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.

Use gRPC Protocol to Define Network Operations with Data Models

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Manage certificates using Certz.proto	Release 24.1.1	Now, you get a unique SSL profile that efficiently combines certificates, CA bundles, keys, Certificate Revocation Lists, and Authentication Policies, enhancing organization and security of certificates. It also provides a bidirectional streaming RPC and a *Finalize* mechanism, leading to improved flexibility and reliability in managing PKI elements when compared to gNOI's cert.proto.

gRPC Network Security Interface (gNSI):

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

gNSI provides security infrastructure services necessary for the safe operation of an OpenConfig platform.

gNSI RPCs

Certz RPCs

The Certz RPCs are used to perform operations on the certificate in the target device. The **certz.proto** file is available in the Github repository.

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. **Note** 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.
DeleteProfile	DeleteProfile is part of SSL profile management. It allows for removing an existing SSL profile. **Note** An attempt to remove an already existing profile is rejected with an error. The profile used by the gRPC server can't be deleted and an attempt to remove it is 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.

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.

Syslogs

You can see informative syslogs in the following conditions:

- When a new SSL profile is added.
- When the SSL profile being used by gRPC is updated/changed.
- Any significant error during RPC like failures during rotate, finalize, failure during sync to standby, failure during backup creation etc.
- When the use of certz service is diabled by config and an an attempt is made to use certz service.

Table 3: Key-Differences Between Cert.proto and Certz.proto

gNOI's cert.proto	gNSI's certz.proto
Cert.proto has a concept of certificate identifier to distinguish between leaf certificates. CA bundle doesn't have any identifier associated with it so a new request to load a bundle overwrites the existing bundle.	Certificate, CA bundle, key, CRL, and authentication policy are bound to a unique SSL profile.
The CSR generation parameter doesn't have SAN (Subject Alternative Name) extension attributes.	SAN is part of CSR. SAN is an extension to X.509 that allows various values to be associated with a single certificate. SANs are generally used in SSL certificates to define all the alternative domain names (including sub-domains) that the certificate should protect.
Cert.proto uses InstallCertificateRequest RPC to onboard a new certificate.	AddProfile RPC adds a new SSL profile which only pushes a new SSL profile name, SSL profile entities are then pushed by RotateCertificateRequest.
RotateCertificateRequest RPC to replace the existing certificates. LoadCertificateAuthorityBundleRequest RPC to load CA bundle. RevokeCertificatesRequest RPC to revoke a certificate.	Single Rotate RPC is used to upload all entities including certificate, key, CA bundle and CRL.
Cert.proto only supports RSA key type for CSR generation.	Certz.proto supports RSA, ECDSA, ED25519.