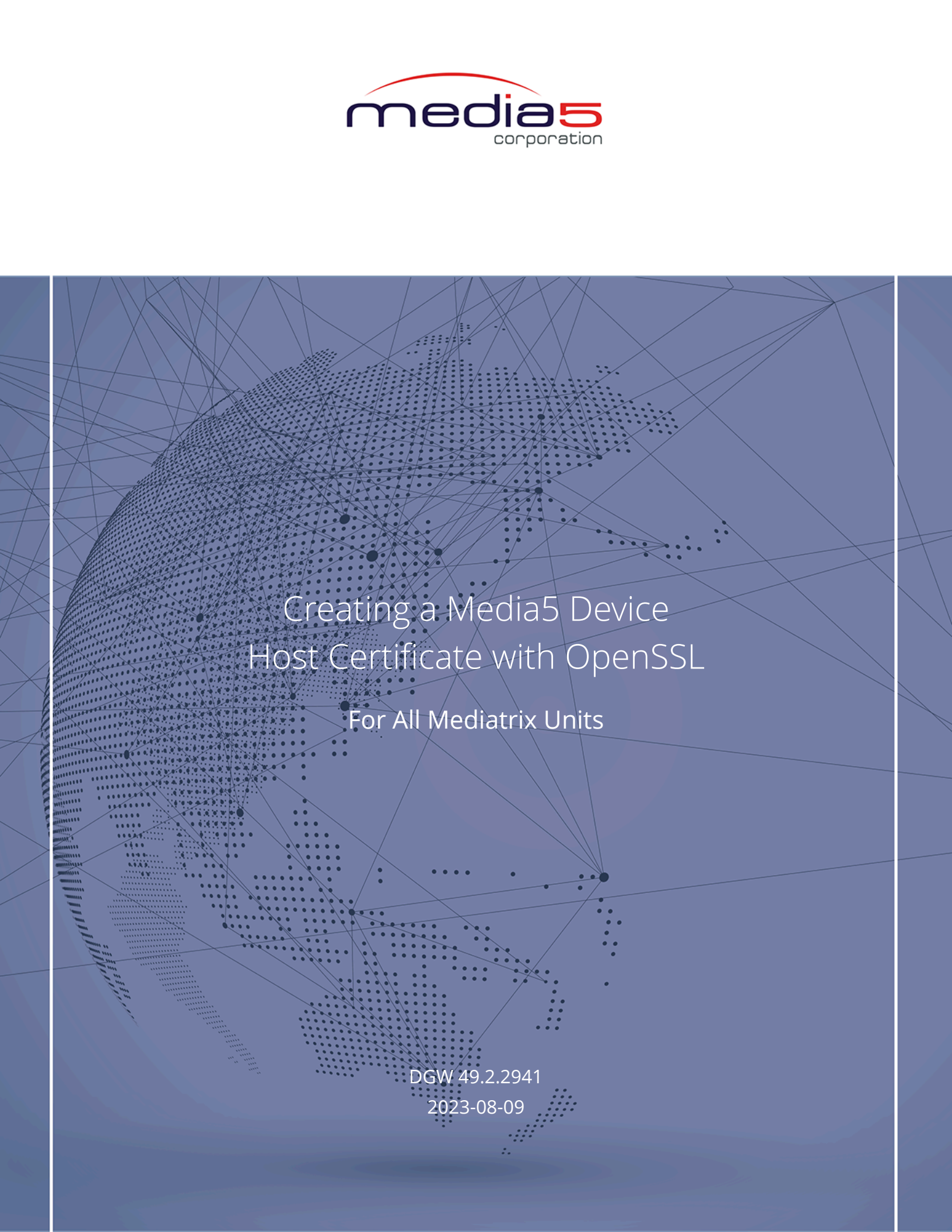


The background of the page is a dark blue gradient with a complex, abstract pattern of white lines and dots. The pattern resembles a network or a stylized map, with lines connecting various points and dots scattered throughout. The overall effect is technical and modern.

Creating a Media5 Device Host Certificate with OpenSSL For All Mediatrix Units

DGW 49.2.2941
2023-08-09

Table of Contents

Generating a Private Key	3
Creating a Certificate Signing Request (CSR) from a Private Key	4
Signing the CSR file by Your Own Certificate Authority (CA)	5
Signing the CSR by a Third Party Certificate Authority (CA)	6
Self-signing the CSR File	7
Combining the Private Key and the Signed Certificate	8
Importing a Host Certificate through the Web Page	10
Importing any Certificate through a Configuration Script	11
Online Help	12
DGW Documentation	13
Copyright Notice	14

Generating a Private Key

Steps

- 1) Enter **openssl genrsa -aes256 -out your_device.key 2048**

Note: The following step is optional.

