AudioCodes Quick Reference Guide

Certificates

Background

When there is a need for additional security of the SIP traffic, the Transport Layer Security (TLS) is used to secure the device's SIP signaling connections. In TLS protocol, the data is encrypted and protected. TLS communication requires certificate to authenticate recipient of the secured data.

What are Certificates?

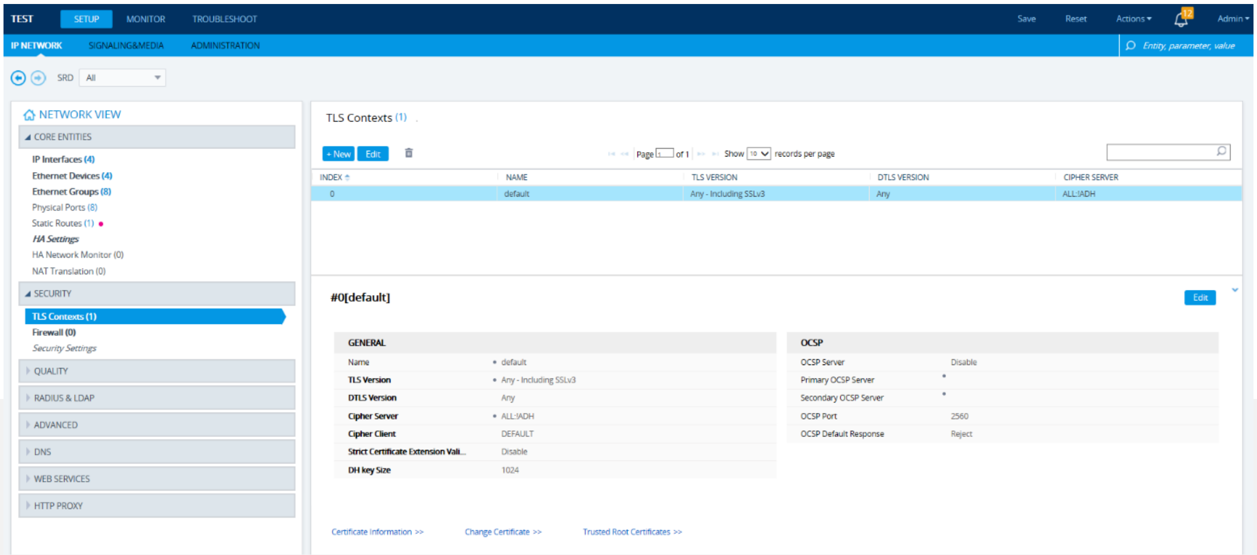
Certificates act as an identification of the device. It is a validation that the SIP traffic is going to a recognized and authenticated destination. The device inherits trust with the other proxy server with the use of certificates.

How does AudioCodes use Certificates?

AudioCodes uses certificates to deliver secured SIP traffic and services. In addition, certificates are used to provide security access to the device, Web (HTTPS) sessions, Telnet sessions and SSH sessions.

How do I load Certificates on the device?

The TLS Contexts Table is located under Setup→IP Network→Security→TLS Contexts. There are links to Change Certificate and Trusted Root Certificates at the bottom.



