

# How to enable TLS + SRTP

Transport Layer Security (RFC 2246) runs at Layer 4 protocol on top of TCP (see DTLS for UDP).

## Advantages

- TLS is the recommended security mechanism for Session Initiation Protocol (SIP).
- NAT traversal -- since IPsec is Layer 3 protocol NAT is not supported, while TLS works flawlessly
- HTTP Digest sessions in SIP environments are based on TLS.
- SIP clients implementations natively supports TLS
- Provides privacy (private user identity)
- Provides user authentication instead of data-origin authentication (higher degree of authentication)

## Disadvantages

- Both of the TLS models require the server and client to support PKI features, such as certificate validation and certificate management. Not all clients and solutions support PKI. PKI is typically used in complex environments
- PKI is computationally expensive since it uses public key cryptography
- TCP and TLS pose significant memory consumption and scaling issues when you have tens of thousands of TCP connections. UDP and IPsec are easier to scale. TCP is not well liked by service providers since the overheads associated with its mass use are significant compared to UDP.
- Runs on top of TCP only (connection-oriented). There is a subset version of TLS that is supported for use with UDP called DTLS (RFC 4347)
- Provides only hop-by-hop security. What this means is that every intermittent hop would need to be secured with TLS. With this, it doesn't provide true end-2-end security
- TLS cannot be used to secure VoIP RTP media streams ----> SRTP is used instead
- In Server-Side Authentication, only one end is authenticated
- TLS does not handle dead office recovery scenarios efficiently. As mentioned, PKI is CPU intensive therefore when you need to handle re-authentications for all endpoints, this is going to significantly slow down your system

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. It was first published by the IETF in March 2004 as RFC 3711. Since RTP is closely related to RTCP (Real Time Control Protocol) which can be used to control the RTP session, SRTP also has a sister protocol, called Secure RTCP (or SRTCP); SRTCP provides the same security-related features to RTCP, as the ones provided by SRTP to RTP.

Deploying TLS for devices that can be provisioned by uniteme/sipxcom (like Polycom phone) is as easy as just setting the transport to TLS in Line->Registration.

The screenshot shows a configuration page for a 'Registration server'. Under the 'Primary registration server' section, the following settings are visible:

- address:** test (Default: test)
- port:** 0 (Default: 0)
- transport:** TLS (Default: TCPOnly). A dropdown menu is open showing options: UDPOnly, TCPpreferred, DNSnaptr, TCPOnly, and TLS (which is selected and highlighted in blue). A tooltip explains the options: 'UDPOnly: If empty or DNSnaptr and if Address is a hostname and Port is 0 or empty, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, address is an IP address, or a port is given, then UDP is used. If set to TCPpreferred: TCP is the preferred transport, UDP is used if TCP fails. If set to UDPOnly: Only UDP'.
- expires:** 3600 (Default: 3600)
- Re-registration interval:** 60 (Default: 60)
- register:** checked (Default: checked)
- retryTimeOut:** 0 (Default: 0)
- retryMaxCount:** 3 (Default: 3)
- expires.lineSeize:** 30 (Default: 30)

To enable TLS on clients that are not provisioned (Zoiper) by uniteme in the case you are using a self signed certificate (default SIP certificate used by sipxcom/uniteme) and if the client doesn't offer the option to import it automatically you will need to first copy Certificate Authority from System ----> Certificates as shown in below screen and then paste it in a txt file renamed as cert.pem