- 2) Enter **cp your_device.key your_device.key.orig**
- 3) Enter **openssl rsa -in your_device.key.orig -out your_device.key** to remove the passphrase.

Example

```
[root@localhost mycert]# cp 192.168.1.31.key 192.168.1.31.key.orig
[root@localhost mycert]# openssl rsa -in 192.168.1.31.key.orig -out
192.168.1.31.key
Enter pass phrase for 192.168.1.31.key.orig:
writing RSA key
[root@localhost mycert]#
```

Result

A private key is generated with:

- a length of 2048 bits
- encryption with a 256 bit AES algorithm.

The output filename is your_device.key.

Next Step

[Creating a Certificate Signing Request \(CSR\) from a Private Key \(p.4\)](#)

Creating a Certificate Signing Request (CSR) from a Private Key

Steps

Enter **openssl req -new -key your_device.key -out your_device.csr -sha256**

Result

A CSR is generated from the private key created in the [Generating a Private Key](#) (p.3) procedure with a SHA256 signature algorithm. This is a result example.

```
[root@localhost mycert]# openssl req -new -key 192.168.1.31.key -out 192.168.1.31.csr -sha256
Enter pass phrase for 192.168.1.31.key:
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank. For some fields
there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code)[XX]:CA
State or Province Name (full name[]):Quebec
Locality Name (eg, city) [Default City]:Montreal
Organization Name (eg, company) [Default Company Ltd]:Media5
Organizational Unit Name (eg, section[]):TAC
Common Name (eg, your name or your server's hostname)[]):192.168.1.31
Email Address[:]:tac@media5corp.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []
:An optional company name []:
[root@localhost mycert]#
```

Next Step

[Signing the CSR file by Your Own Certificate Authority \(CA\) \(p.5\)](#)

Use this procedure if your certificates are signed by a Certificate Authority you have access to.

[Signing the CSR by a Third Party Certificate Authority \(CA\) \(p.6\)](#)

Use this procedure if your certificates are signed by a Certificate Authority you do not have access to.

[Self-signing the CSR File \(p.7\)](#)

Use this procedure if your certificates are self-signed, i.e. security is not an issue.

Signing the CSR file by Your Own Certificate Authority (CA)

Use this procedure if your certificates are signed by a Certificate Authority you have access to.

Steps

Enter **openssl x509 -req -extfile host_ext.cnf -extensions host_ext -sha256 -days 3652 -in your_device.csr -CA CA.crt -CAkey CA.key -CAserial CA.srl -out your_device.crt**

Note:

- **CA.key** is the private key of your CA
- **CA.crt** is the CA's public certificate
- **CA.srl** is the serial number file
- 3652 days is the validity period of the certificate
- **host_ext.cnf** defines the usage of the certificate. It contains:

```
[ host_ext ]
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
```

Result

This is a result example.

```
[root@localhost mycert]# openssl x509 -req -extfile host_ext.cnf -
extensions host_ext -sha256 -days
3652 -in 192.168.1.31.csr -CA CA.crt -CAkey CA.key -CAserial CA.srl -out
192.168.1.31.crt
Signature ok
subject=/C=CA/ST=Quebec/L=Montreal/O=Media5/OU=TAC/CN=192.168.1.31/
emailAddress=tac@media5corp.com
Getting CA Private Key
Enter pass phrase for CA.key:
root@localhost mycert]#
```

When the certificate will be imported to the Mediatrix unit, the information defined for the keyUsage of the host_ext.cnf file will be displayed in **Management>Certificates/Host Certificates** table, under the **Usage** column.

Next Step

[Combining the Private Key and the Signed Certificate \(p.8\)](#)

Signing the CSR by a Third Party Certificate Authority (CA)

Use this procedure if your certificates are signed by a Certificate Authority you do not have access to.

Steps

Send your CSR to the Third Party Certificate Authority agency responsible for signing your Certificate Signing Request.

Note: VeriSign or Entrust are examples of Third Party Certificate Authority Agencies.

Next Step

[Combining the Private Key and the Signed Certificate](#) (p.8)

Self-signing the CSR File

Use this procedure if your certificates are self-signed, i.e. security is not an issue.

Steps

Enter **openssl x509 -req -extfile host_ext.cnf -extensions host_ext -sha256 -days 3652 -in your_device.csr -signkey your_device.key -out your_device.crt**

IMPORTANT: The command must be entered on a single line, otherwise it will not work.

