

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.

Registration server

Primary registration server

address	test	(Default: test)
port	0	(Default: 0)
transport	TLS	(Default: TCPOnly)
expires		(Default: 3600)
Re-registration interval	60	(Default: 60)
register	<input checked="" type="checkbox"/>	(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**

[Hide certificate](#)

```

ca test

-----BEGIN CERTIFICATE-----
MIIDDCAnYgAwIBAgITGAMP1L1JCIMAGCCgdsIhdDQEERQUAMHScKcaBz8gVTRAIT
A1VTBRDQwYVQVQ1T3A8Bsl1P6SFTTQM461IEdwWq8SUVGSpLkDMa4GAIUE
CgwE6VsdEKQGA4GA1DECvWfsc2lv8GVjYjEzQMA4GA1UEAwwHY2EudG9vdDEYMBYg
Cjg9S1Is1dQEVjARV1andwSBQKXHM8KDTIE4M0YwNDEwMDEyODUwNDE0MDYwNDEw
MDg0OvcwY091MDA4A1IEMACTY0aCtFgE3FgYUFRK2E5Y0YVYXN0e0yYVQVQGR
DAdBm1U03suaMQwCwYVQVQDABOEXHOM8aBdYgYVQVQILDAAsXEBYwNwM8aBdYgYV
VQVQDAh3I3S1ZHM8RwFgYUFRK2E5Y0YVYXN0e0yYVQVQJH8R9Q9gEIAAGCCg6
S1h3UQZKAQAAIEM0wEgEKAIEQAQW/ep1Ug9aF68-am5FQF-Cmp0ha0C8989
Yus*gd*WwYRgf1kco2VIGU9s1mGEVmKCF2jF0cV/NNj9*2E3wM6C6e5e0w
Wk0aBgdBTkLVM+eCUCQeW9fjCF4PFTtFqz0JyreaBZIA-qh0ha+EA*2IjF
Cb65w0aM8BjF07QoqTULXa2ON10EXIYhag7Mj4p9yFwDusb7e4nL4TEkK
xS522kour3Dq1YdcE2m5e3wV73M/7cdRgh9vub410eDj3300F4A8oV1Jq
Zm4*E2IEMW2Wangjwaj2jdf6e6vTala*o7y/nf+e30Eew1JjgM8M8GjF3JF
MBIGAUUdWES/+QTHAIBAFCAQAwDQYJKoZIhvcNAQEFQAQDggEBAEY8FOxS8
OT1jusbDQpFE8U4e8F8eoCEFT34ResaWDEL22k2AaEabENTx10Ae/OKO7m
26Ww70w9FFWuQDSF75uF8I0M6q146a130u17h5qj8a12w5414k088a
e78WEQu2GH04F4PgeIaLX82E88T5suYqHt22pw/w13489QMIE8002IDM6gK4C
KIDFDm888A5Fyz+cMMADu01e04k8BcP2Th2m8dQhXWYkwe6cV7j686Q6Q
2dYUv73e+e0809a3A1k8w8WCTW801j1wuc611wgCr1Ad0w7g82e781ka/R
o7oqe7y12D=
-----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

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

Rebuild Self-Signed Certificate Authority

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

Upload Certificate Authority No file selected.

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	Show certificate

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)
0, empty, 1 to 65535
 if set to TCPonly: if empty, 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. If 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 (Default: 3600)

Re-registration interval TLS (Default: 60)
positive integer between 5 and 65535.

register (Default: checked)
0, 1 enable registration

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>

Refresh

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 options 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 option has a default status 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