How to enable TLS + SRTP

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

Advantages

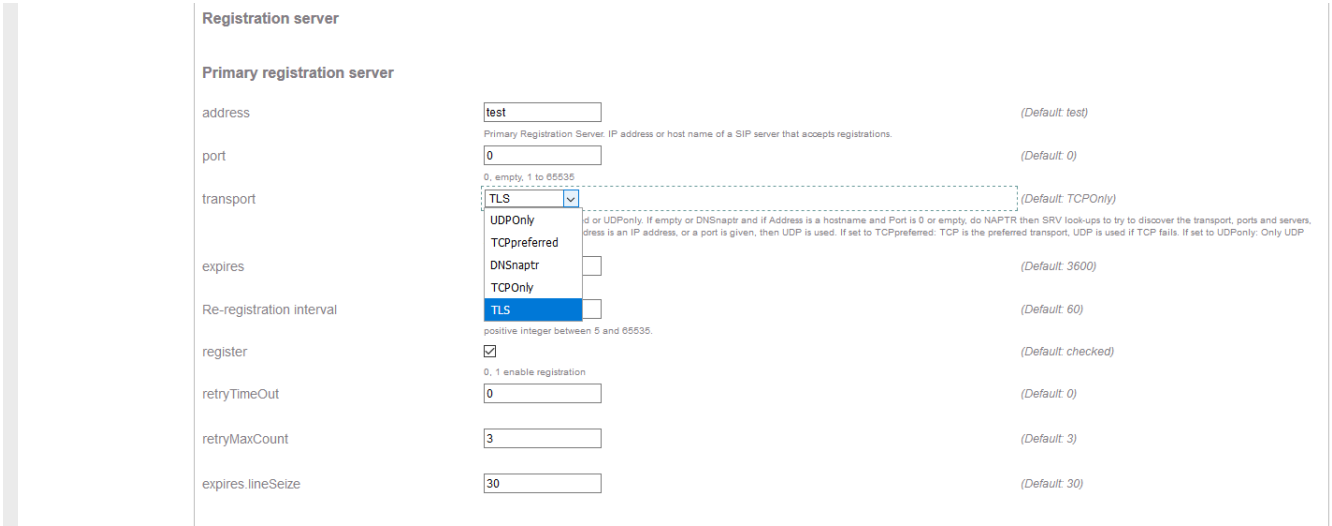
- TLS is the recommended security mechanism for Session Initiation Protocol (SIP).
- NAT traversal -- since IPSec is Layer 3 protocol NAT is not supported, while TLS works flawlessly
- HTTP Digest sessions in SIP environments are based on TLS.
- SIP clients implementations natively supports TLS
- Provides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