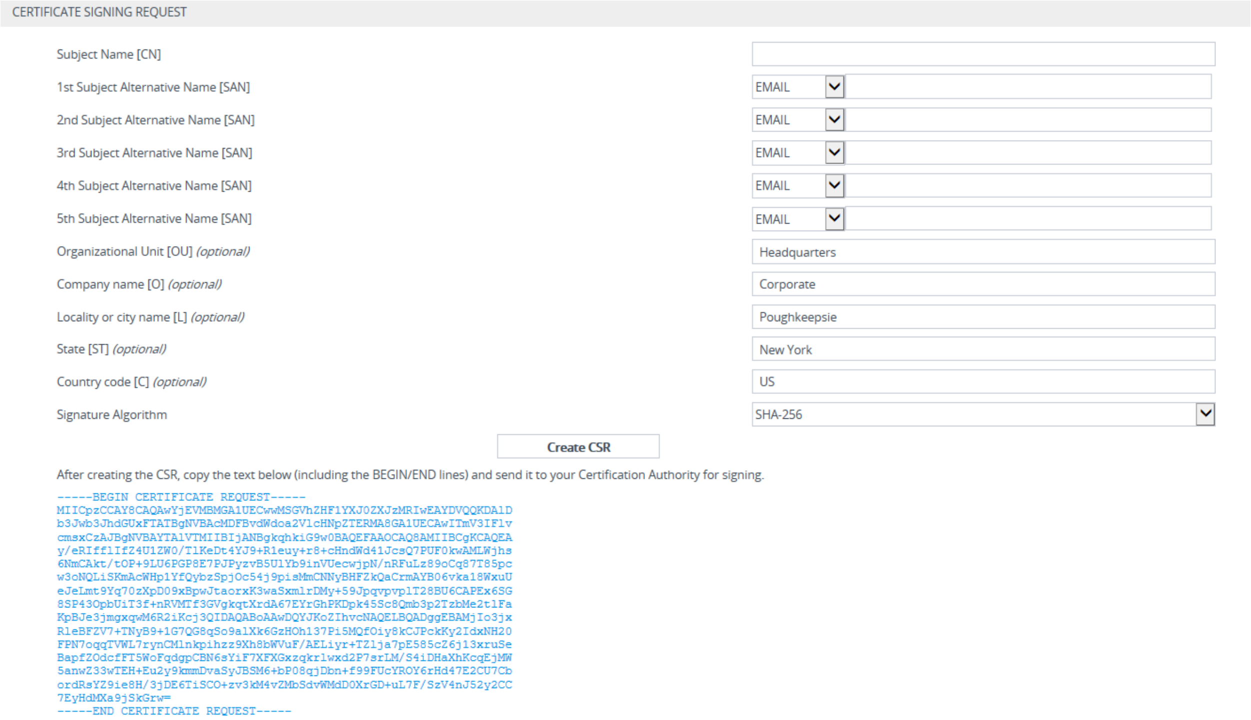
INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	Any - Including SSLv3	Any	ALL:!ADH

#0[default]

GENERAL	
Name	• default
TLS Version	• Any - Including SSLv3
DTLS Version	Any
Cipher Server	• ALL:!ADH
Cipher Client	DEFAULT
Strict Certificate Extension Vali...	Disable
DH key Size	1024

OCSP	
OCSP Server	Disable
Primary OCSP Server	•
Secondary OCSP Server	•
OCSP Port	2560
OCSP Default Response	Reject

Certificate Signing Request (CSR): On Change Certificate page, there is a section “Certificate Signing Request”. Fill in the required fields according to your Certification Authority (CA) or security provider’s instructions. Click Create CSR button. Copy this textual CSR and send to your CA to sign.



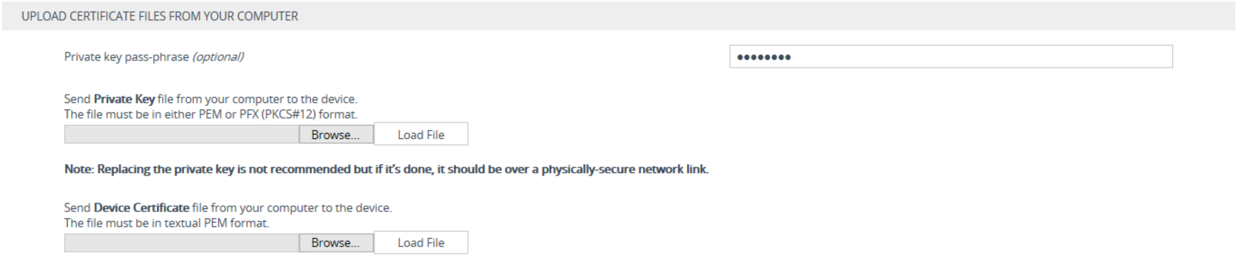
CERTIFICATE SIGNING REQUEST

Subject Name [CN]	
1st Subject Alternative Name [SAN]	EMAIL
2nd Subject Alternative Name [SAN]	EMAIL
3rd Subject Alternative Name [SAN]	EMAIL
4th Subject Alternative Name [SAN]	EMAIL
5th Subject Alternative Name [SAN]	EMAIL
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US
Signature Algorithm	SHA-256

