E-SBC Series

VoIP Gateway Series

MSBG Series

Transport Layer Security (TLS) Configuration Note

January 2012

Document # LTRT-31600

Table of Contents

List of Figures

List of Tables

Notice

This document describes configuration of Transport Layer Security (TLS) on AudioCodes Multi-Service Business Gateways.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: January-19-2012

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Note: In this guide, *device* refers to AudioCodes' Customer Premises Equipment (CPE).

Related Documentation

Document Name
AudioCodes' web site page on AudioCodes TLS Cipher-Suite Support: http://acportal/sites/SYSSW/System%20Software%20Public%20Library/TLS%20Cipher-suite%20support.mht
PowerPoint Presentation on Certificates and PKI Infrastructure on AudioCodes' web site page: http://acportal/sites/SYSSW/System%20Software%20Public%20Library/TLS%20Cipher-suite%20support.mht Click the link 'this presentation'
LTRT-52308 SIP CPE Product Reference Manual Ver. 6.4

1 Overview

AudioCodes devices support Transport Layer Security (TLS) protocol enabling client-server applications to communicate with one another secured against eavesdropping, tampering and message forgery. Applications include HTTPS, SIP, Automatic Update Facility and Telnet. The TLS feature supports 3 attributes:

Table 1-1: TSL Attributes

Attribute	Description
AES (Advanced Encryption Standard)	Uses a Key to encrypt plain text into cipher-text and the same Key to decrypt.
RSA	Enables an entity's identity to be authenticated before it is allowed to operate in your network.
SHA-1 (Secure Hash Algorithm -1)	Ensures integrity by sending a thumbprint from one entity to another.

1.1 AudioCodes Device Security Highlights

Security highlights are:

- Devices are shipped with a Self-Signed Certificate (RSA1024) which includes a Public Key and a Private Key burned in flash memory. TLS server mode requires it. TLS client mode does not require a certificate (default) unless the server requests two-way authentication.
- AudioCodes recommends that you install Certification Authority (CA) Signed device/client and root certificates on the device to join the device to Public Key Infrastructure (PKI).

Note:

- Joining an AudioCodes device to PKI is only possible if you have PKI.
- If you don't, you won't have a CA from whom to obtain Authority-Signed Certificates.
- PKI vendors such as VeriSign and Microsoft sell CA entities/services. AudioCodes does not.

- Customers can join a device to PKI

a. *without replacing* the Private Key (see Section 2.1 on page 9) (recommended)

-OR-

b. *by replacing* the Private Key (see Section 2.2 on page 11) (not recommended)

Note: For a recorded presentation on Certificates and PKI, go to AudioCodes web site page:

http://acportal/sites/SYSSW/System%20Software%20Public%20Library/TLS%20Cipher-suite%20support.mht

Click **this presentation** link.

Read these explanations of basic terms before proceeding:

Table 1-2: Explanations of Basic Terms

Term	Explanation
PKI	If you have Public Key Infrastructure you have a CA and each entity in your network can have two Authority-Signed Certificates installed on it: (1) a device certificate and (2) a trusted root certificate.
CA	Certification Authority whose server can be located externally (VeriSign, Microsoft, etc.) or internally (your IT department). The CA issues 2 Authority-Signed Certificates (1) a device certificate and (2) a trusted root certificate. These can be obtained from the CA and installed on the device.
Entity	An entity can be an AudioCodes device, a management station, a phone, etc., in the network.
Self-Signed Certificate	Burned in the flash memory of each shipped AudioCodes device. Includes a Public Key. Does not enable authentication.
Private Key	Burned in the flash memory of each shipped AudioCodes device. Decodes information encoded by the Public Key.
Public Key	Included in the Self-Signed Certificate and associated mathematically with the Private Key, it decodes information encoded by the Private Key.
Authority-Signed Certificate	Obtainable from a CA (VeriSign, Microsoft, etc.). The CA issues 2 Authority-Signed Certificates (1) a device certificate and (2) a trusted root certificate. Both must be installed on the device to join it to PKI.

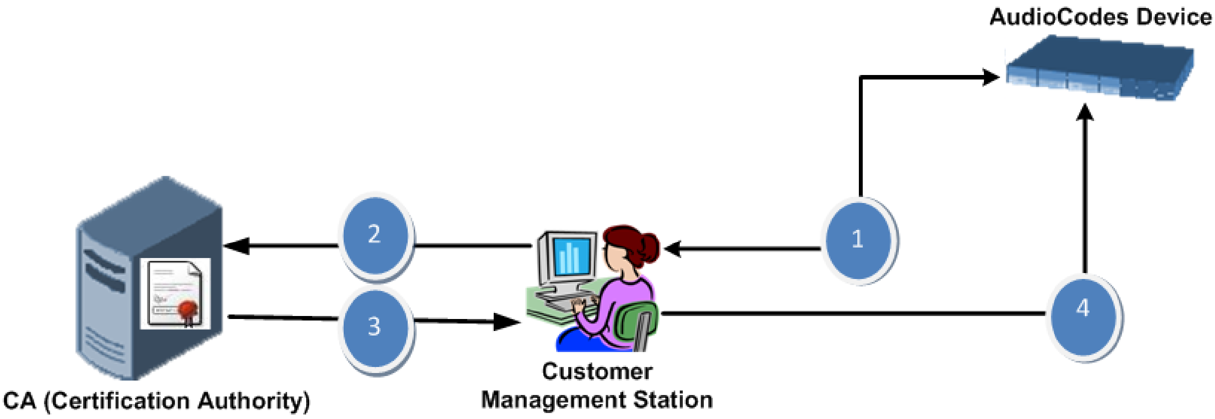
2 Joining an AudioCodes Device to PKI

2.1 Installing Authority Signed Certificates on the Device

Note:

- The recommended method of joining a device to PKI is to install Certification Authority (CA) signed device/client and root certificates on the device, leaving the device's default Private Key installed.
- This method is secure because no private data is transmitted over the network and there's less room for errors.
- If, however, replacing the Private Key is unavoidable, see Section 2.2 on page 11.

