Manage Certificates

This chapter explains how to manage digital certificates by adding, editing, exporting, renewing, and updating them.

Certificates

A certificate is an electronic document that:

- identifies an individual, a server, a company, or entity
- associates the entity with a unique public key, and
- is digitally signed by an issuer (Certificate Authority or self-signed) to enable secure communication.

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.

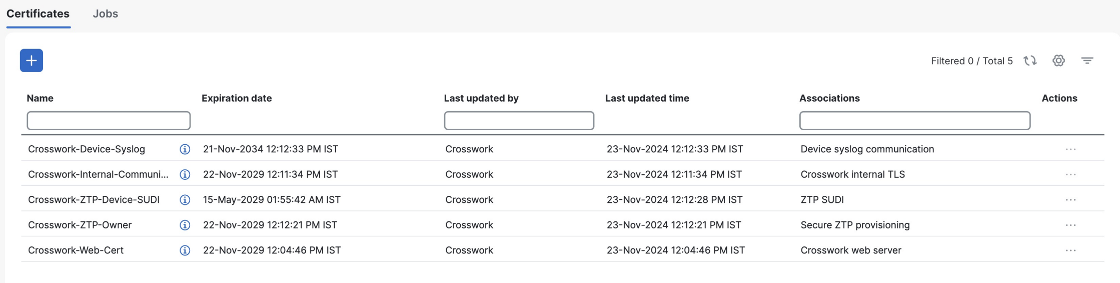
In a TLS exchange, a hierarchy of certificates is used to verify the validity of the certificate's issuer. This hierarchy is called a trust-chain and consists of 3 types of entities: a root CA certificate (self-signed), possibly multiple levels of intermediate CA certificates, and a server (or client) 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. The root certificate's private key signs and issues the next certificate in the chain. Subsequently, the private key for each certificate in the trust chain signs and issues the following certificate, continuing until the end entity certificate is signed. The end-entity certificate is the last certificate in the chain. It is used as a client or server certificate. For more details about these protocols, see *<xref to SSL in security hardening>* and *<xref to HTTPS in security hardening>*.

How are certificates used in Crosswork Network Controller?

Communication between Crosswork Network Controller applications and devices as well as between various Crosswork Network Controller 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 Network Controller uses both generated certificates and certificates uploaded by clients . Uploaded certificates can be purchased from Certificate authorities (CA) or created as self-signed certificates. For example, the Crosswork Network Controller VM-hosted web server and the client browser-based user interface communicate with each other using Crosswork Network Controller generated X.509 certificates exchanged over TLS.