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpzCCAY8CAQAwYjEVMBMGA1UECwwMSGVhZHF1YXJ0ZXJzMRIwEAYDVQQKDAlD
b3Jwb3JhdGUxFTATBgNVBAcMDFBvdWdoa2VlcHNpZTERMA8GA1UECAwITmV3IFlv
cmsxCzAJBgNVBAYTAlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
y/eRIfflIfZ4U1ZW0/TlKeDt4YJ9+R1euy+r8+cHndWd41JcsQ7PUF0kwAMLWjhs
6NmCAkt/tOP+9LU6PGP8E7PJPyzvB5UlYb9inVUecwjpN/nRFuLz89oCq87T85pc
w3oNQLiSKmAcWHp1YfQybzSpjOc54j9pisMmCNNyBHFZkQaCrmAYB06vka18WxuU
eJeLmt9Yq70zXpD09xBpwJtaorxK3waSxmlrDMy+59JpqvpvplT28BU6CAPEx6SG
8SP43OpbUiT3f+nRVMTf3GVgkqtXrdA67EYrGhPKDpk45Sc8Qmb3p2TzbMe2tlFa
KpBJe3jmgxqwM6R2iKcj3QIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAMjIo3jx
RleBFZV7+TNyB9+1G7QG8qSo9alXk6GzHOh137Pi5MQfOiy8kCJPckKy2IdxNH20
FPN7oqqTVWL7rynCMlnkpihzz9Xh8bWVuF/AELiyr+TZlja7pE585cZ6j13xruSe
BapfZOdcfFT5WoFqdgpCBN6sYiF7XFXGxzqkrlwxd2P7srLM/S4iDHaXhKcqEjMW
5anwZ33wTEH+Eu2y9kmmDvaSyJBSM6+bP08qjDbn+f99FUcYROY6rHd47E2CU7Cb
ordRsYZ9ie8H/3jDE6TiSCO+zv3kM4vZMbSdvWMdD0XrGD+uL7F/SzV4nJ52y2CC
7EyHdMXa9jSkGrw=
-----END CERTIFICATE REQUEST-----
```

Device Certificate: On Change Certificate page, there is a section “Upload certificate files from your computer”. For Server Certificate or Device Certificate provided by your CA, upload that certificate as a Device Certificate.



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

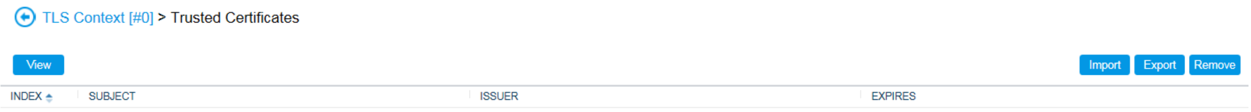
Private key pass-phrase *(optional)* ••••••••

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

Trusted Root Certificate: On Trusted Root Certificates page, this is where you can upload Intermediate Certificate or Root Certificate.



TLS Context [#0] > Trusted Certificates

INDEX	SUBJECT	ISSUER	EXPIRES

What resources or guide do I use in loading certificates?

AudioCodes User's Manual also includes a detailed configuration guide of importing certificates including Private Key and Self Signed Certificates. Please refer to LTRT-27062 Mediant 1000B Gateway and E-SBC User's Manual Ver. 7.2 under Section 10 Configuring SSL/TLS Certificates. Any other Mediant device User's Manual Ver. 7.2 will also have a TLS Certificate Configuration section.

For any further questions regarding this topic or other technical topics:

- Contact your AudioCodes Sales Engineer
- Visit our AudioCodes Services and support page at https://www.audiocodes.com/services-support
- Access our technical documentation library at https://www.audiocodes.com/library/technical-documents
- Access to AudioCodes Management Utilities is available at https://services.audiocodes.com/app/answers/detail/a_id/20
- Contact Technical Support to submit a support ticket at https://services.audiocodes.com

INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED TO THE BEST OF AUDIOCODES KNOWLEDGE, AND AUDIOCODES SHALL NOT BE HELD LIABLE FOR ANY INACCURACIES.