Figure 2-1: Installing Certification Authority Signed Certificates on a Device



Explanation

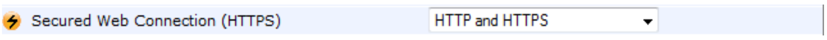
1	In your browser, access the device’s embedded Web server via the device's IP address and in the Web based management tool, generate a Certificate Signing Request (CSR).
2	Submit the CSR to your CA on the CA web site's certificates page.
3	From the CA web site's certificates page, download an Authority-Signed Device/Client Certificate file and an Authority-Signed Root Certificate file to your management station.
4	Save these on your management station and use the Web interface to upload them to the AudioCodes device.

Before joining the device to PKI, configure SIP, cipher-suites and NTP (see Section 3 on page 15).

➢ To join the device to PKI:

1. In your browser access the device’s embedded Web server via the device's IP address and in the Web based management tool that opens, navigate to the WEB Security Settings page (**Configuration** tab > **System** > **Management**).
2. Make sure the 'Secured Web Connection' field is set to **HTTP and HTTPS**.
   This setting will enable you to access the device if the new certificate won't work.

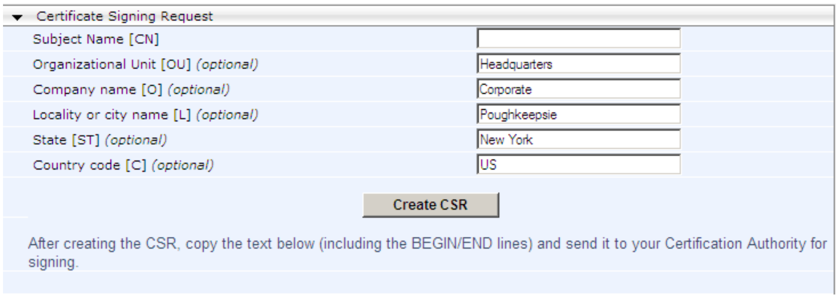
Figure 2-2: Secured Web Connection



Secured Web Connection (HTTPS) | HTTP and HTTPS

3. Open the Certificates page (**Configuration** tab > **System** > **Certificates**) and scroll down to 'Certificates Signing Request'.

Figure 2-3: Certificates Signing Request (CSR)



Certificate Signing Request

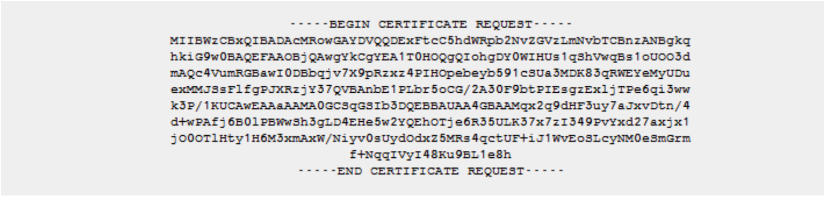
Subject Name [CN]	
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

4. In the 'Subject Name (CN)' field, enter a unique DNS name for the device, for example, "dns_name.corp.customer.com".

5. Click the **Create CSR** button; the CSR text is generated and displayed on the page.

Figure 2-4: CSR Text



```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWzCBxQIBADAcMRowGAYDVQQDExFtcC5hdWRpb2NvZGVzLmNvbTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA1T0HOQgQIohgDY0WIHUs1qShVwqBs1oUOO3d
mAQc4VumRGBawI0DBbqjv7X9pRzxz4PIHOpebeyb591cSUa3MDK83qRWEYeMyUDu
exMMJSsFlfgPJXRzjY37QVBAnbE1PLbr5oCG/2A30F9btPIEsgzExljTPe6qi3ww
k3P/1KUCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAAMqx2q9dHF3uy7aJxvDtn/4
d+wPAfj6B0lPBWwSh3gLD4EHe5w2YQEhOTje6R35ULK37x7zI349PvYxd27axjx1
jO0oTlHty1H6M3xmAxW/Niyv0sUydOdxZ5MRs4qctUF+iJ1WvEoSLcyNM0eSmGrm
f+NqqIVyI48Ku9BL1e8h
-----END CERTIFICATE REQUEST-----
```

6. Copy the CSR text from ----BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST----, paste it into Notepad (for example) and save it as a .txt file on your PC.

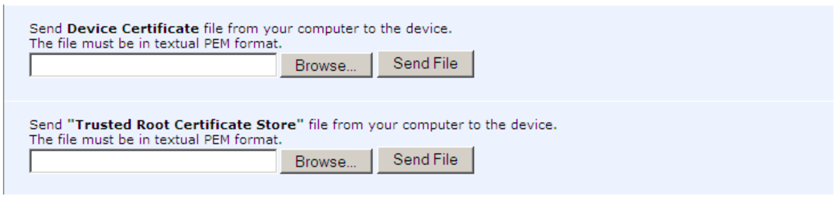
7. Open your CA web site's certificates page, access the screen in which to request a device/client certificate and submit the CSR text that you saved previously, selecting Base 64 encoding option and the textual PEM format option.

8. Download and save the CA signed device/client certificate file on your PC as device.cer (for example). This step differs slightly from one CA web site to another. See an example under Appendix A on page 19.

9. Access the root certificate download page and save the file as root.cer on your PC. The procedure differs from one CA web site to another; see Section A on page 19 for an example.

10. In the Web interface's Certificates page, scroll to 'Upload certificate files from your computer'.

Figure 2-5: Upload Certificate Files from your Computer



Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

Send **"Trusted Root Certificate Store"** file from your computer to the device.
The file must be in textual PEM format.

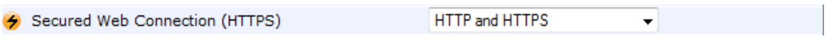
11. Click the **Browse** button under 'Send Device Certificate file from your computer to the device', navigate to the device.cer file, and click the **Send File** button; the CA-issued device/client certificate is installed on the device.

12. Click the **Browse** button under 'Send Trusted Root Certificate Store file from your computer to the device', navigate to the root.cer file, and click the **Send File** button; the CA root certificate is installed on the device.

