

Configuring Certificates

For AudioCodes MediaPack™ Series

This document describes how to configure certificates on the AudioCodes MediaPack Series VoIP Analog Gateways to enable secured management (HTTPS).

The procedure below describes how to exchange a certificate with the AudioCodes Certificate Authority (CA). The certificate is used by the MediaPack device to authenticate the connection in secured mode using HTTPS.

The procedure involves the following main steps:

1. Generating a Certificate Signing Request (CSR)
2. Requesting to sign Device Certificate by AudioCodes CA
3. Obtaining Trusted Root Certificate from AudioCodes CA
4. Deploying Device and Trusted Root Certificates on the MediaPack

To configure a certificate on MP-1xx devices:

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

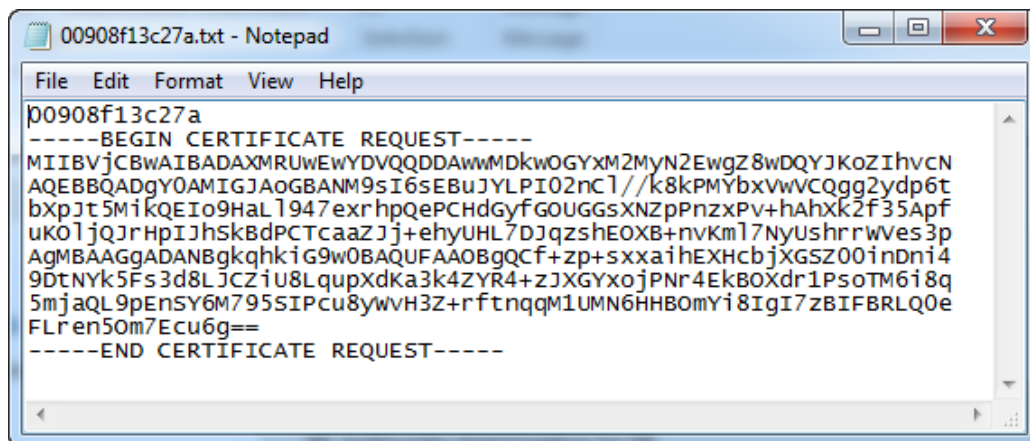
Figure 1: Certificates Page - Creating CSR

Certificate Signing Request	
Subject Name [CN]	00908f13c27a
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
<input type="button" value="Create CSR"/>	
<p>After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.</p> <pre>-----BEGIN CERTIFICATE REQUEST----- MIIBVjCBwAIBADAXMRUwEwYDVQQDDAwMDkwoGYYxM2MyN2EwZ8wDQYJKoZIhvcN AQEBAQADGy0AMIGJAoGBANM9sI6sEBuJYLPi02nCl//k8kPMYbxVwVCQgg2ydp6t bXpJtSMikQEIo9HaL1947exrhpQePCHdGyfgOUGGSXNZpPnzxPv+hAhXk2f35Apf uK01jQ3rHpI3hSkBdPCTcaaZj+ehyUHL7D3qzshEOXB+nvKmL7NyUshrrwVes3p AgMBAAGGADANBgkqhkiG9w0BAQUFAAOBgQCf+zp+sxai1hEXHcbjXGSZ00inDn14 9DtNYkSfS3d8LJCZiU8Lqpxdka3k4ZYR4+zJXGYxoJPnr4EkB0Xdr1PsoTM618q 5mjaQL9pEnSY6M795SIPcu8yVwH3Z+rftnqqM1UMN6HHB0mYi8IgI7zBIFBRLQ0e FLren50m7Ecu6g== -----END CERTIFICATE REQUEST-----</pre>	

2. In the 'Subject Name' field, enter the MediaPack's MAC address (e.g., **00908f13c27a**).
3. Click **Create CSR**; a certificate request is generated.