Disadvantages

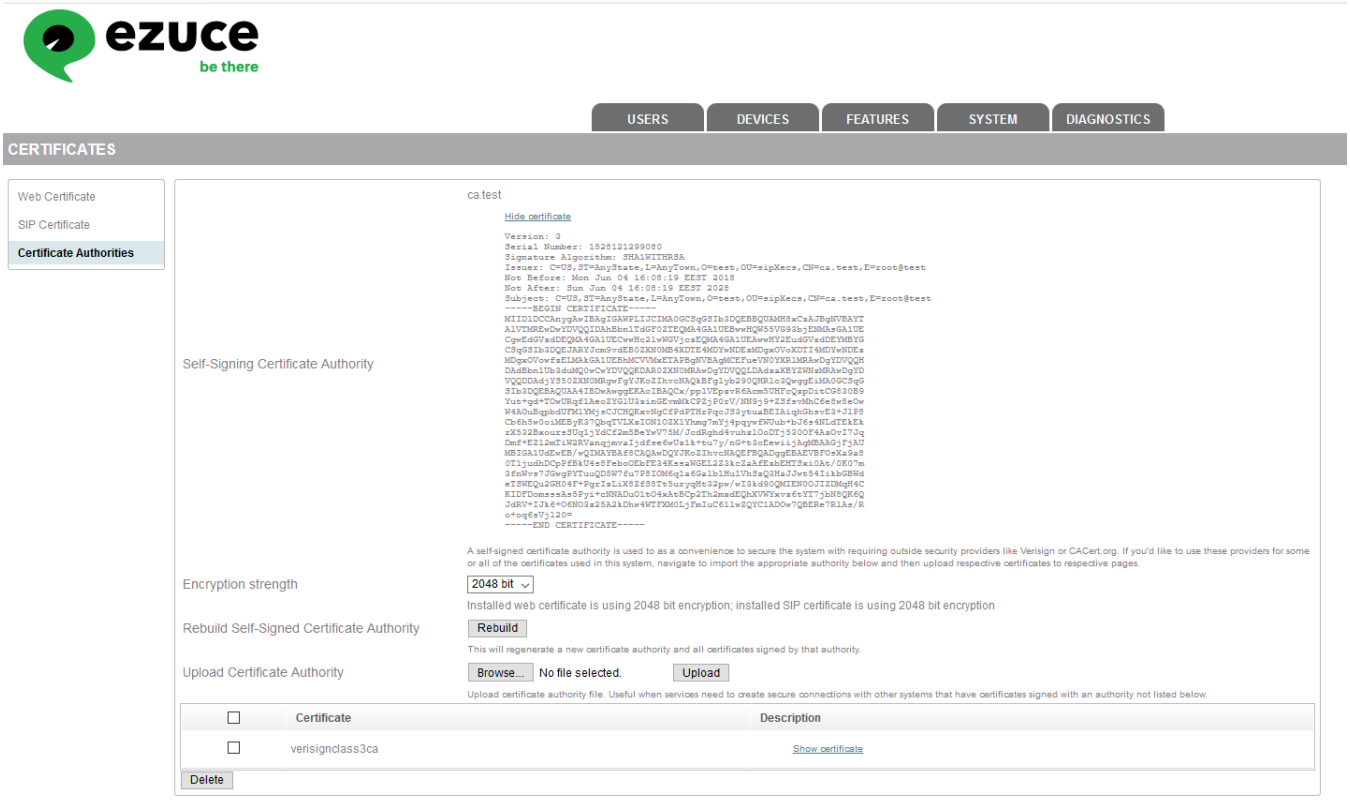
- Both of the TLS models require the server and client to support PKI features, such as certificate validation and certificate management. Not all clients and solutions support PKI. PKI is typically used in complex environments
- PKI is computationally expensive since it uses public key cryptography
- 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.

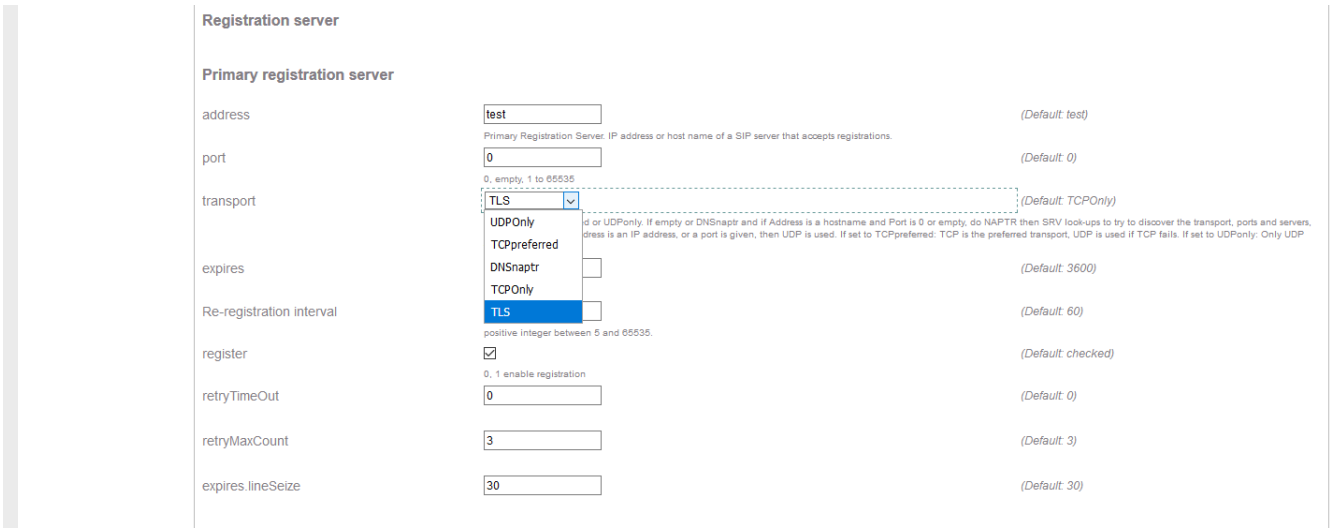
Deploying TLS for devices that can be provisioned by **uniteme**/sipxcom (like **Polycom** phone) is as easy as **just setting the transport to TLS** in Line->Registration.