13. Restart the device; the Web interface now uses the provided CA-issued certificates.

14. In the Web interface open the Certificates page and verify under 'Certificate information' that the status of the 'Private Key' parameter is 'OK', if it's not, consult your security administrator.
15. Open the WEB Security Settings page (**Configuration** tab > **System** > **Management**) and set the 'Secured Web Connection' field to **HTTP Only**.

Figure 2-6: Secured Web Connection



Secured Web Connection (HTTPS) HTTP and HTTPS

Note:

- The CA-issued root certificate can be replaced whenever necessary (for example, when it expires).
- It's possible to use the IP address of the device (e.g., 10.3.3.1) instead of a qualified DNS name in the Subject Name. This is not recommended since the IP address is subject to changes and may not uniquely identify the device.
- The CA-issued device certificate file can alternatively be loaded via the Automatic Update Facility using *ini* file parameter HTTPSCertFileName and the CA-issued root certificate using *ini* file parameter HTTPSRootFileName.

2.2 Replacing the Device's Private Key

AudioCodes devices are shipped with a Self-Signed Certificate that includes a Public Key and a Private Key burned in each device's flash memory.

Joining a device to PKI by replacing its Private Key is *not* recommended because the Private Key, by default installed on the shipped device, is secure, and replacing it is unnecessary.

However, replacing the Private Key may be unavoidable if you:

1. have PKI that doesn’t support CSR
2. have a central provisioning server on which to store all Private Keys
3. want to track the usage of Certificates / Private Keys
4. want to control Certificates / Private Keys replacements
5. are a government agency that wants to keep a copy of the device's Private Key on a third-party entity

Note:

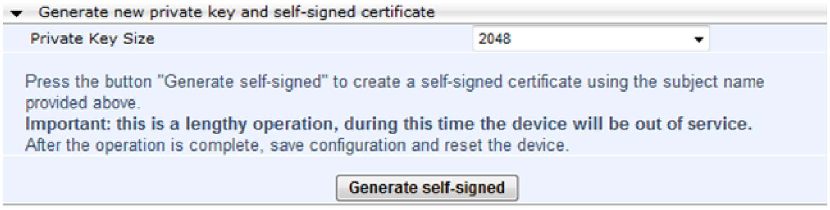
- Each device's Private Key is unique so after an RMA, for example, you cannot use the previous Private Key, you must obtain a new one for the new device received after the RMA.
- Take precautions to load the Private Key over a physically secure connection such as a back-to-back Ethernet cable connected directly to the management station.
- The recommended method of joining PKI is to leave the Private Key installed, to request an Authority-Signed Certificate from your CA via a CSR, and to install the CA- issued files on the device (see Section 2.1 on page 9).

The procedure below describes how to join a device to PKI by replacing its Private Key (not recommended).

➢ To replace a device's Private Key:

1. In the Web interface, open the Certificates page (**Configuration** tab > **System** > **Certificates**), and in the 'Subject Name (CN)' field, enter the fully-qualified DNS name (FQDN) as the Certificate subject (e.g., dns_name.corp.customer.com).
2. Scroll down to 'Generate new private key and self-signed certificate':

Figure 2-7: Generate New Private Key and Self-Signed Certificate



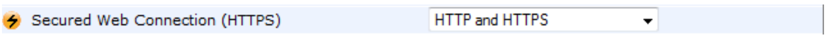
Generate new private key and self-signed certificate

Private Key Size: 2048

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
After the operation is complete, save configuration and reset the device.

3. Make sure that no traffic is running on the device. Generating a new Self-Signed Certificate disrupts traffic and should be done during maintenance time.
4. From the 'Private Key Size' drop-down list, select **2048** if your device is version 6.4. If it's pre 6.4, leave the default **1024**.
5. Click **Generate Self-signed**; wait until a message appears displaying the subject name of the new Self-Signed Certificate; you've successfully generated a new Self-Signed Certificate and changed the name of the default one ('ACL_nnnnnnn', where *nnnnnnn* is the device's serial number).
6. Save the configuration and restart the device for the new Self-Signed Certificate to take effect.
7. Obtain from your security administrator a Private Key in either textual PEM (PKCS #7) or PFX (PKCS #12) format. The file may be encrypted with a short pass-phrase, which should be provided by your security administrator.
8. Open the Web Admin Tool and in the WEB Security Settings page (**Configuration** tab > **System** > **Management**), make sure the 'Secured Web Connection' field is set to **HTTP and HTTPS**.

Figure 2-8: Secured Web Connection

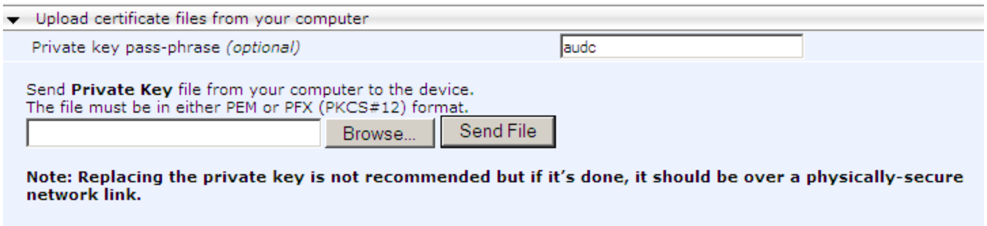


Secured Web Connection (HTTPS): HTTP and HTTPS

With this configuration, you'll be able to access the device if the new Certificate doesn't work. If the Certificate does work, configure the field to **HTTP Only** after testing.

9. In the Web interface, open the Certificates page and scroll down to the 'Upload certificate files from your computer' group.

Figure 2-9: Loading a Private Key to a Device



Upload certificate files from your computer

Private key pass-phrase *(optional)*: audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

10. Enter the 'Private key pass-phrase' field (optional).
11. Click the **Browse** button corresponding to 'Send Private Key', navigate to the private key file, and click **Send File**.
12. If the security administrator provided you with a Device Certificate file, load it now using the 'Send Device Certificate' button (see Figure 4-8 below).