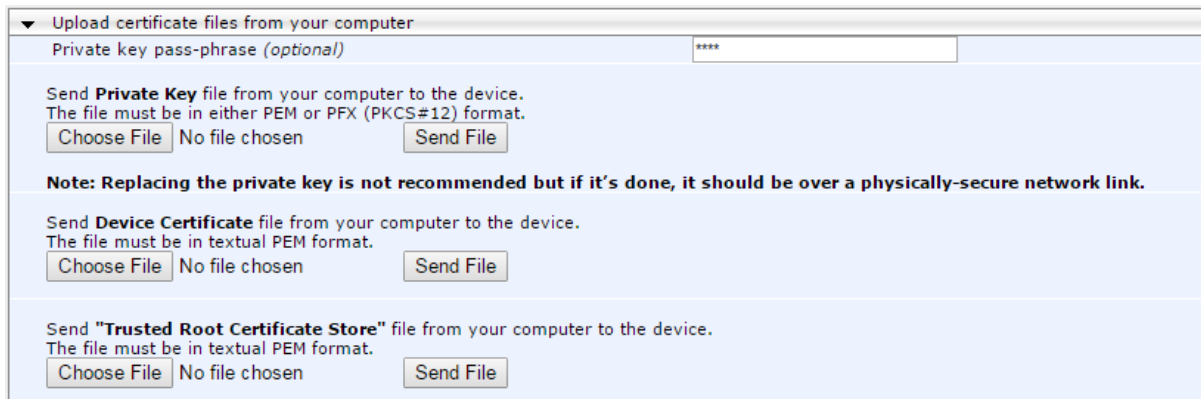
4. Copy the CSR from the line "**-----BEGIN CERTIFICATE REQUEST-----**" to "**-----END CERTIFICATE REQUEST-----**" to a text file (such as Notepad).
5. Enter the MediaPack's MAC address on the first line of the text file and then save the file to a folder on your computer with the file name <MediaPack MAC>.txt (e.g., *00908f13c27a.txt*).

Figure 2: Certificate Request (CSR) Text File



6. Send the saved CSR (*00908f13c27a.txt* file) to the AudioCodes Certificate Authority (CA) Administrator for signing.
7. You will receive a zip file from the AudioCodes Certificate Authority Administrator, containing two files: the signed certificate (in our example, *00908f13c27a.crt*) and the root certificate (*trust.pem*). Save these files to a folder on your computer.
8. In the MediaPack's Web interface, return to the Certificates page (see Step 1), scroll down to the 'Upload certificate files from your computer' group, and then do the following:
 - a. In the 'Send Device Certificate file...' field, click **Choose File**, and then select the *00908f13c27a.crt* certificate file that you saved on your computer in Step 7.
 - b. Click **Send File** to upload the certificate to the MediaPack.
 - c. Confirm that the file was successfully loaded to the device.
 - d. In the 'Send Trusted Root Certificate Store file...' field, click **Choose File**, and then select the *trust.pem* certificate file that you saved on your computer in Step 7.
 - e. Click **Send File** to upload the certificate to the MediaPack.
 - f. Confirm that the file was successfully loaded to the device.

Figure 3: Certificates Page (Uploading Certificate)



▼ Upload 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.

No file chosen

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.

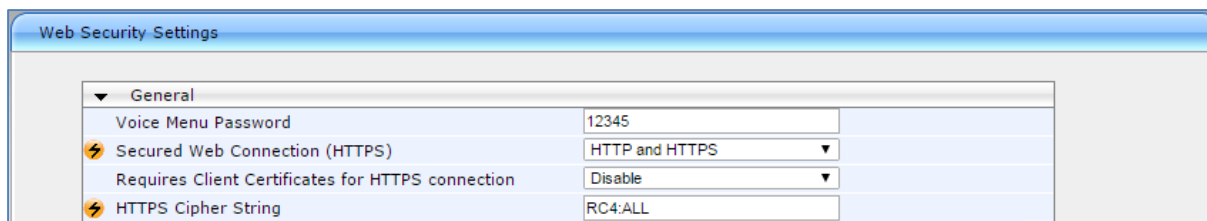
No file chosen

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

No file chosen

9. To avoid connectivity issues of the different browsers, it is recommended to change the default value of the 'HTTPS Cipher String' parameter to **RC4:ALL**:
 - a. Open the Web Security Settings page (**Configuration** tab > **System** > **Management** > **WEB Security Settings**).
 - b. Change the value of the 'HTTPS Cipher String' parameter to **RC4:ALL**.

Figure 4: HTTPS Cipher String



Web Security Settings

▼ General

Voice Menu Password	<input type="text" value="12345"/>
Secured Web Connection (HTTPS)	<input type="text" value="HTTP and HTTPS"/>
Requires Client Certificates for HTTPS connection	<input type="text" value="Disable"/>
HTTPS Cipher String	<input type="text" value="RC4:ALL"/>

10. Reset the MediaPack device with a burn to flash for your settings to take effect.

To verify that an MP-1xx device has the correct signed certificate:

1. Open the Certificates page (**Configuration** tab > **System** > **Certificates**).
2. In the 'Certificate information' group, check that the certificate values are correct:
 - 'Certificate subject' should be equal to the device's MAC address only
 - 'Certificate issuer' should be different than the Certificate subject
 - 'Time to expiration' and 'Key size' values are per requirements
 - 'Private key' status value is **OK**

Figure 5: Certificates Page – Example of the Correct Signed Certificate Information

Certificates	
▼ Certificate information	
Certificate subject:	/O=ACL/CN=00908f13c27a
Certificate issuer:	/O=ACL/CN=CA_1B
Time to expiration:	7259 days
Key size:	1024 bits
Private key:	OK

If the values of the Certificate subject and Certificate issuer are identical and the format is ACL_<Serial Number> (which indicates that the device is loaded with the default, self-signed certificate), the device does **not** include a signed certificate by AudioCodes.