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

Figure 1: Certificate Management Window

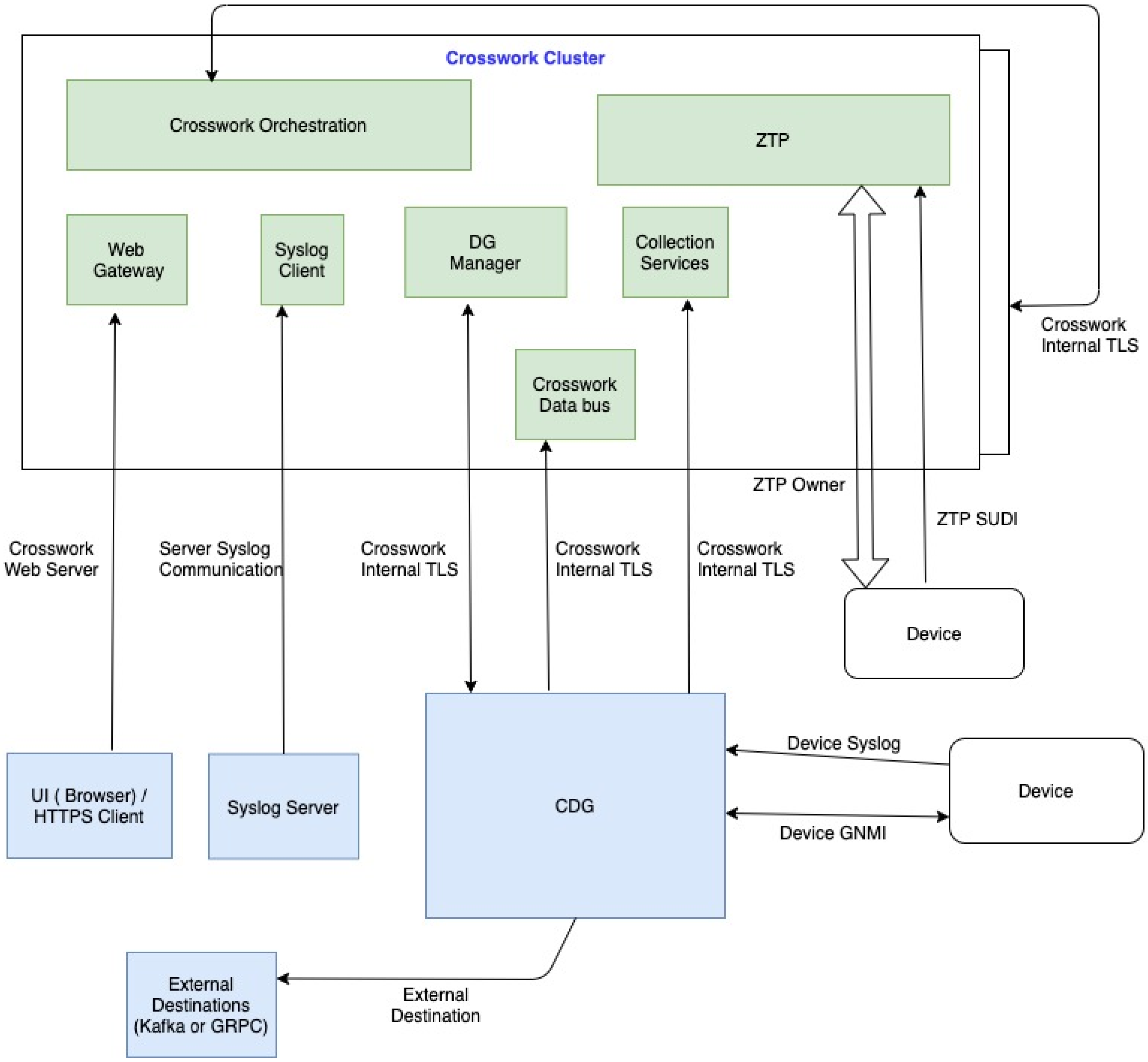


Name	Expiration date	Last updated by	Last updated time	Associations	Actions
Crosswork-Device-Syslog	21-Nov-2034 12:12:33 PM IST	Crosswork	23-Nov-2024 12:12:33 PM IST	Device syslog communication	···
Crosswork-Internal-Communi...	22-Nov-2029 12:11:34 PM IST	Crosswork	23-Nov-2024 12:11:34 PM IST	Crosswork internal TLS	···
Crosswork-ZTP-Device-SUDI	15-May-2029 01:55:42 AM IST	Crosswork	23-Nov-2024 12:12:28 PM IST	ZTP SUDI	···
Crosswork-ZTP-Owner	22-Nov-2029 12:12:21 PM IST	Crosswork	23-Nov-2024 12:12:21 PM IST	Secure ZTP provisioning	···
Crosswork-Web-Cert	22-Nov-2029 12:04:46 PM IST	Crosswork	23-Nov-2024 12:04:46 PM IST	Crosswork web server	···

Usage of certificate types

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

Figure 2: Certificates in Crosswork Network Controller



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

Table 1: Crosswork internal TLS certificate

Role	Crosswork internal TLS
UI Name	Crosswork-Internal-Communication

Description	• Generated and provided by Crosswork Network Controller. • This trust-chain is available in the UI (including the server and client leaf certificates) and is created by Crosswork Network Controller during initialization. They are used for interprocess communications between Crosswork Network Controller and Crosswork Data Gateway and communication between internal Crosswork Network Controller components. • Allows mutual and server authentication.
Server	Crosswork Network Controller
Client	Crosswork Data Gateway Crosswork Network Controller
Allowed operations	Download
Default expiry	5 years
Allowed expiry	—

Table 2: Device syslog communication certificate

Role	Device syslog communication
UI Name	Crosswork-Device-Syslog
Description	• Generated and provided by Crosswork Network Controller. • Provides Syslog telemetry communications between devices and Crosswork Data Gateway. • Allows server authentication.
Server	Crosswork Data Gateway
Client	Device
Allowed operations	Download
Default expiry	5 years
Allowed expiry	—

Table 3: ZTP SUDI certificate

Role	ZTP SUDI
UI Name	Crosswork-ZTP-Device-SUDI

Description	• A public Cisco certificate that is provided as part of Crosswork Network Controller. • Provides ZTP protocol communication channel between the ZTP application and device. • Allows server authentication.
Server	Crosswork ZTP
Client	Device
Allowed operations	• Upload • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 4: Secure ZTP provisioning certificate

Role	Secure ZTP provisioning
UI Name	Crosswork-ZTP-Owner
Description	• Generated and provided by Crosswork Network Controller. • Forwarded by ZTP to devices and used for second layer of encryption.
Server	Crosswork ZTP
Client	Device
Allowed operations	• Upload • Download
Default expiry	5 years
Allowed expiry	31 days to 30 years. The validity period is user-defined.