13. After the files successfully load to the device, save the configuration and restart the device; the Web interface uses the new configuration.
14. In the Web interface open the Certificates page again and verify under 'Certificate information' that the status of the 'Private Key' parameter is 'OK', if it's not, consult your security administrator.
15. Open the WEB Security Settings page (**Configuration** tab > **System** > **Management**) and set the 'Secured Web Connection' field to **HTTP Only**.

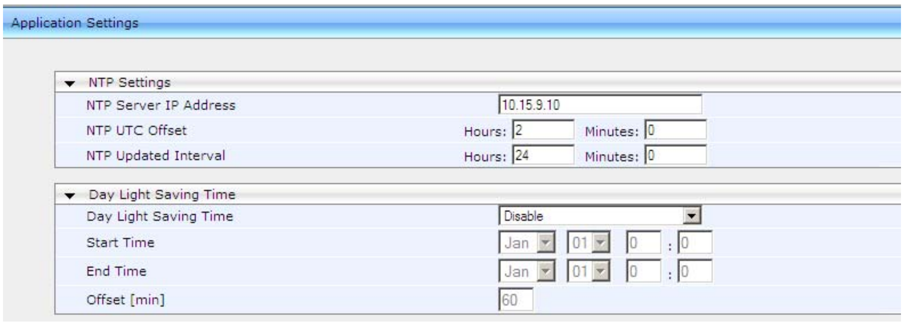
2.2.1 Configuring Network Time Protocol (NTP)

Without the correct date and time, **Self-Signed Certificates** cannot work. After receiving the AudioCodes device, you must configure it to use NTP to obtain the current date and time (since X.509 certificates have an expiration date and time).

➢ **To configure NTP:**

1. In the Web interface, open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).

Figure 2-10: Application Settings



Application Settings

NTP Settings

NTP Server IP Address: 10.15.9.10

NTP UTC Offset: Hours: 2 Minutes: 0

NTP Updated Interval: Hours: 24 Minutes: 0

Day Light Saving Time

Day Light Saving Time: Disable

Start Time: Jan 01 0 : 0

End Time: Jan 01 0 : 0

Offset [min]: 60

2. Configure NTP Settings using Table 2-1 as a reference.

Table 2-1: NTP Settings

Parameter	Description
NTP Server IP Address	Defines the IP address of the NTP server.
NTP UTC Offset	Defines the time offset in relation to the UTC. For example, if your region is 2 hours ahead of the UTC, enter "2".
NTP Updated Interval	Defines the period after which the date and time of the device is updated.

3. Configure daylight saving, if required, using Table 2-2 as a reference:

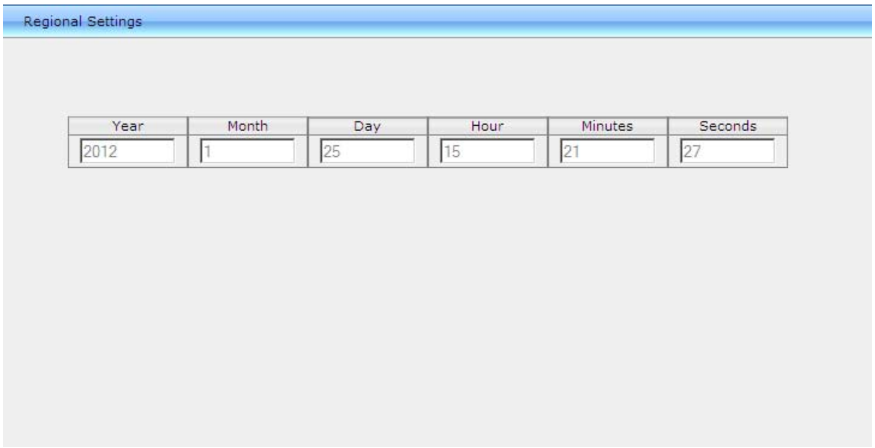
Table 2-2: Daylight Saving Time

Parameter	Description
Day Light Saving Time	Enables daylight saving time.
Start Time and End Time	Defines the period for which daylight saving time is relevant.
Offset	Defines the offset in minutes to add to the time for daylight saving. For example, if your region has daylight saving of one hour, the time received from the NTP server is 11:00, and the UTC offset for your region is +2 (i.e., 13:00), you need to enter "60" to change the local time to 14:00.

4. In the Regional Settings page, verify that the device is set to the correct date and time (**Configuration** tab > **System** menu > **Regional Settings**). If the device is configured

to obtain the date and time from an SNTP (Simple Network Time Protocol Support) server, the fields on this page display the received date and time as read-only.

Figure 2-11: Regional Settings



Regional Settings

Year	Month	Day	Hour	Minutes	Seconds
2012	1	25	15	21	27

3 Securing SIP Application Signaling

AudioCodes devices feature TLS to protect Session Initiation Protocol (SIP) application signaling. TLS provides authentication and encryption of the SIP signaling associated with VoIP and other SIP-based applications.

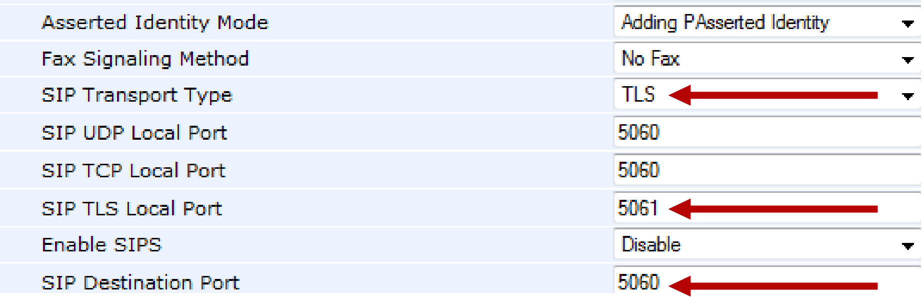
3.1 Configuring SIP Transport Type (TLS) and SIP TLS Local Port

The procedure below shows you how to protect SIP application signaling, by configuring SIP Transport Type (as TLS) and configuring the SIP TLS Local Port.