Figure 6: Certificates Page – Example of the Default Certificate Information

Certificates	
▼ Certificate information	
Certificate subject:	/CN=ACL_1294970
Certificate issuer:	/CN=ACL_1294970
Time to expiration:	4737 days
Key size:	1024 bits
Private key:	OK

To configure a certificate on **MP-1288** devices:

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. On the TLS Contexts page, select the default TLS Context index (0) row, and click the **Change Certificate** link located below the table; the Context Certificates page appears.

Figure 7: Certificates Page - Creating CSR

CERTIFICATE SIGNING REQUEST

Common Name [CN]	<input type="text" value="00908f8bd529"/>
Organizational Unit [OU] <i>(optional)</i>	<input type="text"/>
Company name [O] <i>(optional)</i>	<input type="text"/>
Locality or city name [L] <i>(optional)</i>	<input type="text"/>
State [ST] <i>(optional)</i>	<input type="text"/>
Country code [C] <i>(optional)</i>	<input type="text"/>
1st Subject Alternative Name [SAN]	EMAIL <input type="text"/>
2nd Subject Alternative Name [SAN]	EMAIL <input type="text"/>
3rd Subject Alternative Name [SAN]	EMAIL <input type="text"/>
4th Subject Alternative Name [SAN]	EMAIL <input type="text"/>
5th Subject Alternative Name [SAN]	EMAIL <input type="text"/>
Signature Algorithm	SHA-256 <input type="button" value="v"/>

Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
Note that the certificate will use the subject name configured in "Certificate Signing Request" box.

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

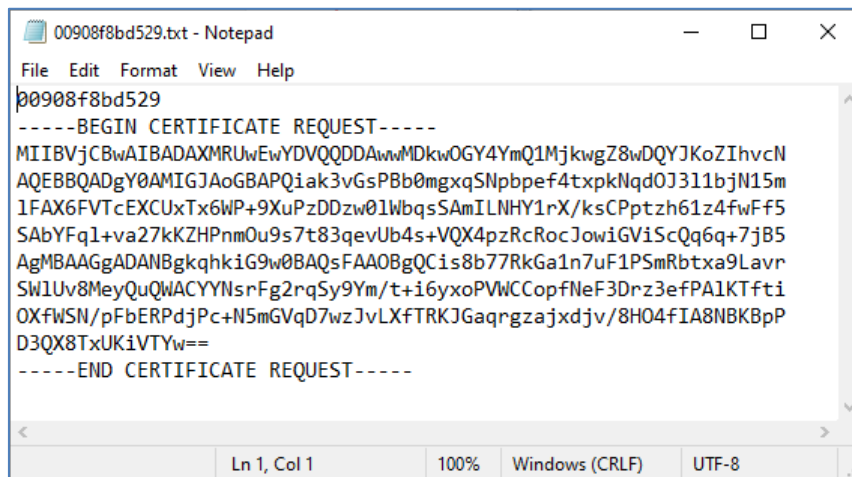
```

-----BEGIN CERTIFICATE REQUEST-----
MIIBVjCBwAIBADAXMRUwEwYDQDDAwMDKwOGY4YmQ1MjkwZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPQia3vGsPBb0mgxqSNpbpef4txpkNqd0J311bJN15m
1FAX6FVTcEXCUXtX6WP+9XuPzDDzw01WbqsSAmILNHY1rX/ksCPptzh61z4fwFf5
SABYFq1+va27kKZHPnmOu9s7t83qevUb4s+VQX4pzRcRocJowiGV1ScQq6q+7jB5
AgMBAAGgADANBgkqhkiG9w0BAQsFAAQBgQCiS8b77RkGa1n7uF1P5mRbtxa9Lavr
SW1Uv8MeyQuQwACYYNsrFg2rq5y9Ym/t+i6yxopVWCCopfNeF3Drz3efPA1KTfti
OXfW5N/pFbERPdjPc+N5mGVqD7wzJvLXFTRKJGaqrgzajxdjv/8H04fIA8NBKBP
D3QX8TxUKiVTYw==
-----END CERTIFICATE REQUEST-----

```

3. In the 'Common Name' field, enter the MP-1288's MAC address (e.g., **00908f8bd529**).
4. Click **Create CSR**; a certificate request is generated.
5. Copy the CSR text (from "**-----BEGIN CERTIFICATE**" to "**-----END CERTIFICATE REQUEST--**" to a text file (such as Notepad).
6. Enter the MP-1288's MAC address on the first line of the text file, and then save the file to a folder on your computer with the file name <MediaPack MAC>.txt (e.g., **00908f8bd529.txt**).

