

AudioCodes Quick Reference Guide Certificates

Background

When there is a need for additional security of the SIP traffic, the Transport Layer Security (TLS) is used to secure the device's SIP signaling connections. In TLS protocol, the data is encrypted and protected. TLS communication requires certificate to authenticate recipient of the secured data.

What are Certificates?

Certificates act as an identification of the device. It is a validation that the SIP traffic is going to a recognized and authenticated destination. The device inherits trust with the other proxy server with the use of certificates.

How does AudioCodes use Certificates?

AudioCodes uses certificates to deliver secured SIP traffic and services. In addition, certificates are used to provide security access to the device, Web (HTTPS) sessions, Telnet sessions and SSH sessions.

How do I load Certificates on the device?

The TLS Contexts Table is located under Setup \rightarrow IP Network \rightarrow Security \rightarrow TLS Contexts. There are links to Change Certificate and Trusted Root Certificates at the bottom.

ISContexes (f) OCSP Reveal 00 66/RPAL 66/RPAL 0CSP Security Security 0000 0059 Server 0csde VADIUS & LOAP 0115 Version A/P, including SSL3 Privary OCSP Server 0csde DIS Security 0115 Version A/L/DOH 0CSP Version 2000 V RDIUS & LOAP OCSP Version 0000 CSP Server - DIS Version A/L/DOH 0CSP Version 2000 Oper Clear Clear Control DEAL 0CSP Version 2000 Oper Clear Clear Clear Clear Clear Control DEAL 0CSP Version 2000 V RB SERVICES Distable Deale 0000 0000	ST SETUP MONITOR TROUBLESHOOT								🕂 Adr
Sk EtWORK VIEW ▲ CORE NUTINS Pitrefaces (0) Etherne Dowces (0) Physical Ports (0) Sace, Societ (1) • • • Maxis N Keensy (0) N Keensy (0) N Tarasiaon (0) • Concent (1) • • • Maxis • Concent (1) • • • • • • • • • • • • • • • • • • •	NETWORK SIGNALING&MEDIA ADMINISTRATION							Q Entity,	parameter, valu
CORE INTRIS Pherefaces (4) Enternet Conces (5) Enternet Conces (6) Enternet Conces (7) Physical Porus (8) Physical Porus (8) Physical Porus (1) • (7) HA Neasons (1) • (7) HA Neasons (1) • (7) Prewall (10) Security Serings J OLALITY Pachulas LDAP PANANCED Dis Dis Dis Dis Dis Mit Stancias Eterneton Value Ete	SRD All								
P Interfaces (4) Different Checkos (4) <th< td=""><td>A NETWORK VIEW</td><td>TLS Contexts (1)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>	A NETWORK VIEW	TLS Contexts (1)							
Initialization Initial Control of Con	▲ CORE ENTITIES								
Etherate Groups (B) 0 default Ary - Induding SSLo3 Ary ALLIDH Physical Ports (B) Sack Route (I) + Ary - Induding SSLo3 Ary ALLIDH Af Serings HAlt Heaving Monter (II) Friendel (II) Friendel (III) Friendel (IIII) Friendel (IIII) Friendel (IIII) Friendel (IIII) Friendel (IIII) Friendel (IIII) Friendel (IIIII) Friendel (IIIII) Friendel (IIIIIII) Friendel (IIIIIIIIII) Friendel (IIIIIIIIII) Friendel (IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	IP Interfaces (4)	+ New Edit 🗎		Page 1 of 1 💀 🗉 Show 10 🗸 records pe	r page				Q
Physical Process 01 Starts Routies (1) • All Ascentage MA Kenneys MA Ke		INDEX 🕆	NAME	TLS VERSION	DTLS VERSION		CIPHER SEF	RVER	
Sums Status Advention (in particular partiter partiter partiter particular particular partiter particular pa		0	default	Any - Including SSLv3	Any		ALL:ADH		
Aff Sensing 1 Sensing 1 At Transidon (0) Indexes (Atomic not (0)) A SECURITY Indexes (Atomic not (0)) In Sensing (1) Indexes (Atomic not (0)) V QUALITY CRERAL In Sensing (1) Atomic (1) In Sensing (1) Atomi									
At Translation (ii) Control Contro Contro Control Cont									
Scourse (1) Scourse (1) Scourse (3) Scourse (3) Scourse (3) Scourse (3) OUGUTY GERRAL Name • default Scourse (3) • default TS beside • default DS ADUARS & LADP Mark D ADVANCED Offs Forver D RS Scottary (2) Scottary (2) Scottary (2) Scotta	HA Network Monitor (0)								