➢ **To configure SIP Transport Type and SIP TLS Local Port:**

1. Open the SIP General Parameters page.

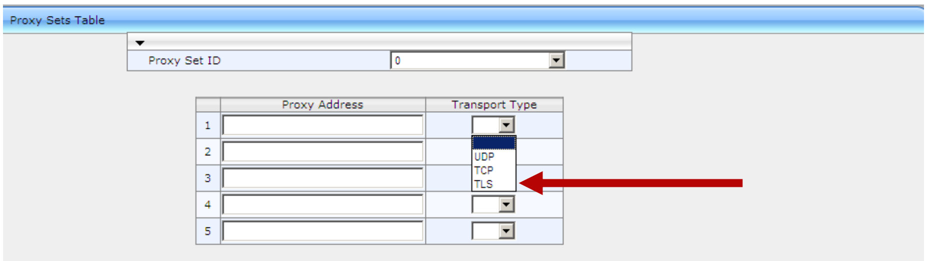
Figure 3-1: SIP Transport Type and SIP TLS Local Port



Asserted Identity Mode	Adding PAsserted Identity
Fax Signaling Method	No Fax
SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
SIP Destination Port	5060

2. From the ‘SIP Transport Type’ drop-down list, select **TLS**.
   This field can also be set *per destination* in the Web interface's:
   - Proxy Sets Table page (see Figure 3-2 below)
   - Tel to IP Routing page (see Figure 3-3 below)

Figure 3-2: Proxy Sets Table

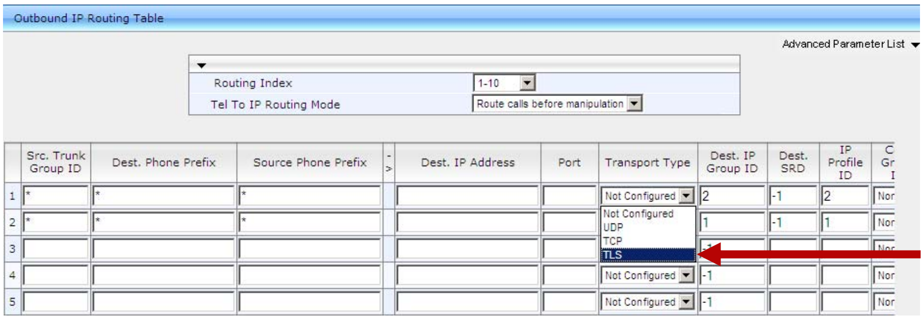


Proxy Sets Table

Proxy Set ID: 0

	Proxy Address	Transport Type
1		
2		
3		
4		
5		

Figure 3-3: Tel to IP Routing



Outbound IP Routing Table

Advanced Parameter List

Routing Index: 1-10

Tel To IP Routing Mode: Route calls before manipulation

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type	Dest. IP Group ID	Dest. SRD	IP Profile ID	C Gr I
1	*	*	*				Not Configured	2	-1	2	Nor
2	*	*	*					1	-1	1	Nor
3							TLS	-1			Nor
4							Not Configured	-1			Nor
5							Not Configured	-1			Nor

3. In the SIP General Parameters page enter the SIP TLS Local Port and the SIP Destination Port.
4. From the 'Enable SIPS' drop-down list, select **Enable**; TLS will be used through the entire connection, over multiple hops, if **TLS** was selected as 'SIP Transport Type',

though if **UDP** was selected as 'SIP Transport Type', the connection will fail. If you leave 'Enable SIPS' at **Disable** (default), TLS will be used for the next network hop only.

3.2 Configuring Two-Way Client-Server Authentication

By default, servers using TLS provide one-way authentication; the client is certain that the identity of the server is authentic.

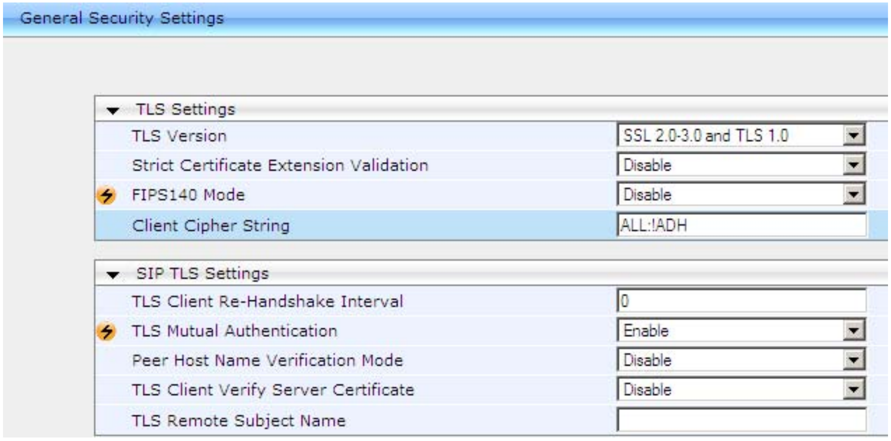
Note: Customers having PKI may want two-way (mutual) client-server authentication.

The procedure below shows how to configure two-way authentication.

➢ **To configure two-way authentication:**

1. In the Web interface, open the General Security Settings page (**Configuration** tab > **VoIP** > select **Full** > **Security** > General Security Settings) and in the 'TLS Mutual Authentication' drop-down list under SIP TLS Settings, choose **Enable**.

Figure 3-4: TLS Mutual Authentication



General Security Settings

TLS Settings

TLS Version	SSL 2.0-3.0 and TLS 1.0
Strict Certificate Extension Validation	Disable
FIPS140 Mode	Disable
Client Cipher String	ALL:!ADH

SIP TLS Settings

TLS Client Re-Handshake Interval	0
TLS Mutual Authentication	Enable
Peer Host Name Verification Mode	Disable
TLS Client Verify Server Certificate	Disable
TLS Remote Subject Name	

The 'TLS Mutual Authentication' field determines the device's behavior when acting as a server for TLS connections.

Table 3-1: TLS Mutual Authentication

Parameter	Description
Disable	(Default) The device does not request the client certificate.
Enable	The device requires receipt and verification of the client certificate to establish the TLS connection

2. For this parameter to take effect, a device reset is required.

Two-way client-server authentication can also be configured using the `SIPSRequireClientCertificate` *ini* file parameter.