Table 5: Crosswork web server certificate

Role	Crosswork web server
UI Name	Crosswork-Web-Cert

Description	• Generated and provided by Crosswork Network Controller. • Provides communication between the user browser and Crosswork Network Controller. • Allows server authentication.
Server	Crosswork Web Server
Client	User browser or API client
Allowed operations	• Upload • Download
Default expiry	5 years
Allowed expiry	Default expiry period is 5 years. Users can override this by uploading their own certificate. The allowed period is 31 days to 10 years.

Table 6: Provider gRPC communication certificate

Role	Provider gRPC communication
UI Name	—
Description	SR-PCE requires gRPC to discover topology and SR-MPLS policies. This certificate enables Transport Layer Security (TLS) and is required when the SR-PCE provider protocol is set to GRPC_SECURE.
Server	Crosswork Network Controller
Client	Clients that want secure connection to the gRPC server (Crosswork Data gateway, Device Group Manager pods, and so on)
Allowed operations	• Upload • Download
Default expiry	—
Allowed expiry	The validity period is user-defined.

Table 7: Device gNMI/gRPC communication certificate

Role	Device gNMI/gRPC communication
UI Name	—
Description	Provides GNMI telemetry communications between devices and Crosswork Data Gateway.
Server	Crosswork Data Gateway

Client	Device
Allowed operations	• Upload • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 8: Server syslog communication certificate

Role	Server syslog communication
UI Name	—
Description	• Allows syslog events and logs from Crosswork Network Controller to an external Syslog server. • Allows server authentication.
Server	External syslog server
Client	Crosswork Network Controller
Allowed operations	• Upload **Note** You can upload multiple certificates associated with different servers. • Download
Default expiry	—
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 9: External destination certificate

Role	External destination
UI Name	—
Description	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a mutual-authentication.
Server	External Destinations (Kafka or gRPC)
Client	Crosswork Data Gateway

Allowed operations	• Upload **Note** You can upload one certificate and associate it with one or more external destinations. To upload multiple certificates, configure and select additional destinations. • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 10: External destination server auth certificate

Role	External destination server auth
UI Name	—
Description	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a server-based authentication.
Server	External Crosswork Data Gateway Destinations (Kafka or gRPC)
Client	Crosswork Data Gateway
Allowed operations	• Upload **Note** You can upload one certificate and associate it with one or more external destinations. To upload multiple certificates, configure and select additional destinations. • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 11: Secure LDAP communication certificate

Role	Secure LDAP communication
UI Name	—
Description	Crosswork Network Controller uses the trust chain of this certificate to authenticate the secure LDAP server.
Server	Secure LDAP server
Client	Crosswork Network Controller

Allowed operations	• Upload **Note** You can upload multiple certificates associated with different servers. • Download
Default expiry	—
Allowed expiry	31 days to 30 years. The validity period is user-defined.

Table 12: Accedian provider mutual auth certificate

Role	Accedian provider mutual auth
UI Name	—
Description	Required to add provider connectivity assurance as a provider
Server	Provider
Client	Crosswork Network Controller
Allowed operations	• Upload • Download
Default expiry	—
Allowed expiry	31 days to 30 years. The validity period is user-defined.

There are two category roles in Crosswork Network Controller:

- 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

This section explains the steps to add a new certificate. You can add certificates for these 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, you upload 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 optional intermediate CA certificates. The last intermediate certificate in the chain and its corresponding private key are uploaded separately in the UI using **Intermediate key** , **Intermediate certificate** , and optionally **Passphrase** (if one was used for generating the intermediate key). Crosswork Network Controller internally creates a client certificate using this intermediate key for Crosswork Data Gateways that connect to the external destination. The destination server certificate trust, such as Kafka, must 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**: You upload the trust chain of the Syslog server certificate. This trust chain is used by Crosswork Network Controller to authenticate the Syslog server. After this trust chain is uploaded and propagated within Crosswork Network Controller, you 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.
- **Device gNMI/gRPC communication**: You upload 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 Add the gNMI certificate.
- **Secure LDAP communication**: You upload the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork Network Controller, you can add the LDAP server and associate the certificate.
- **External destination server auth**:
    - Upload the root CA certificate to establish secure communication between the Crosswork Data Gateway and external destinations, such as Kafka servers.
    - You can upload certificates to the **External Destination Server Auth** role only when the authentication type is set to **Server-Auth**.
    - You can upload certificates for the Crosswork Data Gateway, applications, or both using the same role by selecting the appropriate data destination type.
    - The **Data source** field in the data destination form indicates whether the destination applies to the Crosswork Data Gateway, applications, or both.
- **Provider gRPC communication**: You upload a well-known CA certificate trust chain bundle for secure communication between Crosswork Network Controller and gRPC server configured on an external SR-PCE provider. Mutual authentication is currently not supported.

