AudioCodes Quick Reference Guide

Security Cipher Settings

Background

Security team often point to weak security ciphers as a critical issue when performing audits of network devices. This quick reference guide is aimed at helping you understand what issue is being raised and where to look for a solution.

What are Ciphers?

Ciphers are the algorithms by which data is encoded and decoded from a secure format.

How does AudioCodes Use Ciphers?

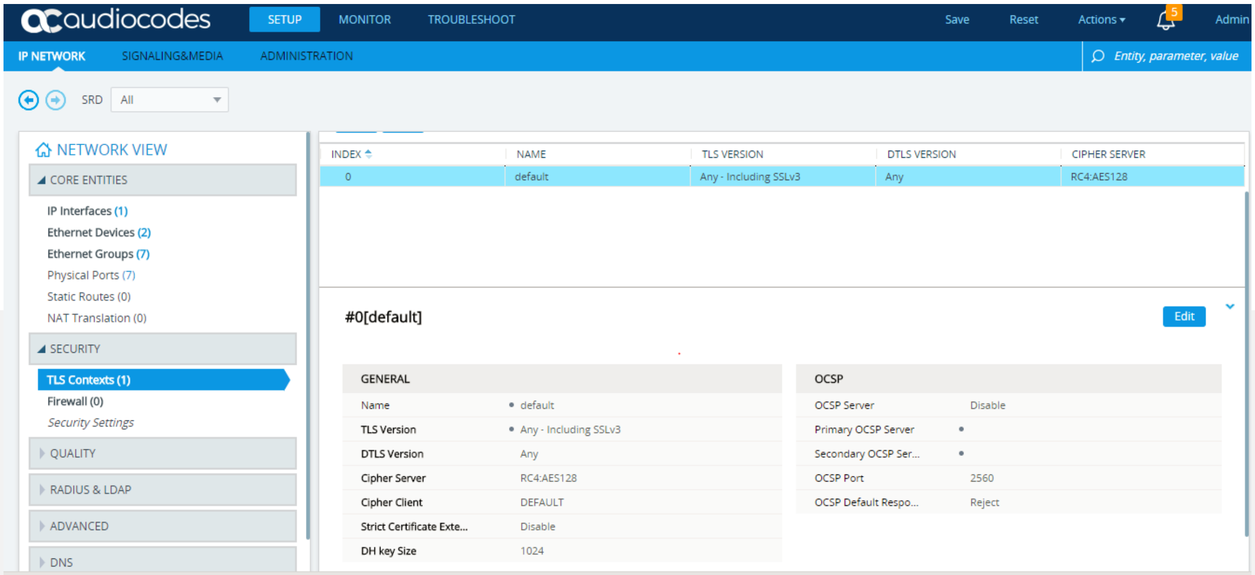
AudioCodes uses ciphers for the encryption and decryption of media, control, and management functionalities. This allows communications to be secured end to end.

Are some ciphers better than others?

Yes. As device processing power and memory increases over time, more complex ciphers are being developed in order to provide better security. The same processing advances that allow for better ciphers also reduce the effectiveness of older ciphers

How do I configure Ciphers on the device?

The TLS Contexts Table is located under Setup→IP Network→Security→TLS Contexts



INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	Any - Including SSLv3	Any	RC4:AES128

#0[default]

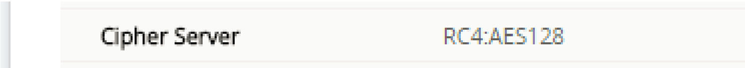
GENERAL	
Name	• default
TLS Version	• Any - Including SSLv3
DTLS Version	Any
Cipher Server	RC4:AES128
Cipher Client	DEFAULT
Strict Certificate Exte...	Disable
DH key Size	1024

OCSP	
OCSP Server	Disable
Primary OCSP Server	•
Secondary OCSP Ser...	•
OCSP Port	2560
OCSP Default Respo...	Reject

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

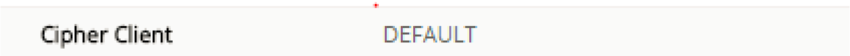
Under the Settings for the TLS contexts there is a Cipher Server and Cipher Client String location.