4 Enabling Cipher-Suites

A cipher-suite is a predefined combination of algorithms that customers select to control the type of encryption performed.

Combinations are made up of a session key management algorithm used to exchange session keys (ADH, EDH, or RSA), an authentication algorithm used to verify the identity of the peer (RSA, DSA or none), a cipher algorithm used to encrypt data (RC4, AES, DES, 3DES, etc.), bit strength, i.e., key size used for encryption (56, 128, 256, etc.) and an integrity algorithm used to validate that the data is transmitted correctly (MD5 or SHA1).

Selection[1] depends on the PKI vendor and the type of PKI installed by the customer. Each PKI allows a specific algorithms combination.

➢ **To select a cipher-suite:**

1. Set the `HTTPSCipherString` *ini* file parameter. To see all possible values, see http://www.openssl.org/docs/apps/ciphers.html. By default, it's set to **EXP**, though if the 'Strong Encryption' Software Upgrade Key is enabled (depending on the customer's order), the default is **EXP:RC4** enabling RC4-128 bit.

Note: If the 'Strong Encryption' Software Upgrade Key feature is disabled, TLS is limited to the **EXP** cipher-suite, i.e., the only ciphers available will be RC4 and DES, and the cipher bit strength will be limited to 56 bits.

2. For additional cipher-suites, set this parameter to **ALL**.

[1] RSA keys are most popular though DSA keys are sometimes used by US government PKIs. Some security-sensitive customers won't use RSA for session key management since using the same RSA key for key transport and authentication is considered unsafe. These customers may require EDH, which is slower than RSA. Cipher selection usually impacts performance. AES and RC4 are fast algorithms compared to 3DES which is slow and may degrade device performance.

Reader's Notes

A Example of Joining a Device to PKI

This example shows you how to request a certificate from the Microsoft CA entity and install it on the AudioCodes device.

Follow this procedure:

1. Configure the Gateway Name (see Step 1)
2. Generate a CSR (see Step 2)
3. Get a Microsoft CA Certificate and a Trusted Root Certificate (see Step 3 on page 20)
4. Load the Certificates to the Device (see Step 4 on page 23)

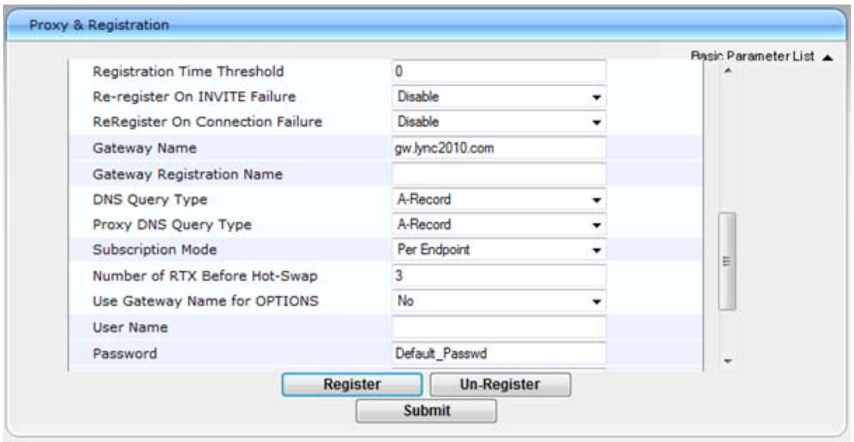
A.1 Step 1: Configure the Gateway Name

The procedure below describes how to configure the host name for the PSTN Gateway. This appears as the URI host name in the SIP From header in INVITE messages sent by the PSTN Gateway to the Mediation Server. This allows the Mediation Server to identify the PSTN Gateway (if required), when using certificates for TLS.

➢ To configure the SIP gateway name:

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** sub-menu > **Proxy & Registration**).

Figure 4-1: Proxy & Registration Page



Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	gw.lync2010.com
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Subscription Mode	Per Endpoint
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd

2. In the 'Gateway Name' field, assign a unique FQDN name to the PSTN Gateway within the domain, for example,"gw.lync2010.com". This name is identical to the name that is configured in the Lync Topology Builder.

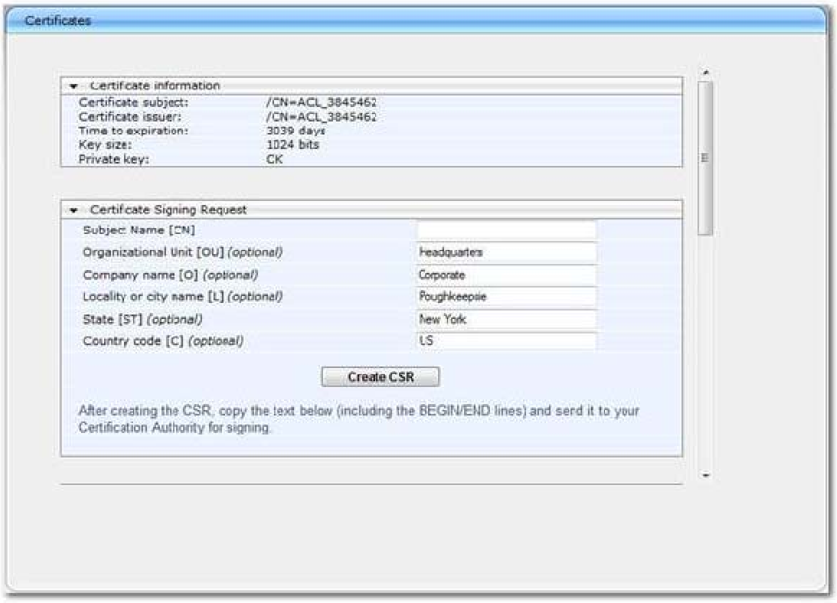
A.2 Step 2: Generate a CSR

The procedure below describes how to generate a CSR (Certificate Signing Request) by the PSTN Gateway. This CSR is later sent to Microsoft CA.

