allows you to manage alarms.</p> <p>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.</p> <p>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.</p> <p>The DELETE permission allows you to delete REST destinations, Syslog destinations and trap destinations.</p>
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	<p>Allows you to use external storage for longer retention, and to manage external datastore used by Service Assurance for archiving service metrics data.</p> <p>The READ permission allows you to get storage provider information, check storage stats, etc.</p> <p>The WRITE permission allows you to sync the local CW datastore with the external storage and run diagnostics.</p> <p>The DELETE permission allows you to delete an external storage provider.</p>

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

Category	Role Permission	Description
Change Automation	Administration APIs	<p>Provides administrative control to manage job scheduling, manage override credentials, and configuration of user roles for playbook executions.</p> <p>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.</p>
	Application APIs	<p>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.)</p> <p>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.</p>
	Playbook APIs	<p>Allows you to manage playbooks.</p> <p>The READ permission allows you to retrieve playbooks, params, and policy specs.</p> <p>The WRITE permission allows you to import/export, and generate playbooks.</p> <p>The DELETE permission enables you to delete playbooks.</p>
	Play APIs	<p>Allows you to manage plays.</p> <p>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.</p>
Collection Infra	Collection APIs	<p>Permissions for APIs to manage collection jobs.</p> <p>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.</p> <p>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.</p>
	Data Gateway Manager APIs	<p>Permissions to perform CRUD operations on Destinations, Data Gateways, Custom Packages, etc.</p> <p>The READ permission allows you to view the data, while the WRITE permission allows you to add/update/delete the data.</p>



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

Category	Role Permission	Description
Data Gateway Troubleshooting	Data Gateway Reboot API	Reboots a Crosswork Data Gateway (CDG). The WRITE permission allows you to reboot the CDG.
	Data Gateway Showtech API	Generates and downloads showtech logs for a CDG 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 Health 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	Role Permission	Description
Inventory	Inventory APIs	<p>Allows you to manage inventory.</p> <p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>• Fetch the list of nodes, the node credentials, and the count of nodes in the database.</li> <li>• Retrieve the list of HA pools, DG enrollments, virtual data gateways, and inventory job information.</li> <li>• Retrieve the list of policies, providers, and tags.</li> </ul> <p>The WRITE permission allows you to</p> <ul style="list-style-type: none"> <li>• Update device mapping to virtual data gateway pool.</li> <li>• Lock/unlock the requested nodes.</li> <li>• Remove tag associations from nodes. Does not support partial un-assignment.</li> <li>• Update input data to a set of devices.</li> <li>• Set API endpoint for provider onboarding.</li> </ul> <p>The DELETE permission allows you to</p> <ul style="list-style-type: none"> <li>• Perform bulk deletion of credential profiles and nodes.</li> <li>• Upload CSV for delete operations.</li> <li>• Delete HA pools, Data Gateway enrollments, and virtual data gateways.</li> <li>• Delete policies, providers, and tags.</li> </ul>

Category	Role Permission	Description
Platform	Platform APIs	<p>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.</p> <p>The WRITE permission allows you to</p> <ul style="list-style-type: none"> <li>• Enable/disable the xFTP server</li> <li>• Manage cluster (set the login banner, restart a microservice, etc.)</li> <li>• Rebalance cluster resources</li> <li>• Manage nodes (export cluster inventory, add VM, apply VM configuration, remove VM from a cluster, etc.)</li> <li>• Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, etc.)</li> <li>• Perform normal/data-only backup and restore operations.</li> <li>• Manage applications (activate, deactivate, uninstall, add package, etc.)</li> </ul> <p>The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.</p>
	Distributed Cache APIs	The READ permission allows you to fetch cache statistics for troubleshooting.
	Grouping APIs	<p>Grouping management and Topology groups selection tree.</p> <p>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.</p>
	View APIs	<p><i>Views Management in Topology.</i></p> <p><i>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.</i></p>
Topology	Geo APIs	<p>Provides geo service for offline maps.</p> <p>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.</p>
	Topology APIs	<p>Allows you to manage topology pages, settings, or any other pages that uses the Topology visualization framework.</p> <p>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.</p>

Category	Role Permission	Description
Proxy	Crosswork Proxy APIs	Permissions to manages CNC 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.
Service Health	Archiver APIs	The READ permission allows you to <ul style="list-style-type: none"> <li>• Check if Historical Data exists for a given service.</li> <li>• Get the Historical Timeline series for a given service.</li> <li>• Get a Service Graph for a selected timestamp of the service.</li> <li>• Get Service-Metric data</li> </ul> <p>The WRITE/DELETE permissions are not applicable for these APIs.</p>
	Assurance Graph Manager APIs	The READ permission allows you to <ul style="list-style-type: none"> <li>• Fetch details of a service.</li> <li>• Get the impacted list of services.</li> <li>• Retrieve the list of matching sub-services (transport or device only).</li> </ul> <p>The WRITE/DELETE permissions are not applicable for these APIs.</p>
	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	Role Permission	Description
Zero Touch Provisioning	CW Config Service APIs	<p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>List all day-0 configuration files stored in the ZTP config repository.</li> <li>Fetch count of day-0 configuration files stored in the ZTP config repository.</li> <li>Download the day-0 configuration file from the ZTP config repository.</li> <li>List all device family/device versions and device platforms based on information associated with day-0 config files stored in the CW ZTP repository.</li> </ul> <p>The WRITE permission allows you to</p> <ul style="list-style-type: none"> <li>Upload the day-0 config file or script to the ZTP config repository.</li> <li>List/update relevant metadata associated with specific day-0 config files stored in the ZTP config repository</li> </ul> <p>The DELETE permission allows you to delete config files and scripts uploaded in the ZTP config repository.</p>
	CW Image Service APIs	<p>The READ permission allows you to</p> <ul style="list-style-type: none"> <li>List all device image files stored in the ZTP image repository.</li> <li>List all device platform/family names associated with image files stored in the CW ZTP repository.</li> <li>Download the device image file by ID.</li> </ul> <p>The WRITE permission allows you to update relevant metadata associated with specific image files stored in the ZTP image repository.</p> <p>The DELETE permission allows you to delete image files uploaded in the ZTP image repository</p>
	CW ZTP Service APIs	<p>Allows you to manage the ZTP devices and profiles - add/update/delete into Crosswork.</p> <p>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.</p> <p>The WRITE permission allows you to add ZTP devices, serial numbers/OVs, profiles and add/update the ZTP device's attributes.</p> <p>The DELETE permission allows you to delete ZTP devices, profiles, serial numbers/ownership vouchers.</p>