Note Crosswork Network Controller 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 Crosswork Network Controller), use the Edit function (see Edit certificates, on page 11).

Before you begin

- Upload all certificates in Privacy Enhanced Mail (PEM) format. Also, note the location of the certificates on the system for easy navigation.
- Uploaded Trust chain files 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.
- Ensure the intermediate keys are either in PKCS1 or PKCS8 format.

- Configure a data destination before you add 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.
- Ensure that the *tyk* service is in a healthy state.

Procedure

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

Step 2 Enter a unique name for the certificate.

Step 3 From the **Certificate Role** drop-down, select the purpose for which the certificate is to be used. For more information, see Usage of certificate types , 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
After you upload the certificate, the Crosswork Cert manager accepts it, validates it, 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.

Related Topics

Usage of certificate types , on page 2
Add or edit a data destination

Edit certificates

Crosswork Network Controller allows you to update web certificates by importing an intermediate Certificate Authority (CA) certificate. You can edit certificates to add or remove connection destinations, and upload or replace expired or misconfigured certificates. This applies to user-provided certificates , ZTP certificates, and web certificates. However, you cannot modify the system certificates provided by Cisco Crosswork. These certificates will not be available for selection.

Crosswork Network Controller also allows you to configure the client authentication for web certificates. Client authentication offers an alternative method for setting up user authentication in Crosswork. It requires both the client and server to present digital certificates to verify their identities. Enabling this feature can provide a more seamless login experience for users.

You can also remove a certificate by following this procedure to replace the certificate or by disabling security (**Enable Secure Communication**) option for any assigned destinations (see Add or edit a data destination). You cannot permanently delete a certificate from the Crosswork system.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- Restart Crosswork server during this process. The restart will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

Step 1 Choose **Administration** > **Certificate Management** to view the **Certificate Management** window.

Step 2 To update a certificate:

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

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

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

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

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

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

b) Check the **Enable** checkbox.

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

The **OCSP** settings are enabled by default, but you can disable them if you prefer. When these settings are enabled, you can check the certificate revocation status using the Online Certificate Status Protocol (OCSP).

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

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

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

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

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

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

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

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

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

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

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

Download certificates

To export certificates, perform these steps:

Procedure

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

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

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

Renew certificates

- Kubernetes certificate renewal, on page 13
- Automatic renewal of internal certificates, on page 15

Kubernetes certificate renewal

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

Note If you renew certificates before they expire, it is recommended to perform this activity during a maintenance window to keep the cluster in an operational state.

To renew a certificate, perform these steps:

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.

Procedure

Step 1 Create a backup of your Crosswork Network Controller.

Step 2 Log in to one of your hybrid nodes.

Step 3 Renew the Kubernetes certificates using the `renew_k8s_cert` command. The required parameters depend on whether the certificates have already expired.

- **Before certificate expiry** : If the certificates have not yet expired, you can renew them by running the following command. You do not need to specify the hybrid or worker node management IP addresses.

  ```
  renew_k8s_cert --user=<ssh-username> --passwdfile=<passfile-path>
  ```

  Example:

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

- **After certificate expiry** : If the Kubernetes certificates have already expired, you must specify the management IP addresses of the hybrid and (if applicable) worker nodes in your cluster.

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

  Replace the parameters as follows:

  - **hybridNodeMgmtIP** : Management IP of each hybrid node (comma-separated).
  - **workerNodeMgmtIP** : Management IP of each worker node (comma-separated, optional if you have no worker nodes).
  - **ssh-username** : The SSH username to use.
  - **passfile-path** : Path to the plain text file containing the SSH login password.

