



# Frequency Synchronization

---

Frequency Synchronization is used to distribute precision frequency around a network. Frequency is synchronized accurately using Synchronized Ethernet (SyncE) in devices connected by Ethernet in a network.

This module describes the tasks required to configure frequency synchronization on Cisco IOS XR software.

- [Manage certificates using Certz.proto, on page 2](#)
- [Configure gNSI Certz, on page 4](#)
- [grpc gnsi service certz ssl-profile-id, on page 5](#)
- [show grpc certificate, on page 6](#)

# Manage certificates using Certz.proto

Table 1: Feature History Table

| Feature Name                          | Release Information | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manage certificates using Certz.proto | Release 24.1.1      | <p>Instead of using multiple RPCs, Certz.proto provides a bidirectional Rotate RPC to replace, revoke, or load a certificate. It also provides additional APIs to install Public Key Infrastructure (PKI) entities such as like identity certificates, trust-bundles, and Certificate Revocation Lists (CRLs) for a gRPC Server.</p> <p>This feature introduces the following changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> <li>• <b>grpc gnsi service certz ssl-profile-id</b></li> <li>• <b>show grpc certificate</b></li> </ul> <p>Yang Data Models:</p> <ul style="list-style-type: none"> <li>• Cisco-IOS-XR-man-ems-cfg.yang (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>)</li> </ul> |

## gRPC Network Security Interface (gNSI):



**Note** When both gNSI and gNOI are configured, gNSI takes precedence over gNOI.

## Certz RPCs

The Certz RPCs are specific methods used for executing operations on the certificate that resides in the target device.

In cert.proto, a certificate identifier differentiates between leaf certificates. However, the CA bundle lacks an identifier, meaning a new request to load a bundle could overwrite the existing one. On the other hand, in certz.proto, entities like Certificate, CA bundle, key, CRL, and authentication policy are tied to a unique SSL profile.

Unlike cert.proto, the certz.proto, entities like Certificate, CA bundle, key, CRL, and authentication policy are all tied to a unique SSL profile. This means that each SSL profile has its own set of these entities and doesn't overwrite existing bundle.

The certz.proto differs from the cert.proto in the way that it handles the upload of all entities. While in cert.proto, separate RPCs are used to replace, load, and revoke a certificate, in certz.proto, a single Rotate() RPC is used to upload all entities at once. This includes the certificate, the key, the CA bundle, and the CRL.

In addition to these features, certz.proto also provides support for different cryptographic algorithms, including Rivest-Shamir-Adleman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and ED25519, a public-key signature system.

These functionalities make certz.proto a comprehensive solution for managing SSL profiles, providing a streamlined process for handling cryptographic entities and algorithms.



**Note** If neither cert.proto nor certz.proto is configured, then tls trustpoint data is considered for certificate management.

### SSL Profile

An SSL profile is a named set of SSL settings that determine how end-user systems connect to or from SSL-based applications or interfaces. The settings in an SSL profile include information about the version of SSL/TLS to be used, certificates, keys, and other parameters related to SSL/TLS communication. By using profiles, administrators can manage and apply these settings more easily across multiple applications or connections.

Here are some key-points regarding SSL profile:

- SSL profiles logically groups certificate, private key, Certificate Authority chain of certificates (a.k.a. a CA trust bundle) and a list of Certificate Revocation Lists into a single set that then can be assigned to a gRPC server.
- There's at least one profile present on a target - the one that is used by the gRPC server. Its ID is gNxI but when the ssl\_profile\_id field in the RotateCertificateRequest message isn't set (or set to an empty string) it also refers to this SSL profile by default.
- You can't remove the gRPC SSL profile (gNxI).

The following table describes the RPCs supported under Certz.proto.