CERTIFICATES

- Web Certificate
- SIP Certificate
- Certificate Authorities

ca test

[Hide certificate](#)

```
Version: 3
Serial Number: 1528121299080
Signature Algorithm: SHA1withRSA
Issuer: CN=US, ST=MaryState, L=MaryTown, O=test, OU=sipXecs, CN=ca.test, E=root@test
Not Before: Mon Jun 04 16:08:19 EEST 2018
Not After: Sun Jun 04 16:08:19 EEST 2028
Subject: CN=US, ST=MaryState, L=MaryTown, O=test, OU=sipXecs, CN=ca.test, E=root@test
-----BEGIN CERTIFICATE-----
MIIDDCAYqAwIEAgITGMPF11JCIMAGCCqgSiIDQEBRQUMMSKcaBZgWVBAIT
A1VtRDEuCWUVQQU1BaRbLlF6SFTTQM46IIEEwWQ6SU6VSpLKDMA6A1UE
CgwE5dVsdEKGGA4GA1DECVw5c2lv6GVjcaEQMAGAIUEAwvHYZEuo5VadEYMVg
C9g8I6IsDQEIARVzaw5v8EBOZKH08KXDTE4M0YwNDEaMdgoVVOXDI4M0YwNDEa
MDgoVVOwaf1MA6A1DEEMACTVtAETAFBQVtB5MCETa5T05YXZ1M5a3cyTVQ09
DAdBm1U3sduMQoCwYDQ0QDAB0EKX086A5DgYDQ0LDAaXEBYRwARaWdYD
VQ0DA9j18S1Z0M8p5F9fJ0o2IhvcRQKaf7g1y69Q8R6e9Ug9gEiMAAGCCqg
S1b3DQEBRQUMMSKcaBZgWVBAITGAGCw/ep1T9paR963amS0H9C9p58S098
Yus*gd*OwTRgfl3eo2VIGUSimQVmkCF2jF0aV/BN3j9*2E3w0C6e5eOw
Wk0aRg6dITR1M5eCUC09w89gCf84P7HtF9z3JyruaBZIAqhm+e3*21P8
C6h5w0eMESyE37QoqVtLXsZ0N10ZKX1Yhaq7M3j4p3yE9Duh+76e4N4TEAK
xS5ZKouru3Dq1YdCF2m5B5wV73M/7o8Rgh6vuba1o0E7j3400FAs0v1Jq
Dm4*E11E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1E1
MBIGAIUEwES/wQZTBAB5CAG5wDQYJ0o2IhvcRQEBRQUMMSKcaBZgWVBAIT
OT1YudhDQpF8A0e8Feb0CEFT34Resaw0E1L23kcaEabENTx10Ac/0K07m
26bv870w9P7wQ087F87B910MGgla65ab30u3W54q3M43w5411ab0884
eTSWQu2GH04F*PpeIaLIX82E8875suYqHt22pw/w13469QMIEE002I2DMgk4C
KIDF0m5eAs5Pz1+c08ADu01e04x8bCp2Th2meDqkXWVwre6vT7j686Q6Q
24RUV734e+08085a33Ak2hw5WCT001jTmuc611w9Ct18X0wq82se781ba/R
o*oq6vY120=
-----END CERTIFICATE-----
```

Self-Signing Certificate Authority

Encryption strength:

Rebuild Self-Signed Certificate Authority:

Upload Certificate Authority:

Certificate  verisignclass3ca

After importing Certificate Authority you will need to set transport to TLS.

Registration server

Primary registration server

address:  (Default: test)

port:  (Default: 0)

transport:  (Default: TCPOnly)

expires:  (Default: 3600)

Re-registration interval:  (Default: 60)

register:  (Default: checked)

retryTimeOut:  (Default: 0)

retryMaxCount:  (Default: 3)

expires.lineSeize:  (Default: 30)

Once the transport was changed to TLS one can simply verify this by looking on the registration page for ""transport=tls"" option.

sip:200@test <:sip:200@10.3.0.200:34274;transport=tls;x-sipX-nonat>

## Enabling SRTP

For provisioned phones go to Phone Settings page --> Security tab and enable SRTP:

The screenshot shows the ezuce web interface. At the top left is the ezuce logo with the tagline 'be there'. A navigation bar contains tabs for 'USERS', 'DEVICES', 'FEATURES', 'SYSTEM', and 'DIAGNOSTICS'. Below this is a 'PHONE SETTINGS' header. On the left is a sidebar menu with options like 'Identification', 'Lines', 'E911 Location', 'Date/Time', 'User Preferences', 'DTMF', 'Sound Effects', 'Voice/Codecs', 'Video', 'Voice Quality Monitoring', 'Quality of Service', 'SNTP', 'RTP', 'TCP Keep-Alive', 'Web Server', 'Call Handling', and 'Hold Reminder'. The main content area shows settings for 'Phone: 0004f2819fa3 / Polycom VVX 500'. Under the 'Security' section, there are settings for 'tagSerialNo', 'Password Length' (with input fields for 'admin' and 'user'), and 'SRTP'. The 'SRTP' section includes 'Enable SRTP' (checked), 'Offer SRTP' (unchecked), and 'Require SRTP' (unchecked). Each checkbox has a '(Default: unchecked)' label.

For Zoiper you need to manually select SRTP (TLS with SDES SRTP).

Next step to verify that your communications are secure will be to take a packet capture either by port mirroring on switch level if you are using just hard phones or launching a Wireshark capture on the PC where softphone is installed.

**Warning: Using TLS/SRTP may introduce interoperability issues between SBCs, gateways, and phones. Its use may break certain call features such as Bridged Line Appearance (BLA) / Shared Line Appearance (SLA), or introduce issues with call scenarios such as conferencing and call transfers.**

**Note: Polycom does not support wild-card certificates**