IPv4 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
```

IPv4 example for a 3-node cluster (hybrid nodes only):

```
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
```

IPv4 example for single VM deployment:

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

IPv6 example for a dual-stack cluster:

```
renew_k8s_cert --hybrid=fded:1bc1:fc3e:96d0:192:168:5:451,fded:1bc1:fc3e:96d0:192:168:5:452,
                                fded:1bc1:fc3e:96d0:192:168:5:453
--worker=fded:1bc1:fc3e:96d0:192:168:5:454,fded:1bc1:fc3e:96d0:192:168:5:455
                                --user=cw-admin --passwdfile=/home/cw-admin/password.txt
```

Attention

- The `--worker` parameter is optional if you do not have worker nodes in your cluster.
- Line breaks in the commands above are for display only. Remove all line breaks before executing the command.

Step 4 (Optional) **Recover cluster:** If multiple pods are stuck in `ContainerCreating` or `terminating` state after you renew the Kubernetes certificate, run these commands on any hybrid node.

```
kubectl delete pod -n kube-system -l k8s-app=calico-kube-controllers --grace-period=0 --force
```

Wait for the `calico-kube-controllers` pods to start, and run this command:

```
kubectl delete pod -n kube-system -l k8s-app=calico-node --grace-period=0 --force
```

After all the Calico pods are up and running, all other pods will recover and enter a running state. If any pods remain in a non-running state, wait at least 10 minutes after the Calico pods started, and then run this command:

