How To?

Tips and Tricks about ScopTEL. Because Communication Matters!

SCOPSERV INTERNATIONAL INC.

How to Use the ScopTEL Certificate Manager to Enable TLS Encryption

What is TLS Encryption?

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as «SSL», are cryptographic protocols that provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). The Transport Layer Security protocol aims primarily to provide privacy and data integrity between two communicating computer applications. *(Wikipedia: https://en.wikipedia.org/wiki/Transport_Layer_Security)*

Certificate Manager integrated in ScopTEL IP PBX

You can create TLS certificate using the Certificate Manager module integrated to ScopTEL PBX.

Self Signed Certificates are generally not supported by phone Manufacturer's therefore it is recommended you check with your phone hardware vendor to see which Certificate Authorities are supported.

You will first have to use the ScopTEL Certificate Manager to create your own Certificate Signing Request (CSR) in order to purchase a Signed Certificate from a supported Certificate Authority. Most Certificate Authorities will provide you with a Root Certificate and a Chained Certificate (Chained Certificates are not mandatory but are very commonplace).

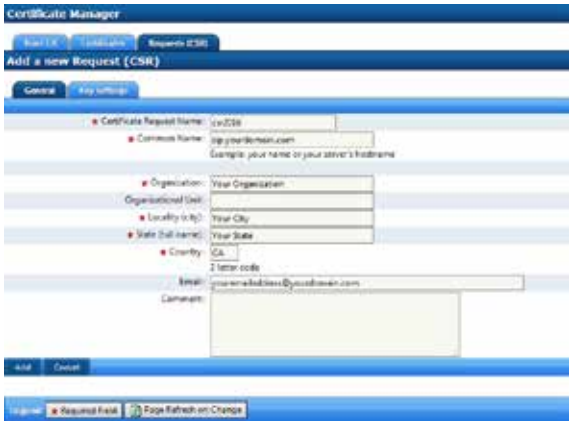
Once you have the Root CA, Certificate Chain and a Signed Certificate from a supported Certificate Authority, you can use the ScopTEL Certificate Manager to create Certificates for the following purposes:

- Encrypting GUI communications using SSL (HTTPS)
- Encrypting Phone Provisioning files during phone download using SSL (HTTPS)
- Encrypting SIP signalling with SSL (TLS)
- Encrypting SIP audio streams with SSL (SRTP)

Procedure

To create the CSR, open Certificate Manager and click on Add a New CSR.

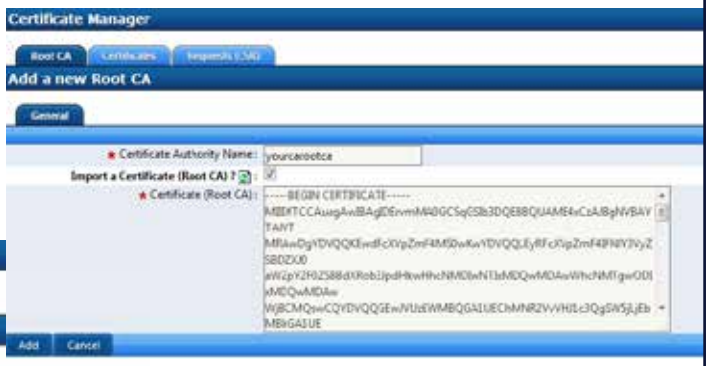
In the Key Settings tab, select a Digest Algorithm supported by your IP phone's manufacturer. Click Add and download your CSR.

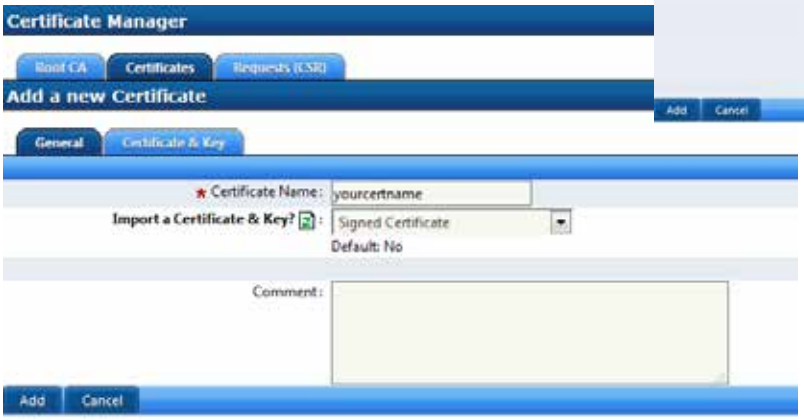


Copy and Paste your Certificate Request to your Certificate Authority when you your purchase your CA for Domain Validation. Wait for your CA to send you your Certificate before generating your Certificate. You will copy and paste the Private Key Data into your Server Authentication Certificate in a later step

Copy and Paste your CA's Root CA into the text box and click Add.

In Certificates Tab, Give your Certificate a name.
Select Import Certificate & Key = Signed Certificate.
Then click on the Certificate & Key tab.





Copy and Paste your CA's Signed Certificate data into the Signed Certificate text box. Copy and Paste your CSR's Private Key data into the Private Key text box and click Add. Copy and Paste the Certificate Chain data you received from your CA when they issued your Certificate and click Add.

Congratulations you have configured your Certificates! But there's more!

You can now configure the Server to enable SSL and to use HTTPS Provisioning for your IP Phones. To continue and get the complete procedure, access the Client Portal of the website and dowload 'ScopTEL - Certificate Manager' training module in the ScopServ University page.

Our team of experts can help you! Contact us for more information or to find the reseller in your region.

Tel.: 1 866-722-3292 •• info@scopserv.com

ScopServ International Inc. recommends using the latest ScopTEL version available. Update your software to get all features.

www.scopserv.com