

Enabling TLS for Business Systems

This applies to On Premise Business Systems and Call Center Systems and assumes you already have your certificate files. UX customers please contact support, and they will be able to assist you.

It is important to note, TLS encrypts the SIP portion of your call. To encrypt your actual conversation, you must use SRTP.

Server Setup

1. Browse to Settings → Protocols → SIP → enable TLS
2. Create an asterisk.pem file which should consist of the Private key and Certificate.
3. SSH to the server
4. Change directories to `cd /opt/pbxware/pw/etc/asterisk/`
5. If there is an existing asterisk.pem file rename it.
`asterisk.pem.bak`
6. Now place the new asterisk.pem file into
`/opt/pbxware/pw/etc/asterisk/`
7. Next, access asterisk by typing the following command
`asterisk -rvvv`
8. Restart asterisk by typing `restart now`
9. Access asterisk again `asterisk -rvvv`
10. Check if TLS is enabled by entering `pjsip show transports`

Extensions Setup

1. Log into the GUI.

Network Related

Transport:	TLS
WebRTC Enabled:	UDP
Encryption:	TCP
	TLS
NAT:	yes
Direct media:	No
Direct RTP setup:	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Not Set
Qualify (ms):	8000
Host:	dynamic
Default IP:	
Maximum Connected Devices:	10

2. Browse to Extensions.
3. Edit the extension in question.
4. Select Show Advanced Options, if it is not set to show by default.
5. Go to the Network Related section.
6. Click the drop-down arrow in the Transport field and select TLS.

SRTP

To add encryption to your RTP traffic

1. Move to the Encryption field and select: Offer if possible TLS (TLS only)

Version01.01202024