```
kubectl get po --all-namespaces | awk '{if ($4 != "Running") system ("kubectl -n " $1 " delete pods
 " $2 " --grace-period=0 " " --force ")}'
```

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 two years will face certificate expiry. This expiry disrupts TLS communication and impacts 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 90 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:**

- For a Geo HA deployment, the certificate renewal is triggered in the active AZ cluster. 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. After the renewal job is completed on the active cluster, the job automatically runs in the standby cluster after a delay. The standby cluster then displays job progress and alarm events.

  In a Geo HA setup with auto-arbitration, the certificate is first renewed on the active cluster, then simultaneously renewed on the standby cluster and the arbiter VM.

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

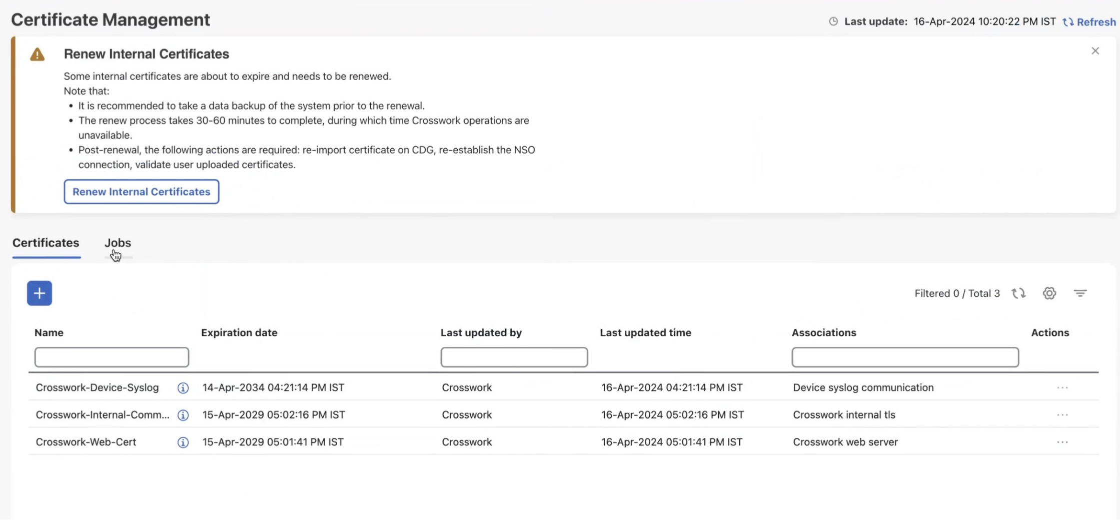
To renew an internal certificate, perform the following:

Procedure

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

Note
The Crosswork dashboard displays alerts about certificate expiry when you log in. The system generates alerts at various stages of the certificate expiry, increasing severity as the expiry date approaches.

Figure 3: Renew Internal Certificate prompt



Certificate Management

Last update: 16-Apr-2024 10:20:22 PM IST Refresh

Renew Internal Certificates

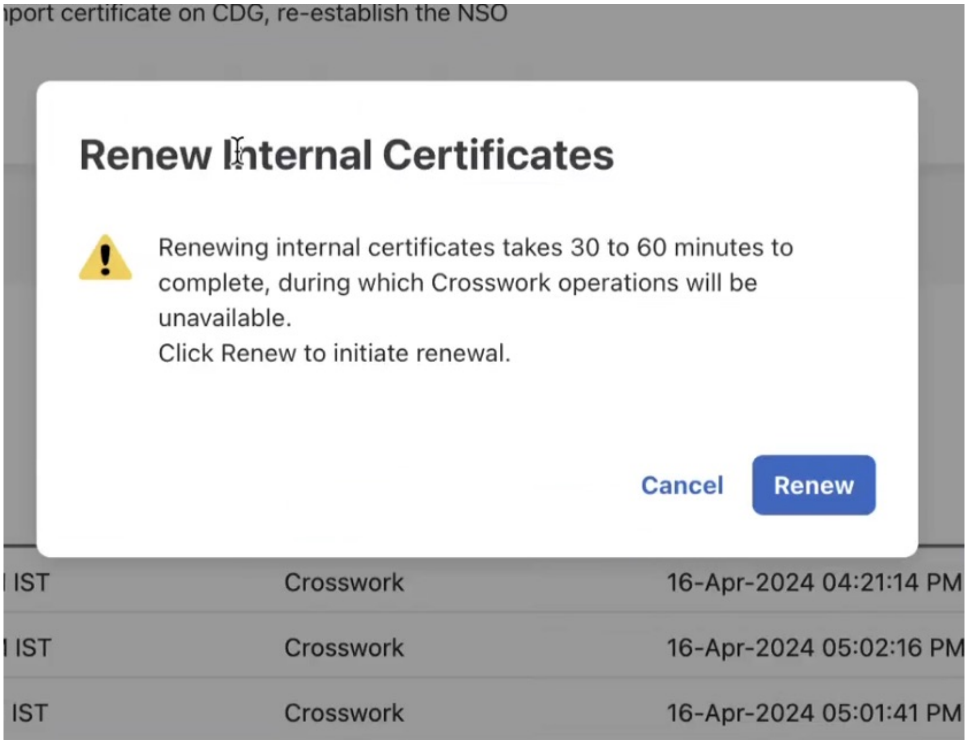
Some internal certificates are about to expire and needs to be renewed.
Note that:

- It is recommended to take a data backup of the system prior to the renewal.
- The renew process takes 30-60 minutes to complete, during which time Crosswork operations are unavailable.
- Post-renewal, the following actions are required: re-import certificate on CDG, re-establish the NSO connection, validate user uploaded certificates.

Name	Expiration date	Last updated by	Last updated time	Associations	Actions
Crosswork-Device-Syslog	14-Apr-2034 04:21:14 PM IST	Crosswork	16-Apr-2024 04:21:14 PM IST	Device syslog communication	···
Crosswork-Internal-Comm...	15-Apr-2029 05:02:16 PM IST	Crosswork	16-Apr-2024 05:02:16 PM IST	Crosswork internal tls	···
Crosswork-Web-Cert	15-Apr-2029 05:01:41 PM IST	Crosswork	16-Apr-2024 05:01:41 PM IST	Crosswork web server	···

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

Figure 4: Renewal Confirmation Prompt



port certificate on CDG, re-establish the NSO

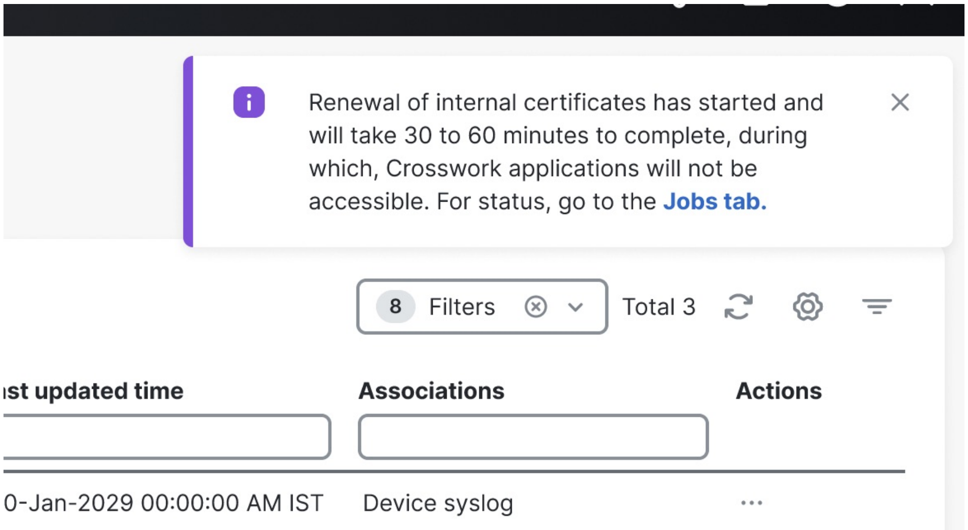
Renew Internal Certificates

Renewing internal certificates takes 30 to 60 minutes to complete, during which Crosswork operations will be unavailable.
Click Renew to initiate renewal.

IST	Crosswork	16-Apr-2024 04:21:14 PM
IST	Crosswork	16-Apr-2024 05:02:16 PM
IST	Crosswork	16-Apr-2024 05:01:41 PM