Category	Role Permission	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




### Note


- 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 cannot view the **Active Sessions** window.

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

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

**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.

**Note** 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.

**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](#).

## Set Up User Authentication (TACACS+ and LDAP)

In addition to supporting local users, Cisco Crosswork supports TACACS+ and LDAP users through integration with the TACACS+ and LDAP servers. The integration process has the following steps:

- Configure the TACACS+ and LDAP server.
- Create the roles that are referenced by the TACACS+ and LDAP users.
- Configure AAA settings.

**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 19](#).
- 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.

## Manage TACACS+ Servers

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

**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 TACACS+ changes and submit them in a single session.

### Before you begin

You must create the required user role in TACACS+ server, before configuring the same in Cisco Crosswork. You can integrate Crosswork with an application such as Cisco ISE (Identity Service Engine) to authenticate using the TACACS+ protocols. To avail this service, you must configure Crosswork as a client in Cisco ISE. For more information, see the [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 settings, and delete a new TACACS+ server.

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

- Click the  icon.
- Enter the required TACACS+ server information.


**Note**

- You can specify a unique priority value to assign precedence in the authentication request.
- For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this page must match with the shared secret value configured on the TACACS+ server.




- c) Select the authentication type.
- 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).
- d) After you enter all the relevant details, click **Add**.
- Note** The **Policy ID** field corresponds to the user role that you created in the TACACS+ server. If you try to login to Cisco Crosswork 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.
- e) 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.

## 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 6](#).



**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 LDAP server changes and submit them in a single session.

**Step 1** From the main menu, select **Administration > AAA > Servers > LDAP** tab. Using this window, you can add, edit settings, 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.


**Note**

- Like TACACS+ server, you can specify a unique priority value to assign precedence in the authentication request.
- To add a secure LDAP server, enable the **Secure Connection** toggle button and select the relevant secure LDAP certificate from the **Certificate** drop-down list.
- The **Policy ID** field corresponds to the user role that you created in the LDAP server. If you try to login to Cisco Crosswork 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.


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:**

- Click the checkbox next to the LDAP server and click .
- After making changes, click **Update**.

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

- Click the checkbox next to the LDAP server and click .
- 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.

**Step 5** 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 Cisco Crosswork, and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

---

## 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 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 send system events, audit events, and internal collection jobs to the Syslog and Trap servers.
- Define and filter which kind of events should be forwarded as a syslog, per consumer.
- Define the rate of 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.

---


### Before you begin

Ensure that you have uploaded the Syslog TLS server certificate. For more information, see [Add a New Certificate, on page 6](#).

- 
- Step 1** From the main menu, choose **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 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**.
- 

## Configure a Trap Server

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**.
- 

## Enable Layered Service Architecture (LSA)

This procedure is applicable only when you have opted for Cisco NSO LSA deployment to add arbitrarily many device nodes for improved memory and provisioning throughput.

**Step 1** From the main menu, select **Administration > Settings > System Settings > Layered Service Architecture**.

The screenshot shows the 'Layered Service Architecture' configuration page. The breadcrumb trail is 'Administration / Settings'. The page has two tabs: 'System Settings' (selected) and 'User Settings'. On the left, a sidebar lists various settings categories: Servers, Maintenance Mode, Providers, Notifications, and Topology. Under 'Providers', 'Layered Service Architecture' is selected. The main content area is titled 'Layered Service Architecture' and contains the following options:

- Enable/disable layered service architecture for NSO providers.**
  - Enable
  - Disable
- Spreading Method**
  - Choose the method to be used to spread devices across multiple NSO instances.
  - Round Robin ?
  - Capacity ?
  - User Defined ?

At the bottom of the configuration area, there are three buttons: 'Save', 'Discard Changes', and 'Reset to Default'.

**Step 2** Select **Enable**.

**Step 3** Select the method to spread the devices across multiple NSO instances:

- **Round Robin** - Even distribution of devices to RFS nodes in a cyclical manner (for example, Device 1 to RFS1, Device 2 to RFS2, and so on).
- **Capacity** - The number of devices are assigned to each RFS instance based on its total capacity.
- **User Defined** - Devices are assigned to the NSO providers specified for the device in the device settings. For more information, see [Add Devices through the UI](#).

**Step 4** Click **Save**.

**Note** Once you have saved the settings, you cannot disable it without removing all the NSO providers.

## 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:
- Check the **Enabled** checkbox.
  - Customize the banner **Title**, the **Icon**, and the **Disclaimer Text** as needed.
  - 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.
  - 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:
- From the main menu, choose **Administration > Settings > System Settings > File Servers**
  - Under FTP, select on the **Enable** radio button.
  - Click **Save** to save your settings.
- Step 2** To enable SFTP server:
- From the main menu, choose **Administration > Settings > System Settings > File Servers**
  - 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.
- Click **Save** to save your settings.
-