➢ To generate a CSR:

1. Open the Certificates Signing Request page (**Configuration** tab > **System** menu > **Certificates**).

Figure 4-2: Certificates Page



Certificates

Certificate information

Certificate subject: /CN=ACL_3845462
Certificate issuer: /CN=ACL_3845462
Time to expiration: 3039 days
Key size: 1024 bits
Private key: OK

Certificate Signing Request

Subject Name [CN]	
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

2. In the ‘Subject Name’ field, enter the SIP URI host name that you configured for the PSTN Gateway.
3. Click **Create CSR**; a Certificate request is generated and displayed on the page.
4. Copy the certificate from the line “----BEGIN CERTIFICATE” to “END CERTIFICATE REQUEST----” to a text file such as Notepad and then save it to a folder on your PC with the file name certreq.txt.

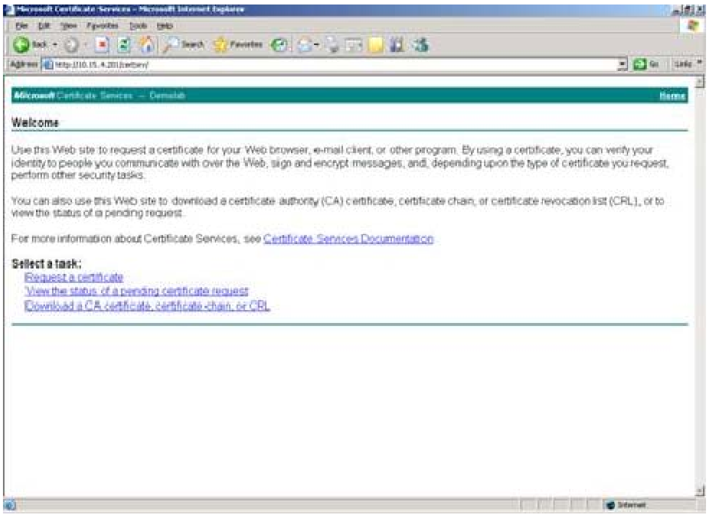
A.3 Step 3: Get a Microsoft CA Certificate and a Trusted Root Certificate

After generating the certreq.txt file, upload it to Microsoft Certificate server and request a CA certificate and a trusted root certificate.

➢ **To obtain a Microsoft CA certificate and a trusted root certificate:**

1. Open a Web browser and navigate to Microsoft Certificate Services at **http://< certificate server address >/certsrv**.

Figure 4-3: Microsoft Certificate Services Web Page



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/
Go Links

Microsoft Certificate Services -- Demolab Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

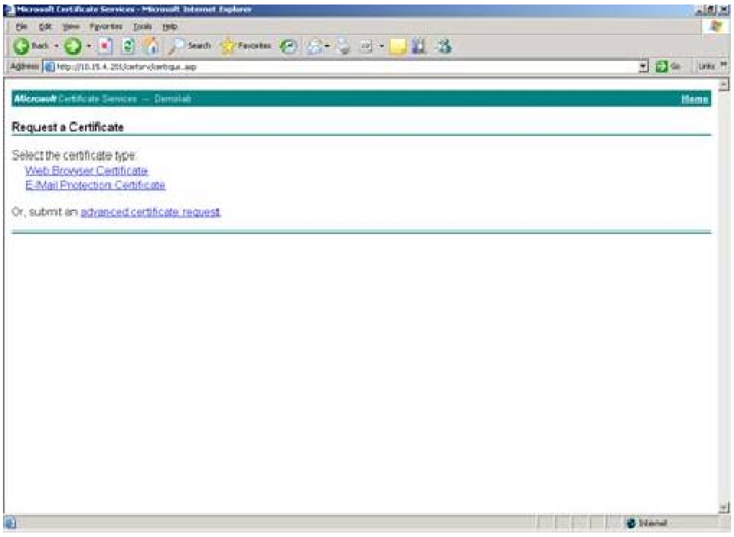
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. Click the **Request a certificate** link.

Figure 4-4: Request a Certificate Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/certrqus.asp
Go Links
Microsoft Certificate Services -- Demolab
Home
Internet

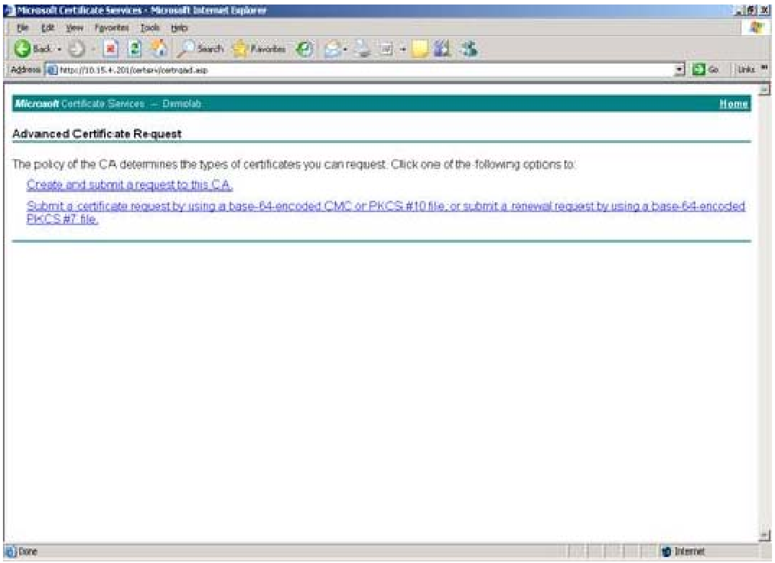
Request a Certificate

Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an advanced certificate request.