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



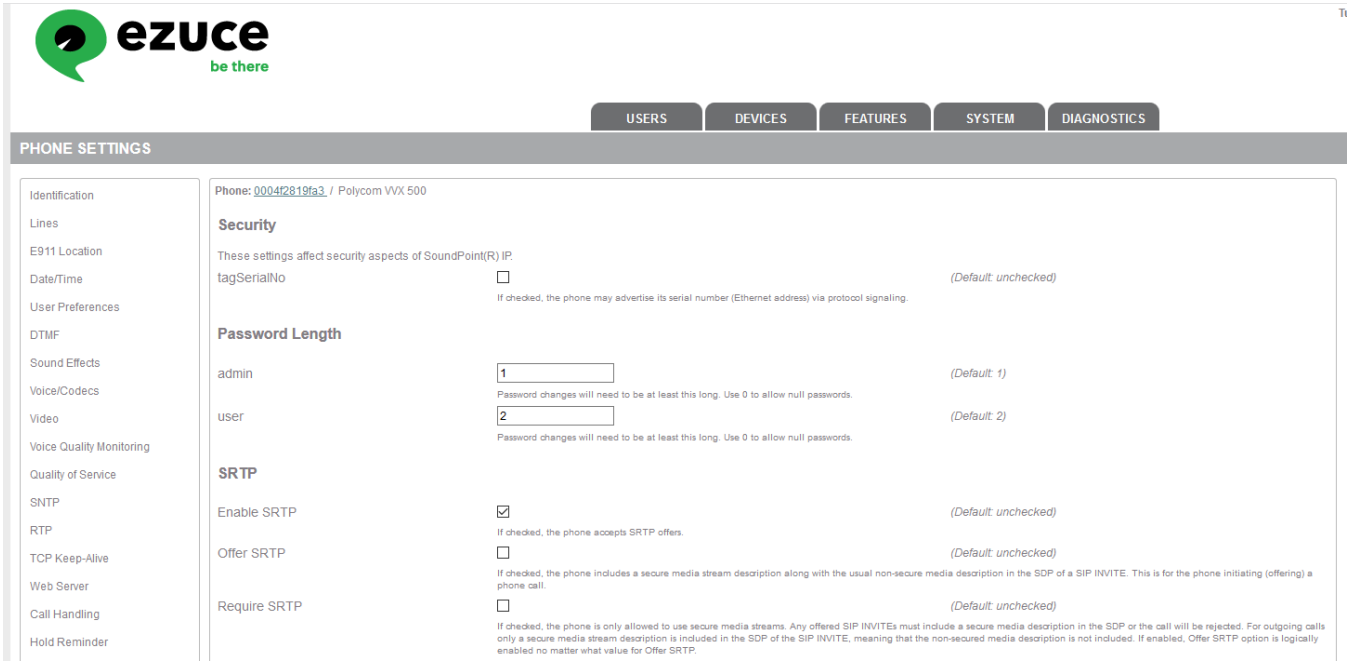
After importing Certificate Authority you will need to **set transport to TLS**.



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

Enabling SRTP

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



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