This action invokes the REST API (/v2/cert/renew) and initiates the certificate expiry check. The **Certificate Management** window displays a notification about the new renewal job.

Figure 5: Renewal Job Notification



Renewal of internal certificates has started and will take 30 to 60 minutes to complete, during which, Crosswork applications will not be accessible. For status, go to the Jobs tab.

ist updated time	Associations	Actions
0-Jan-2029 00:00:00 AM IST	Device syslog	···

You can view progress of the renewal job from the **Jobs** tab. After the job completes, an Info alarm event indicates successful completion of the job. 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 because the API is repeatable.

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 After the renewal job completes, perform these steps to maintain TLS communication between Crosswork and other external components:

a) **Crosswork with Crosswork Data Gateway**: When Crosswork certificates are renewed, it automatically pushes the updated certificates to each Crosswork Data Gateway. During the update process, Crosswork raises alarms for each Data Gateway to indicate these events:

- Certificate update started
- Certificate update completed

Note
The automatic certificate renewal happens as part of the Crosswork Data Gateway day-N enablement process.

b) **In case of Geo HA deployment:**

- The automatic certificate renewal process starts when the certificates are updated. After DG-Manager pushes the updated certificates to the Data Gateway, all the affected Data Gateways automatically restart. The restart causes a brief service interruption.
- If certificate renewal fails, the Crosswork Data Gateway enters error state after the DG-Manager restarts. To recover, manually reimport the certificates on the affected Data Gateway. For more information, see Import a certificate.

c) **Crosswork Data Gateway and Device Syslog**: If device syslog root and intermediate certificates are renewed, 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 jobs.

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

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

e) **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 *<xref to Configure standalone NSO topic>* section.

Update the web certificate using a certificate signing request

Update the web certificate to use one signed by an Enterprise or Commercial CA, without exposing the private key outside Crosswork Network Controller.

Starting with version 7.0.1, Crosswork Network Controller enables updating web certificates via a Certificate Signing Request (CSR) to enhance trust and security.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.

- This process requires the Crosswork server to be restarted, which will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

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