**Table 2: Certz RPCs**

| RPC        | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AddProfile | AddProfile is part of SSL profile management. It allows adding a new SSL profile. When an SSL profile is added, all its elements, that is, certificate, CA trusted bundle and a set of certificate revocation lists are NULL/Empty. So, before an SSL profile can be used these entities have to be 'rotated' using the 'Rotate()' RPC.<br><br><b>Note</b> An attempt to add an already existing profile is rejected with an error. |
| Rotate     | Rotate replaces/adds an existing device certificate and/or CA certificates (trust bundle) or/and a certificate revocation list bundle on the target. The new device certificate can be created from a target-generated or client-generated CSR (Certificate Signing Request). In the latter case, the client must provide the corresponding private key with the signed certificate.                                                |

| RPC            | Description                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeleteProfile  | DeleteProfile is part of SSL profile management. It allows for removing an existing SSL profile.<br><br><b>Note</b> An attempt to delete a not existing profile results in an error. The profile used by the gRPC server can't be deleted and an attempt to remove it will be rejected with an error. |
| GetProfileList | GetProfileList is part of SSL profile management. It allows for retrieving a list of IDs of SSL profiles present on the target.                                                                                                                                                                       |
| CanGenerateCSR | An RPC to ask a target if it can generate a CSR.                                                                                                                                                                                                                                                      |

## Configure gNSI Certz

### Before you begin

- Ensure you've created and stored SSL Profile at `cd/misc/config/grpc/gnsi/certz/ssl_profiles/`

**Step 1** Create SSL Profile using **AddProfile** RPC.

**Step 2** Rotate SSL profile using **Rotate** RPC. You can't rotate SSL profile using a command line interface.

**Step 3** Activate the profile using the **grpc gnsi service certz ssl-profile-idssl-profile-name** command.

#### Example:

Router (config-grpc) **#gnsi service certz profile ssl-profile gnxi**

**Step 4** Verify that certz.proto is configured using the **show grpc certificate** command. The below-mentioned command output is truncated version.

#### Example:

```
Router#show grpc certificate
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 32 (0x20)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=localhost,O=OpenConfig,C=US
    Validity
      Not Before: Nov  8 08:49:38 2023 GMT
      Not After : Mar 22 08:49:38 2025 GMT
    Subject: CN=ems,O=OpenConfig,C=US
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (4096 bit)
      Modulus:
        00:ea:6a:6c:25:be:9f:15:71:ce:74:89:03:ec:ef:
        0b:3b:de:58:a8:7e:28:b8:cf:b3:82:91:b4:5c:42:
        e7:d8:28:98:35:bd:35:60:a7:4e:f8:77:02:46:5f:
        27:a4:16:cf:3c:e3:24:28:69:9c:22:1e:e3:52:96:
        71:87:7c:40:0c:1f:dd:30:ea:dc:40:ca:93:00:54:
        5e:de:20:54:5b:f4:2f:9f:19:6f:71:61:28:69:3d:
        97:26:ab:e1:5f:53:3c:f1:a2:c3:14:f4:01:90:1a:
```

```

      .
      .
      .

      Exponent: 65537 (0x10001)
X509v3 extensions:
      X509v3 Key Usage: critical
      Digital Signature
      X509v3 Extended Key Usage:
      TLS Web Client Authentication, TLS Web Server Authentication
      X509v3 Authority Key Identifier:
      keyid:0A:A8:9A:6A:23:34:AE:CA:96:00:2C:F3:04:38:14:E3:D4:8D:77:BD

      X509v3 Subject Alternative Name:
      DNS, IP Address:64.103.223.56
Signature Algorithm: sha256WithRSAEncryption
b9:89:ec:60:3d:8d:7d:9c:dc:08:56:89:99:44:92:98:45:b6:
97:ba:e3:e5:f2:48:b2:44:8d:db:23:bb:a1:c0:62:79:78:18:
d7:55:f6:4a:67:5b:75:e0:c0:0b:52:51:07:36:d5:6c:c7:67:
48:86:8d:dd:70:1c:9f:7c:a1:7b:aa:a5:4e:e1:ad:cf:4c:e5:
81:db:92:cf:88:70:5a:1c:8d:de:0d:e8:b3:05:de:b9:04:4d:
23:e1:de:66:e5:08:bd:2e:31:0a:07:a6:c0:00:3a:38:2f:00:
.
.
.

```

## grpc gnsi service certz ssl-profile-id

To instruct the router to load the certz.proto, use the **grpc gnsi service certz ssl-profile-id** command in Global Configuration Mode. To disable the SSL profiles configured with certz.proto, use the no form of the command.