I Scareas (I) Occase (I) Freedal (I) CAREBAL OCSP V UAUTY 0.55 Servir 0.55 Servir 0.55 Servir Name + default 0.55 Servir 0.55 Servir NAMA CED 015 Version + Ary-Incluing SSL03 Primary (CSP Servir) DTIS Version - Ary-Incluing SSL03 Primary (CSP Servir) - Concard (CSP Servir) DTIS Version - Ary-Incluing SSL03 Orsonary OCSP Servir) - Concard (CSP Servir) DTIS Version - Ary-Incluing SSL03 Orsonary OCSP Servir) - Concard (CSP Servir) DTIS Version - Ary-Incluing SSL03 Orsonary OCSP Servir) - Concard (CSP Servir) DTIS Version - Ary-Incluing SSL03 Orsonary OCSP Default Response - Seconary OCSP Default Response DTIS Version - Orsonary OCSP Default Response - Seconary OCSP Default Response - Seconary OCSP Default Response D Net SERVICES - Intel Start Seconary OCSP Default Response - Seconary OCSP Default Response - Seconary OCSP Default Response	NAT Translation (0)								
In Connect(1) CARRENC CCSP Freeding - CARRAN - CARRAN - CASP County Sentrys - CARRAN - CASP - Casada CARLING & - Connect Sentrys - CASP - Casada - Casada CARLING & - Connect Sentrys - Casada - Casada - Casada CARLING & - Connect Sentrys - Casada - Casada - Casada CARLING & - Connect Sentrys - Casada - Casada - Casada Carling - Carling - Carling - Carling - Casada - Casada - Casada - Casada Carling - Car	▲ SECURITY	#0[default]							Edit
Security Settings CREMIN CREMIN CREMIN VQUITY Name - doubt Off Server Name VQUITY Tailwain - kny-Including SSL3 Name Scotiage VQUITY Tailwain - kny-Including SSL3 Name Scotiage VQUITY Option - kny-Including SSL3 Scotiage - control VQUITY - kny-Including SSL3 - kny-Including SSL3 Scotiage - control VQUITY - kny-Including SSL3 - kny-Including SSL3 Scotiage - control VQUITY - kny-Including SSL3 - kny-Including SSL3 Scotiage - control VQUITY - kny-Including SSL3 - kny-Including SSL3 Scotiage - control VQUITY - kny-Including SSL3 - kny-Including SSL3 Scotiage - control VQUITY - kny-Including SSL3 - kny-Including Scotiage - control	TLS Contexts (1)								
Name ódialt OdS Server Isubia NGMUTY 15 Version 4/ny-Induity SSU3 Primury OSS Server - NGUIS LDAP MIT 4/ny-Induity SSU3 Primury OSS Server - NGUIS LDAP MIT 4/ny-Induity SSU3 Secondary OSS Server - NGUIS LDAP MIT 4/lunct 4/lunct OSP Portu - NGUIS SECONDER 05/HET 05/RECT 05/RECT 2/lunct -	Firewall (0)	CONTRAL			70				
Instruction Inst	Security Settings								
Displayse LDAP DTLS Version Any Secondary OSCP Server A DUVANCED Opter Server A LLADH OSCP Port 2800 A DUVANCED Opter Gerver A LLADH OSCP Port 2800 A DUVANCED Opter Gerver DEFLUT OSCP Default Response Reject A DUVANCED Secondary OSCP Server OscP Default Response Reject Default Response A DUVANCED Default Secondary Nalue OscP Default Response Reject Default Response Reject) QUALITY					Disable			
ADVANCED Opper Server + ALL/ADH OCSP Port 280 ADVANCED Opper Gent DERULT OCSP Default Response Reject Sind Certificate Extension Valu Disable Intervention Intervention VMB SERVICES Intervention Intervention Intervention									
ADVANCED Opper Client DEFAULT OCSP Default Response Reject ID NS SINC CettRicale Strension Value Disale Interview						2560			
) WEB SERVICES DH key Size 1024	> ADVANCED								
) WEB SERVICES	> DNS	Strict Certificate Extension Va	i Disable						
	h with strategy	DH key Size	1024						
	# WED SERVICES								
P HTP PROAT	HTTP PROXY								

INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED TO THE BEST OF AUDIOCODES KNOWLEDGE, AND AUDIOCODES SHALL NOT BE HELD LIABLE FOR ANY INACCURACIES.



Certificate Signing Request (CSR): On Change Certificate page, there is a section "Certificate Signing Request". Fill in the required fields according to your Certification Authority (CA) or security provider's instructions. Click Create CSR button. Copy this textual CSR and send to your CA to sign.