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

The **Certificate Update Method** window appears.

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

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

The **Certificate Signing Request (CSR)** window appears.

b) Click **Create CSR** .

The **Create Certificate Signing Request (CSR)** window appears.

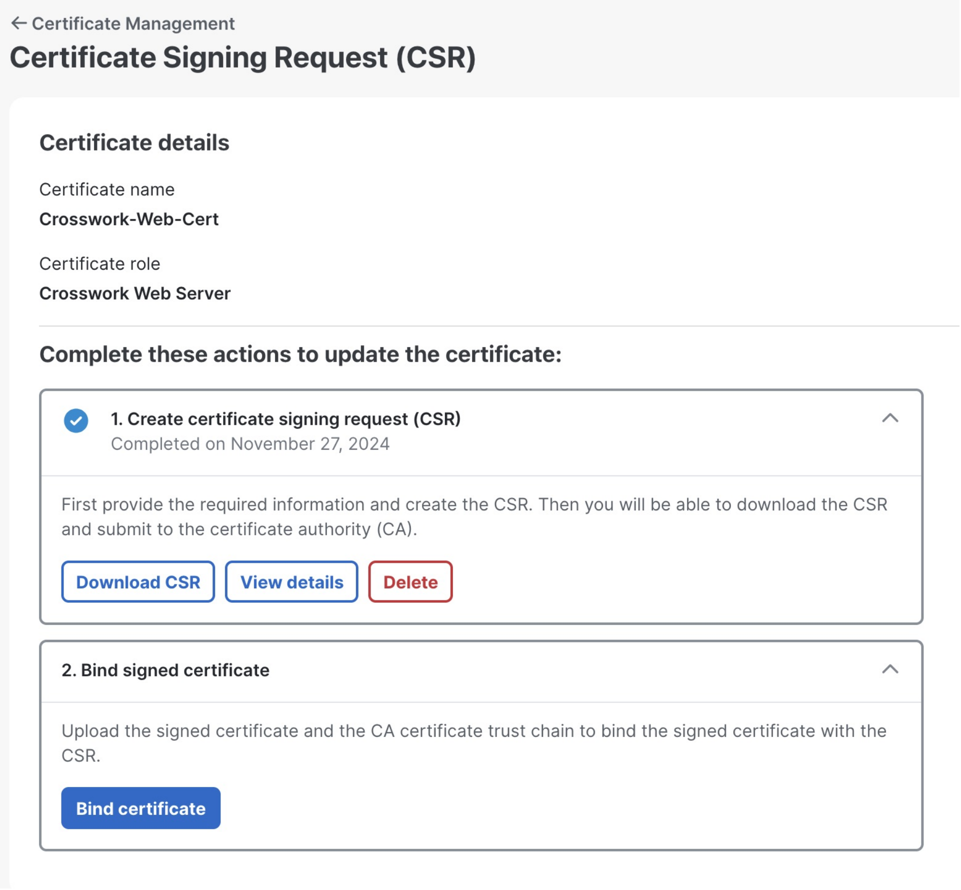
c) Enter the required relevant values for the fields. Click the ⓘ icon next to the field for more information. The mandatory fields are:

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

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

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

Figure 6: Certificate Signing Request (CSR) window



← Certificate Management

Certificate Signing Request (CSR)

Certificate details

Certificate name
Crosswork-Web-Cert

Certificate role
Crosswork Web Server

Complete these actions to update the certificate:

1. Create certificate signing request (CSR)
Completed on November 27, 2024

First provide the required information and create the CSR. Then you will be able to download the CSR and submit to the certificate authority (CA).

2. Bind signed certificate

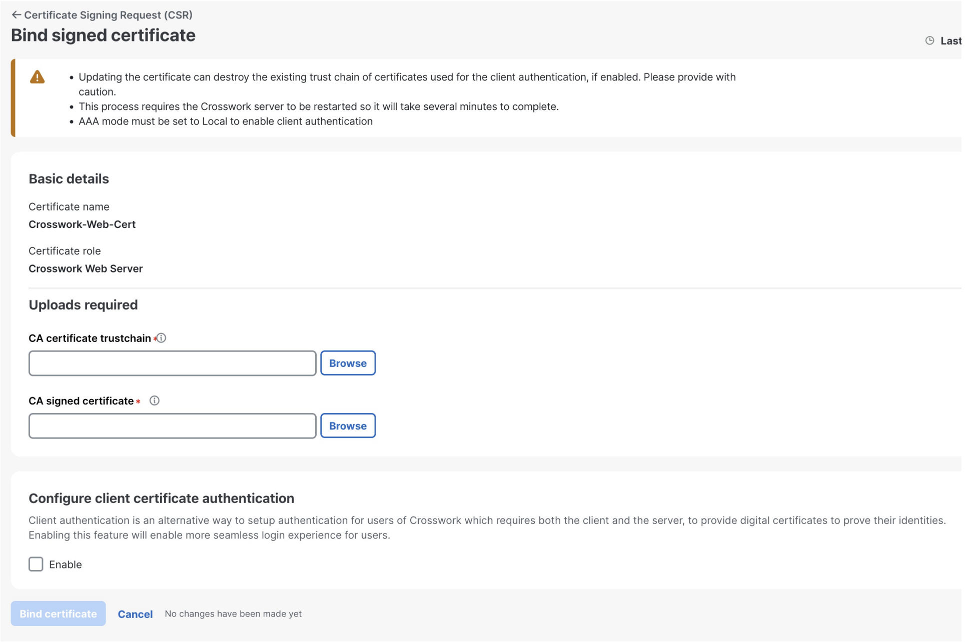
Upload the signed certificate and the CA certificate trust chain to bind the signed certificate with the CSR.

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

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

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

Figure 7: Bind signed certificate



← Certificate Signing Request (CSR)

Bind signed certificate

- Updating the certificate can destroy the existing trust chain of certificates used for the client authentication, if enabled. Please provide with caution.
- This process requires the Crosswork server to be restarted so it will take several minutes to complete.
- AAA mode must be set to Local to enable client authentication

Basic details

Certificate name
Crosswork-Web-Cert

Certificate role
Crosswork Web Server

Uploads required

CA certificate trustchain *

CA signed certificate *

Configure client certificate authentication

Client authentication is an alternative way to setup authentication for users of Crosswork which requires both the client and the server, to provide digital certificates to prove their identities. Enabling this feature will enable more seamless login experience for users.

□ Enable

No changes have been made yet

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

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

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

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

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

The Crosswork Network Controller's web certificate is updated with the CA-signed certificate and trust chain after server restart.