Oct 22, 2020 21:25

How to install certificate from an SSL Certificate Provider to PBX

In case you've decided to use specific SSL certificate or PBX has no access to Wildix certificate-updater service.

Created: February 2020

Updated: August 2020

Permalink: https://confluence.wildix.com/x/O4O5Aw

Important: in WMS 5.0X Custom certificates are accepted only with signature algorithm not lower than SHA256.

Intro: What is SSL and an SSL Certificate

Secured Socket Layer (SSL) is the technology that ensures that data between two machines (in our case – a browser/ phone and PBX) is transmitted securely in an encrypted connection (HTTPS).

An SSL Certificate is a digital certificate that confirms the identity of a website. It is usually represented as a pair of small text files with encrypted data (Certificate *.crt and Private Key *.key).

To implement SSL on your PBX in the absence of access to Wildix certificate-updater service, you need to:

- submit a CSR (Certificate Signing Request) to an SSL Certificate Provider (Certification Authority) and get an SSL Certificate

or

- create **self-signed certificate** by you own. These certificates are easy to make and they are free. However, they do not provide all of the security properties that certificates signed by a CA aim to provide.

Then you need to import certificate and private key to PBX.

Step-by-step guide

Step 1.

You can rather request a certificate from a Certification Authority or generate a self-signed certificate.

Get a certificate from a Certification Authority

1. Select one of Certificate Providers that suit your requirements. For instance, SSL.com, Namecheap, TheSSLStore, GoDaddy, GlobalSign, DigiCert, Thawte, GeoTrust, Entrust, Network Solutions, etc.
2. Create a CSR (Certificate Signing Request) either using a Linux shell (PBX shell preferred) or Certificate Provider tools:

   Linux shell command to create CSR

   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
   ```

   CSR configuration requires the details as follows below:

   - *Common Name (the domain name of PBX).* ***It is highly recommended to use sub-domain wildcard (*.<yourdomain>.<com>)***
   - *Country (two-letter code)*
   - *State (or province)*
   - *Locality (or city)*
   - *Organization*
   - *Organizational Unit (Department)*
   - *E-mail address*
3. Keep resulting key and csr files. Its content should include encrypted data and headers :

   -----BEGIN CERTIFICATE REQUEST-----

   ...some data...

   -----END CERTIFICATE REQUEST-----

   and

   -----BEGIN PRIVATE KEY-----

   ....some data...

   -----END PRIVATE KEY-----
4. Order a certificate from one of Certificate Providers and provide them the CSR file
5. Validate domain ownership with CA using one of three validation types: Domain Validated (DV), Organization Validated (OV), Extended Validation (EV)

   > Please note that some sub-types require internet connection.

Generate self-signed certificate

Generate certificate on LINUX system using the command:

```
openssl genrsa -des3 -out server.key 2048
openssl rsa -in server.key -out server.key
openssl req -sha256 -new -key server.key -out server.csr -subj "/C=IT/ST=TN/L=My City/O=My Company
/CN=examplecompany.com"
openssl x509 -req -sha256 -days 3650 -in server.csr -signkey server.key -out server.crt
```

⚠ Use your country instead of IT (Italy) and your region instead of TN (Trento) in the string **"/C=IT/ST=TN /L=My City/O=My Company/CN=examplecompany.com"**

Output:

server.crt server.csr server.key

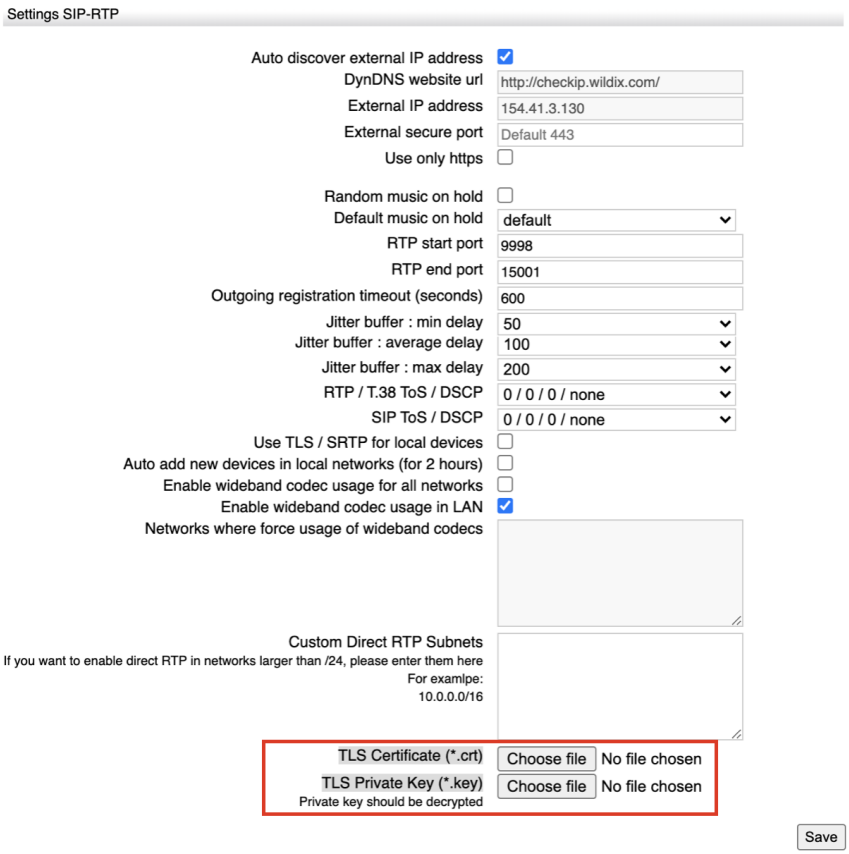
Step 2. Configure internal DNS

Configure internal DNS. PBX domain name should correspond IP of PBX.

Step 3. Import the certificate

To import the certificate:

1. Login PBX web interface with administrative account
2. Go to WMS *Settings -> PBX -> SIP-RTP*
3. Upload certificate files: Certificate *.crt and Private Key *.key
4. Click **Save**


Settings SIP-RTP
Auto discover external IP address
DynDNS website url
http://checkip.wildix.com/
External IP address
154.41.3.130
External secure port
Default 443
Use only https
Random music on hold
Default music on hold
default
RTP start port
9998
RTP end port
15001
Outgoing registration timeout (seconds)
600
Jitter buffer : min delay
50
Jitter buffer : average delay
100
Jitter buffer : max delay
200
RTP / T.38 ToS / DSCP
0 / 0 / 0 / none
SIP ToS / DSCP
0 / 0 / 0 / none
Use TLS / SRTP for local devices
Auto add new devices in local networks (for 2 hours)
Enable wideband codec usage for all networks
Enable wideband codec usage in LAN
Networks where force usage of wideband codecs
Custom Direct RTP Subnets
If you want to enable direct RTP in networks larger than /24, please enter them here
For examlpe:
10.0.0.0/16
TLS Certificate (*.crt)
Choose file
No file chosen
TLS Private Key (*.key)
Private key should be decrypted
Choose file
No file chosen
Save