**grpc gnsi service certz ssl-profile-id** *ssl-profile name*

|                           |                                                                                                                                                                             |                              |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Syntax Description</b> | <i>ssl-profile name</i> Specifies the SSL-profile name for which certz. proto needs to be activated.                                                                        |                              |
| <b>Command Default</b>    | None                                                                                                                                                                        |                              |
| <b>Command Modes</b>      | XR Config mode                                                                                                                                                              |                              |
| <b>Command History</b>    | <b>Release</b>                                                                                                                                                              | <b>Modification</b>          |
|                           | Release 24.1.1                                                                                                                                                              | This command was introduced. |
| <b>Usage Guidelines</b>   | If Certz. proto is not active, then gNOI cert.proto is taken into consideration. If neither certz.proto nor cert.proto is active, then TLS trustpoint's data is considered. |                              |

| Task ID | Task ID         | Operation      |
|---------|-----------------|----------------|
|         | config-services | read,<br>write |

This example shows how to activate the certz.proto in the router.

```
Router(config)#grpc gnsi service certz ssl-profile-id gNxi
Router(config)#commit
```

## show grpc certificate

To display the active gRPC certificate management policies on the router, use the **show grpc certificate** command in EXEC mode.

### show grpc certificate

|                           |                                                        |                             |
|---------------------------|--------------------------------------------------------|-----------------------------|
| <b>Syntax Description</b> | This command has no keywords or arguments.             |                             |
| <b>Command Default</b>    | None                                                   |                             |
| <b>Command Modes</b>      | EXEC mode                                              |                             |
| <b>Command History</b>    | <b>Release</b>                                         | <b>Modification</b>         |
|                           | Release 24.1.1                                         | The command was introduced. |
| <b>Usage Guidelines</b>   | No specific guidelines impact the use of this command. |                             |
| <b>Task ID</b>            | <b>Task ID</b>                                         | <b>Operation</b>            |
|                           | config-services                                        | read                        |

This example displays the active gRPC certificate management policies on the router. The below-mentioned command output is truncated version.

```
Router#show grpc certificate
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 32 (0x20)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=localhost,O=OpenConfig,C=US
    Validity
      Not Before: Nov  8 08:49:38 2023 GMT
      Not After : Mar 22 08:49:38 2025 GMT
    Subject: CN=ems,O=OpenConfig,C=US
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
```

```
RSA Public-Key: (4096 bit)
Modulus:
  00:ea:6a:6c:25:be:9f:15:71:ce:74:89:03:ec:ef:
  0b:3b:de:58:a8:7e:28:b8:cf:b3:82:91:b4:5c:42:
  e7:d8:28:98:35:bd:35:60:a7:4e:f8:77:02:46:5f:
  27:a4:16:cf:3c:e3:24:28:69:9c:22:1e:e3:52:96:
  71:87:7c:40:0c:1f:dd:30:ea:dc:40:ca:93:00:54:
  5e:de:20:54:5b:f4:2f:9f:19:6f:71:61:28:69:3d:
  97:26:ab:e1:5f:53:3c:f1:a2:c3:14:f4:01:90:1a:
  .
  .
  .

Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature
  X509v3 Extended Key Usage:
    TLS Web Client Authentication, TLS Web Server Authentication
  X509v3 Authority Key Identifier:
    keyid:0A:A8:9A:6A:23:34:AE:CA:96:00:2C:F3:04:38:14:E3:D4:8D:77:BD

  X509v3 Subject Alternative Name:
    DNS, IP Address:64.103.223.56
Signature Algorithm: sha256WithRSAEncryption
  b9:89:ec:60:3d:8d:7d:9c:dc:08:56:89:99:44:92:98:45:b6:
  97:ba:e3:e5:f2:48:b2:44:8d:db:23:bb:a1:c0:62:79:78:18:
  d7:55:f6:4a:67:5b:75:e0:c0:0b:52:51:07:36:d5:6c:c7:67:
  48:86:8d:dd:70:1c:9f:7c:a1:7b:aa:a5:4e:e1:ad:cf:4c:e5:
  81:db:92:cf:88:70:5a:1c:8d:de:0d:e8:b3:05:de:b9:04:4d:
  23:e1:de:66:e5:08:bd:2e:31:0a:07:a6:c0:00:3a:38:2f:00:
  .
  .
  .
```

 show grpc certificate