Figure 8: Certificate Request (CSR) Text File



7. Send the saved CSR (*00908f8bd529.txt* file) to the AudioCodes Certificate Authority (CA) Administrator for signing.

You will receive a zip file from the AudioCodes Certificate Authority Administrator, containing two files: the signed certificate (in our example, *00908f8bd529.crt*) and the root certificate (*trust.pem*).

8. Unzip and save the two files to a folder on your computer.
9. On the MP-1288's Web interface, return to the **TLS Contexts** page (see Step 1) and do the following:
 - a. In the TLS Contexts page, select the default TLS Context index (0) row and click the **Change Certificate** link located below the table; the Context Certificates page appears.
 - b. Scroll down to the Upload certificates files from your computer group.
 - c. Click the **Choose File** button corresponding to the '**Send Device Certificate...**' field.
 - d. Navigate to the certificate file obtained from the CA (in our example, *00908f8bd529.crt*) and saved on your computer in Step 8 and click **Load File** to upload the certificate to the MP-1288 device.

Figure 9: Uploading the Certificate Obtained from the Certification Authority

UPLOAD 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.

Choose File
No file chosen
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.

Choose File
No file chosen
Load File



10. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
11. On the MP-1288's Web interface, return to the **TLS Contexts** page.
 - a. On the TLS Contexts page, select the default TLS Context index (0) row, and click the Trusted Root **Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
 - b. Click the **Import** button, and then select the *trust.pem* certificate file saved on your computer in Step 8.
12. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:

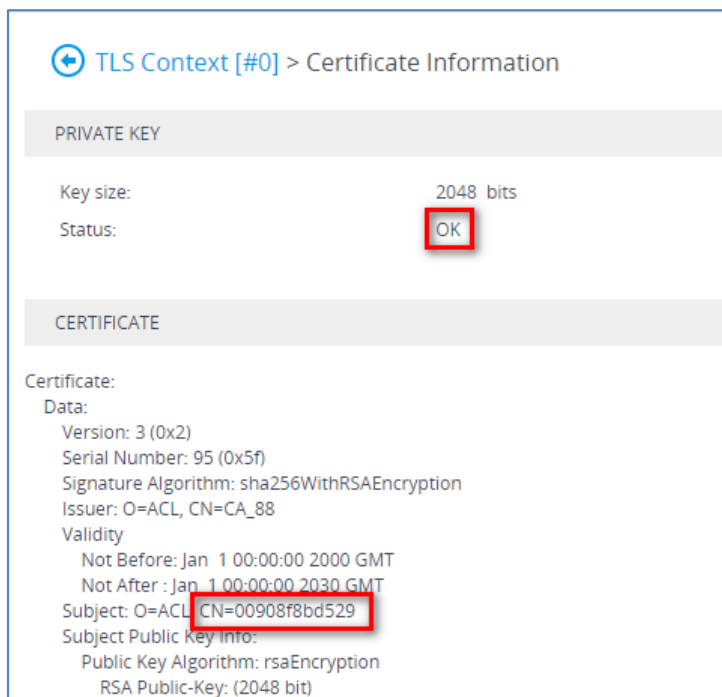
Figure 10: Example of Configured Trusted Root Certificates

 TLS Context [#0] > Trusted Root Certificates			
View		Import Export Remove	
INDEX	SUBJECT	ISSUER	EXPIRES
0	CA_88	RootCA	1/01/2030
1	RootCA	RootCA	1/01/2030

To check that the MP-1288 device has the correct signed certificate:

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the default TLS Context index (0) row, and then click the **Certificate Information** link located at the bottom of the TLS.
3. Validate the certificate **Status** and **Common Name**:

Figure 11: Certificate Information Example



⊕ TLS Context [#0] > Certificate Information

PRIVATE KEY

Key size: 2048 bits

Status: **OK**

CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 95 (0x5f)

Signature Algorithm: sha256WithRSAEncryption

Issuer: O=ACL, CN=CA_88

Validity

Not Before: Jan 1 00:00:00 2000 GMT

Not After : Jan 1 00:00:00 2030 GMT

Subject: O=ACL, **CN=00908f8bd529**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)