# Preferences
# TCP, TLS and Secure RTP Options
# TCP, TLS and Secure RTP Options

We support both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) communication protocols. While UDP is by far the most common of the two protocols TCP is stated to have advantages.

## TCP advantages

- **Keep Alives:** SIP must periodically send out keep-alives to maintain the NAT table entry. The required frequency of keep-alives is much higher for UDP (maybe every 30 seconds) vs TCP (maybe every 15 minutes). While not relevant for small installations TCP has significant advantages within enterprise installations.
- **TLS:** In a security conscious world TCP enables your end points with Transport Layer Security (TLS) which over the separate port 5061 instead of the normal 5060 for UDP.
- **SRTP (Secure Real-Time Transport Protocol or Secure RTP):** SRTP encrypts or "codes" the voice data itself so that no one can understand what is being said except the person who has the decoding "key", or the person to whom the call is being made. SRTP and SIP TLS encrypt different parts of the VoIP service but together security conscious organisations such as financial or military to use this service.

If you choose to use Secure Encrypted RTP this may cause calls to fail if you have not configured SRTP on your client.

# Preferences

## Quick Guide

### Step One: TCP, TLS & Secure RTP Options

1. Log into [https://now.tel2.co.uk](https://now.tel2.co.uk) > select number you wish to set up remote call back on.
2. Select **CloudPBX > Advance > TCP, TLS & Secure RTP Options.**
3. Select one of the SIP Transport options.
4. Enable Secure Encrypted RTP
5. Click **Save settings** to update

SIP over TCP and TLS support for secure encrypted signalling on calls. SRTP is now also supported for encrypted calls.

SIP Transpor
| |
| --- |
| ✓ Support for UDP, TCP and TLS (Default) |
| Force Support for UDP Only |
| Force Support for TCP Only |
| Force Support for TLS Only |

☐ Force calls                                may cause calls to fail if you have not configured SRTP on your client)

☐ Force calls to use Secure Encrypted RTP? (WARNING: This may cause calls to fail if you have not configured SRTP on your client)

# Preferences

## Step Two: Change PBX/handset transport

1. Log into IP PBX / Handset
2. Select Account
3. Find option to change Transport > TLS

# Preferences

| | |
|---|---|
| Register Status | Registered |
| Line Active | Enabled |
| Label | Mike |
| Display Name | MikeJ |
| Register Name | 6128970750 |
| User Name | 6128970750 |
| Password | •••••••• |
| Enable Outbound Proxy Server | Disabled |
| Outbound Proxy Server | Port 5060 |
| Transport | **(1)** TLS |
| NAT | Disabled |
| STUN Server | 0.0.0.0 Port 3478 |

**SIP Server 1**

| | |
|---|---|
| Server Host | **(2)** tls.l2access.com.au Port 5061 |
| Server Expires | 180 |
| Server Retry Counts | 0 |

**SIP Server 2**

Unique solution ID: #1038
Author: Support
Last update: 2016-05-28 08:10