3. Click the **advanced certificate request** link.

Figure 4-5: Advanced Certificate Request Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/certrqad.asp
Go Links
Microsoft Certificate Services -- Demolab
Home
Done
Internet

Advanced Certificate Request

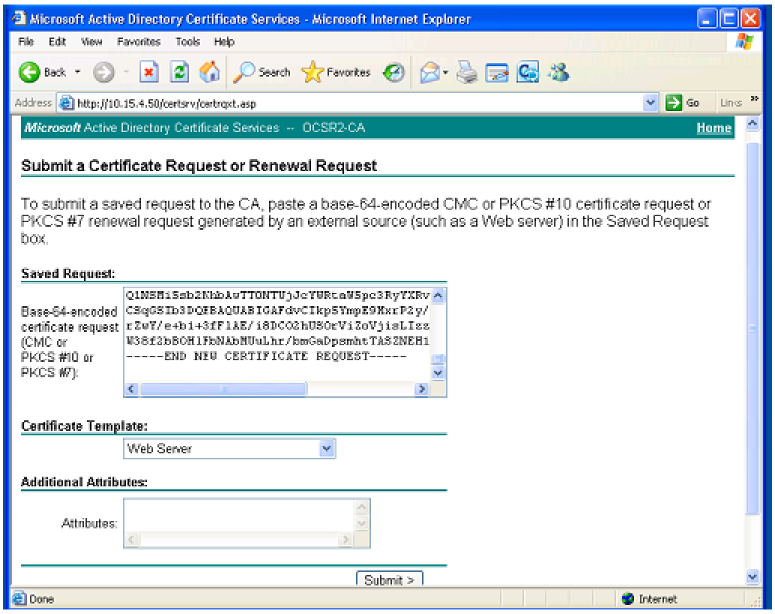
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

4. Click the **Submit a Certificate request by using base-64-encoded...** link.

Figure 4-6: Submit a Certificate Request or Renewal Request Page



Microsoft Active Directory Certificate Services - Microsoft Internet Explorer

Address: http://10.15.4.50/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services -- OCSR2-CA | Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
Q1NSM1Smb2NhbAwTTONTUjJcYURtaW5pc3RyYXRv
CSqGSIb3DQEBAQUABIGAFdvCIkp5YmpE9MxrP2y/
rZwT/e+b1+3fF1AE/i8DCO2hUSOrViZoVjisLIzz
W38f2bBOH1FbNAbMUuLhr/bmGaDpsmhtTAS2NEH1
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template: Web Server

Additional Attributes:

Attributes:

Submit >

Done | Internet

<ol start="5">
</ol>

5. Open the certreq.txt file that you created and saved previously and copy its contents into the **Saved Request** pane.

6. From the 'Certificate Template' drop-down list, select **Web Server**.

7. Click **Submit**.

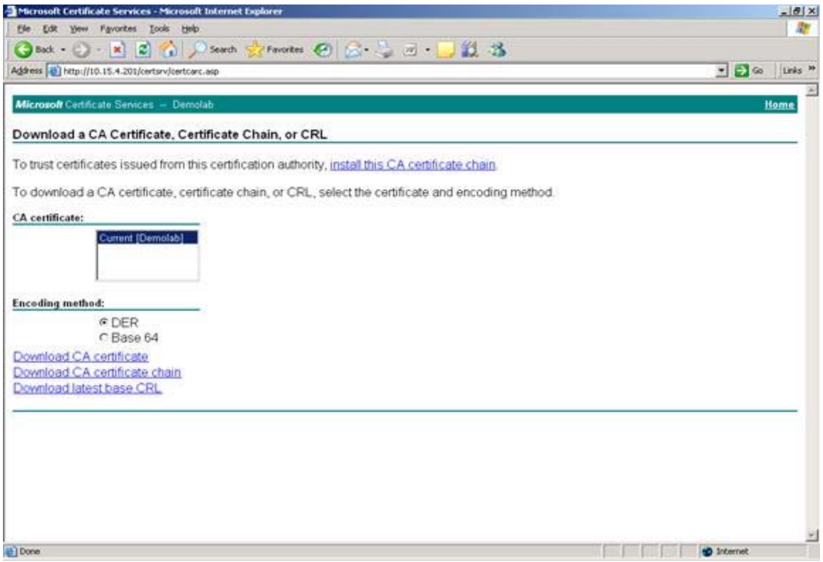
8. Select the **Base 64** encoding option.

9. Click the **Download CA certificate** link and save the file with the name gateway.cer on your PC.

10. Navigate again to the Microsoft Certificate Services page at **http://< certificate server address >/certsrv**.

11. Click the **Download a CA certificate**, **certificate chain or CRL** link.

Figure 4-7: Download a CA Certificate, Certificate Chain, or CRL Page



Microsoft Certificate Services - Microsoft Internet Explorer

Address: http://10.15.4.201/certsrv/certcarc.asp

Microsoft Certificate Services -- Demolab | Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate: Current [Demolab]

Encoding method:

● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL

Done | Internet

12. Under **Encoding method**, select the **Base 64** option.

13. Click the **Download CA certificate** link, and save the file with the name certroot.cer on your PC.

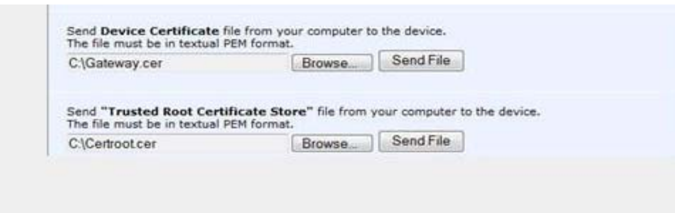
A.4 Step 4: Load the Two Certificates to the Device

After obtaining the CA and trusted root certificates from Microsoft, load these two certificates to the device.

➢ **To load the 2 certificates to the device:**

1. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**) and scroll to 'Upload certificate files from your computer'.

Figure 4-8: Certificates Page



Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.
C:\Gateway.cer

Send **"Trusted Root Certificate Store"** file from your computer to the device.
The file must be in textual PEM format.
C:\Certroot.cer

2. Adjacent to the 'Device Certificate' field click **Browse**, select the gateway.cer file that you saved on your PC and click **Send File**.
3. Adjacent to the 'Trusted Root Certificate Store' field click **Browse**, select the certroot.cer file that you saved on your PC and click **Send File**.
4. On the toolbar, click **Burn** to save the certificates to the device; the device resets, saving the settings to flash memory.

Transport Layer Security (TLS) Configuration Note

www.audiocodes.com