Cipher Server: This is the string used when the device is acting as the recipient of a connection request for TLS. A web browser requesting access to the AudioCodes device web GUI will send a Client Hello that contains a list of ciphers that must be in the Cipher Server suite to enable communication with the device web page.



Cipher Server RC4:AES128

Cipher Client: This is what the device will use when making an outgoing TLS/SSL request such as for secure SIP TLS connections to another device at a session initiation.



Cipher Client DEFAULT

What resources do I use to configure these strings?

http://www.openssl.org is a site that provides a toolkit for rolling out the ciphers and a list of acceptable ciphers.

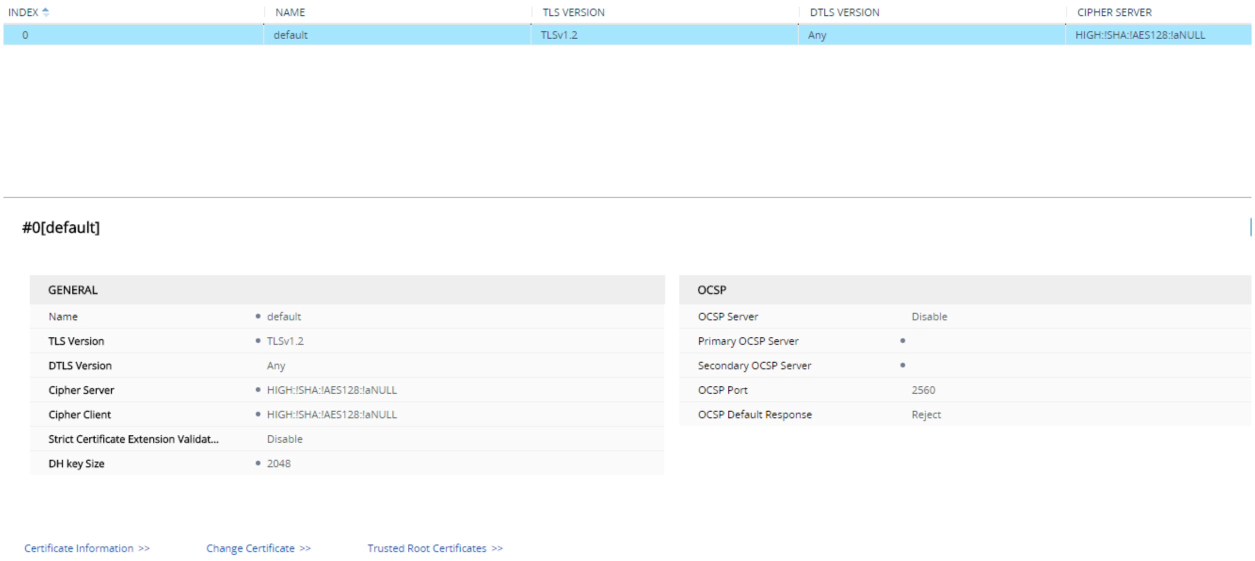
AudioCodes provides a document on Security Settings for our devices LTRT-30209-Recommended Security Guidelines Version 72.pdf. Your security team and IT team can also provide guidance on acceptable ciphers within the company. AudioCodes support will be happy to guide you with any questions on how to configure these ciphers for use.

Current Strong Cipher Settings: The current cipher settings that will pass stringent network security requirements are below.

TLS Version: 1.2

Client/Server Ciphers: HIGH:!SHA:!AES128:!aNULL

DH Key Size: 2048



INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.2	Any	HIGH:!SHA:!AES128:!aNULL

#0[default]

GENERAL	
Name	• default
TLS Version	• TLSv1.2
DTLS Version	Any
Cipher Server	• HIGH:!SHA:!AES128:!aNULL
Cipher Client	• HIGH:!SHA:!AES128:!aNULL
Strict Certificate Extension Validat...	Disable
DH key Size	• 2048

OCSP	
OCSP Server	Disable
Primary OCSP Server	•
Secondary OCSP Server	•
OCSP Port	2560
OCSP Default Response	Reject

Do I have to use these features?

Your device will be more secure with the use of features that encrypt and decrypt communication. Security is optional as some deployments have other means of securing the communication outside of the device.

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.