

# 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 for the dropdown explains the logic: '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: 1528121299090
Signature Algorithm: SHA1withRSA
Issuer: CN=J, ST=HayState, L=HayTown, O=test, OU=sipXecs, C=ca.test, E=root@test
Not Before: Mon Jun 04 16:08:19 EST 2018
Not After: Sun Jun 04 16:08:19 EST 2028
Subject: CN=J, ST=HayState, L=HayTown, O=test, OU=sipXecs, C=ca.test, E=root@test
-----BEGIN CERTIFICATE-----
MIIDDCANyAgwIEAg1GAMP1L1JCIMAGOCg8IhdDQERBQUAMH9kcaAb7gWVBAIT
A1VTRBwCwYVQ1Q1aB8e1f6SFTTQMA4IEdewWgP6V95pL2M4aGAIUE
CgwE5vSadEKQA4GA1DECvWfC2lv8GVjcaEQMA4GA1UEAwwSY2EudG9udEYMBYg
C9g5I6sDQERARVZm5wE8B0XNHR8KXTE4M0YwNDEaMgQvOVoKDI4M0YwNDEa
MgQvOVoE8I6A4A1DEEMCT7M6E7AF8V783MCTEua78V783M6BwCytVYVQ8
DAdBm1Ub3suaMQwCwYDQ0QDAB0EXNHR8wDgYDQ0LDAaXEBYwNwARwDgYD
VQ0DAj13S1ZEMH9wFgfJk0z2IhvcNKA8Fg1yb9QjR8e9QggEAMAGOCg8I
S1s3UQ8MAQAAsIEdewWgE8aIEQAQw/ep1VQp9rF68amSDFE8Cw8aCS9098
Yus*gd*0w7Bqf1ke0ZVIGU9aimGEvMkCF2jP0cV/NNj9*2EymhC6e5e0w
Wk0u8gdeITK1Mj+eCUCQ8w89gCF84F7HfPq03jyua8EIA4q8ha+e3*21PF
Ch65w0eM8BjE37Q0qVUXaZON10ZK1Yhag7Mj4p9y9EWDub+76e4NLTAEk
xS52Ekcurea3Dq1YdCF2m5e3wV73M/7cdRgh9vuba10eD7j3400FA8e017Jg
Zm4*E11E1M2E7wagjwv1jdfef6vTa1A*o7j/nf+e3eEw1j3gM8M3F7AD
MBIGAUdEwE8/wQ2HABAF8CAQAwDQYJKoZIhvcNAQEFQAQDgEAEVFP0Xa9a8
OT1jushDQpF8A0e8F6b0CEFT3AResawGEL22kcaAEabEHTx10Ae/OK07m
26bva70w9PYwQD8F78V783M6g1a6a13a3u17b3q8M12w5414k888a
e78WQ2u8H04F*PgeIaLX82E887+5urygHt22pw/w13489QMIE8002I2DMgK4C
KIDF0m8e8A5Fyz+c8MADu01e04k88Cp2Th2m8dQhXWYwv6e7T7j68QK6Q
248V73E+e0809a3A3k8w8WCTM01jTmuc611wQc11k0w*888e781ka/A
o*oq6v7120=
-----END CERTIFICATE-----
    
```

A self-signed certificate authority is used to as a convenience to secure the system with requiring outside security providers like Verisign or CAcert.org. If you'd like to use these providers for some or all of the certificates used in this system, navigate to import the appropriate authority below and then upload respective certificates to respective pages.

Encryption strength: **2048 bit**

Installed web certificate is using 2048 bit encryption; installed SIP certificate is using 2048 bit encryption

Rebuild Self-Signed Certificate Authority: **Rebuild**

This will regenerate a new certificate authority and all certificates signed by that authority.

Upload Certificate Authority: **Browse...** No file selected. **Upload**

Upload certificate authority file. Useful when services need to create secure connections with other systems that have certificates signed with an authority not listed below.

<input type="checkbox"/>	Certificate	Description
<input type="checkbox"/>	verisignclass3ca	<a href="#">Show certificate</a>

**Delete**

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

Registration server

Primary registration server

address:  (Default: test)

port:  (Default: 0)

transport: **TLS** (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.

**Refresh**

## Enabling SRTP

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

The screenshot shows the ezuce web interface for configuring a phone. The top navigation bar includes 'USERS', 'DEVICES', 'FEATURES', 'SYSTEM', and 'DIAGNOSTICS'. The 'PHONE SETTINGS' page is displayed, with a sidebar on the left listing various settings categories. The main content area shows the 'Security' settings for a phone with ID '0004f2819fa3' and model 'Polycom VVX 500'. The 'Security' section includes a 'tagSerialNo' checkbox (unchecked), a 'Password Length' section with input fields for 'admin' (1) and 'user' (2), and an 'SRTP' section with three checkboxes: 'Enable SRTP' (checked), 'Offer SRTP' (unchecked), and 'Require SRTP' (unchecked). Each checkbox has a default status note in parentheses.

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**