Resource - siptlsprofile

About this Resource

Defines a **TLS Profile Table** to be used in a SIP Signaling Group.

REST API Methods for this Resource

- GET siptlsprofile
- GET siptlsprofile id
- POST siptlsprofile id
- PUT siptlsprofile id
- DELETE siptlsprofile id

Resource Schema

Configuration

Parameter Name	Required	Service Affecting	Data Type	Default Value	Possible Values	Description
Description	No	No	string	none	64 - Max Length	Description of the profile
TLSVersion	Yes	Yes	Enum	2	Possible values: • 0 - e_tls1_2 • 1 - e_tls1_0 • 2 - e_tlsany	Defines TLS Protocol Version. By default system would accept all TLS protocol versions up to 1.2. SBC Edge Client would initiate highest supported version, which is TLS 1.2.
HandshakeTimeout	Yes	Yes	int	10	Possible values: • 1 - Minimum • 30 - Maximum	Specifies the SIP TLS client and server handshake inactivity timeout interval. The control timeout setting will abnormally terminate the TLS handshake session for a long period of inactivity between each TLS handshake message exchange. Recommended setting should be set to maximum 30 seconds due to network congestion.
MutualAuth	Yes	No	int	1	Possible values: • 0 - Minimum • 1 - Maximum	Specifies the authentication method option using the Mutual TLS in the SIP TLS server handshake exchange message. This enables the Mutual authentication request and verifications of the SIP peer client certificate.

VerifyPeersCertificate	Yes	No	int	1	Possible values: • 0 - Minimum • 1 - Maximum	Specifies the authentication method option of verifying the identity of the received SIP peer server certificate during the SIP TLS client handshake exchange message. This enables the verifications of the SIP peer server certificate.
ClientCipherSequence	Yes	No	string	6,5,7,4,3,1,0,2	32 - Max Length	Set of cipher suite(s) as comma seperated string in order of preference as security parameter negotiation with the remote system. Enumeration List: • **0 AES128-SHA** • **1 AES256-SHA** • **2 DES-CBC3-SHA** • **3 AES128-SHA256** • **4 AES256-SHA256** • **5 ECDHE-RSA-AES128-SHA256** • **6 ECDHE-RSA-AES256-SHA384** • **7 ECDHE-RSA-DES-CBC3-SHA**
ValidateClientFQDN	Yes	No	int	1	Possible values: • 0 - Minimum • 1 - Maximum	If enabled runs reverse DNS lookup to verify peer's FQDN.
ValidateServerFQDN	Yes	No	Enum	1	Possible values: • 0 - btFalse • 1 - btTrue	If enabled performs validation of configured SIP Server host FQDN with the verify peer's FQDN.
FallbackCompatibleMode	Yes	No	Enum	0	Possible values: • 0 - btFalse • 1 - btTrue	If enabled SSLv2 and SSLv3 variants to TLS1.0 will be negotiated when the compatibility with the peer is important.