CERTI	FICATE SIGNING REQUEST					
	Subject Name [CN]					
	1st Subject Alternative Name [SAN]			EMAIL	~	
	2nd Subject Alternative Name [SAN]			EMAIL	\checkmark	
	3rd Subject Alternative Name [SAN]			EMAIL	\checkmark	
	4th Subject Alternative Name [SAN]			EMAIL	\checkmark	
	5th Subject Alternative Name [SAN]			EMAIL	\checkmark	
	Organizational Unit [OU] (optional)			Headquart	ers	
	Company name [O] <i>(optional)</i>			Corporate		
	Locality or city name [L] <i>(optional)</i>			Poughkeep	isie	
	State [ST] <i>(optional)</i>			New York		
	Country code [C] <i>(optional)</i>			US		
	Signature Algorithm			SHA-256		~
		Create CSR				
	After creating the CSR, copy the text below (including the $\ensuremath{BEGIN}\xspace{END}END$	send it to your Certification A	uthority for signi	ng.		
	BEGIN CERTIFICATE REQUEST BIGIN CERTIFICATE REQUEST BIGIN CERTIFICATE NVBACHDFWWWGAUCX/LHF1YXJ02XJ2HRIWEAYDVQCMD b3Jwb3JhdGUFTATENWIHIB1JANBQAUCAMSGVALHF1YXJ02XJ2HRIWEAYDV CHRWARDAUNAUTHIB1JANBQAUCAMSGVALHF1KUAGAGUCCAUTHW3IE NMCALK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD1V951NUCcuCjM/ARTL289CCG9T88 NGCAUK/LOH9UUGFBPESTPJ2YZBSUD12951NUCCUCJM/SSCB00392TL2MA21, SEPTINGG1YUL13f+NRMT1SGV4KG1XK1AG7EYCG1RKDk45SS6B00392TL2MA21, REDBESTV14TNN504107058G508LXK6GHDh137E55MDC0198CJPCKK21G4MH SEPTINGG1YUL174NCAUKJL289KHBV07KJL1W4/LE1j147L21j37E558C2913371 SepT234C357TEH452098kmBV785JUS5664b908g1Dn+f99TUCYR0V6FH47E2CU CGR19T291E6H/3jDEGT15C0+zv3kH4V2MBS34MMD0XFGD+u17F/SzV4nJ52j2 7E5MHdKa3JSSCFF	Flv JEA Jhs spc kuU SSG JFA J3X J20 J3X J20 J3W J60 Cb				

Device Certificate: On Change Certificate page, there is a section "Upload certificate files from your computer". For Server Certificate or Device Certificate provided by your CA, upload that certificate as a Device Certificate.

LOAD CERTIFICATE FILES FROM YOUR COMPUTER						
Private key pass-phrase (optional)		******				
	Send Private Key file from your computer to the device. The file must be in either PEM or PFX (PKCS#12) format.					
	Browse Load File					
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link. Send Device Certificate file from your computer to the device. The file must be in textual PEM format.						
	Browse Load File					

INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED TO THE BEST OF AUDIOCODES KNOWLEDGE, AND AUDIOCODES SHALL NOT BE HELD LIABLE FOR ANY INACCURACIES.



Trusted Root Certificate: On Trusted Root Certificates page, this is where you can upload Intermediate Certificate or Root Certificate.

★ TLS Context [#0] > Trusted Certificates			
View			Import Export Remove
INDEX 🔶 SUBJECT	ISSUER	EXPIRES	

What resources or guide do I use in loading certificates?

AudioCodes User's Manual also includes a detailed configuration guide of importing certificates including Private Key and Self Signed Certificates. Please refer to LTRT-27062 Mediant 1000B Gateway and E-SBC User's Manual Ver. 7.2 under Section 10 Configuring SSL/TLS Certificates. Any other Mediant device User's Manual Ver. 7.2 will also have a TLS Certificate Configuration section.

For any further questions regarding this topic or other technical topics:

- Contact your AudioCodes Sales Engineer
- Visit our AudioCodes Services and support page at https://www.audiocodes.com/services-support
- Access our technical documentation library at https://www.audiocodes.com/library/technical-documents
- Access to AudioCodes Management Utilities is available at https://services.audiocodes.com/app/answers/detail/a_id/20
- Contact Technical Support to submit a support ticket at https://services.audiocodes.com

INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED TO THE BEST OF AUDIOCODES KNOWLEDGE, AND AUDIOCODES SHALL NOT BE HELD LIABLE FOR ANY INACCURACIES.