Note:

host_ext.cnf is a file containing the following which defines the usage of the certificate:

```
[ host_ext ]
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
```

Next Step

[Combining the Private Key and the Signed Certificate](#) (p.8)

Combining the Private Key and the Signed Certificate

Information

The host certificate required by the Mediatrix contains two parts: the private key and the signed certificate.

Steps

Enter **cat your_device.key your_device.crt > your_device.pem**

Result

This is a result example:

```
[root@localhost mycert]# cat 192.168.1.31.key 192.168.1.31.crt >
192.168.1.31.pem
[root@localhost mycert]# more 192.168.1.31.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAuxKD066oK0igcHQ1r1lnXLiQT9R0oQkE/pp0Do9vXZVsc8D6
uyFldRoDnm6wBHbbrhLgBfsZ5nVHwZ2KCsJJB2THehDXUskLS/4EWMveLcrzGygH
+qjHARwYmYQdEQrYrd/RqkDgnR2j9gocZBRXBfAWYtLgacJe4xLPy317JyR7YrLL
Qfv2hZAXqSdutmYJCys0405oEv1Dv7kfIDQvxP74Qsh0JgmW4Kq0eQdkfo+Xkwlp
pIdYyIHi+5TgWz4YoMRbZHZfKF+VdwOGAeSy2X+QCmHP81GR+SPefHzzn9oUk0Ha
DpjAPgKWUaaJPHrC8k+gsu6Wi0+dCRcUWnX47QIDAQABAoIBAQCnEMFia3iCED44
L5BCKPXG0I2ovXPq3MM5HVTYbABO8ykHtzA0Ln8NNU5GD1PiqMNHkL0/A6D9z39l
yeud9fKSR85dl0y3YhRUqWX4ZxjkjHrPpdB6aoBQU0snLnVG4wjfPyNfiNEPf4k0
EbmJJyEQjHlxiCIiUR0sfM5mTInPSZ3Glgm9l3gRZCBLLf6js+NiLYYi2ASyw6i
F1+Kxw0KTvxKa1TR0HYH35urPW528dFyZp8/f2QUUSM4aN5uQrKj8jDwEOIORsw6
+ybzM0pIbbS2I+cbmtDgr5KjjLE1+7dMY3K/hUmUkE+FPZiJf3v8vFFsRucAQcxq
1lg33ogBAoGBAOjZLXyIiz10RC/poRyMEhQ8xRUQaZiI279/J7N426F1G4An8yUl
8Qcmj2PXraLwnl6kX08Mmul7DN78BD0C7LSKK17PIFMH3NV8vWM8eWaE7nP9EqAJ
l0Lt0Gn2t+WeNL/Mc551XeBCCG9Ifg+pfnjF8kDPjqTe+8U4BEt4dYQxAoGBAM2s
K9vLoXoxJ50ay+ojTMYSuqPfeIND9WuzUJvLAjtgJGKUJsXYUnk5zVZ2IYRmt2EV
nCuAsemwComgDfLimCAEHuzGURG6t0pB7u2FWYiLm+ZJquCxL66p7zrQ/3hc2Q+Y
61mJ3lEay/IIRksS807Pck/k8q9tmG0Yg7mQcP19AoGATzg8coceIFB1gHuTFdxN
9laqr0PwBan90H1BumSh78JCTQ0VFAxTcZ/uG9TowEMUJTJ3GIkflUgDuldI8jP
8aikktATZkxhhLy4zn9vqkKFwi6S3KIGtX1yZGVKsbN+rNaJa5rwwnCU4A+g3AFF
hx+JiSVUmaFHTVSWmXq10LECGYAomyRmauA33GL39UAngWLWalFr0WoV00AZv+0
Mol3RY0JdwyORR5LVtEmj94gK7FM1qJlqFv34kzCTTpTyM9ILNxQgxsAYBfN7mSI
unopzj5yYfr9r7Jdxqk3uImnrtUgEjXtEJ427w5y86nNoqks1w2XJoGPhxi+GR9w
pIbaVQKBgBX/k9qc/wXf8uI6R650Jn8HiFFI0nr6brscnmd00D7bJPf2b4tKv1ap
CwSwj/BxYt9agncccXyEG8vHVLCTJYNYHJ/+0wID0ttN9dLE2fLPV1sgigMSY9oP
R9KrLT+LPKL1V11s033vuLcD6j0knH2kLKNRSNyxjGt+of0YxRaw
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIJA0cfW0xpBWD+MA0GCSqGSIb3DQEBCwUAMIGLMQswCQYD
VQQGEwJDQTEPMA0GA1UECAwGUXVlYmVjMREwDwYDVQQHDAhNb250cmVhbDEPMA0G
A1UECgwGTWVkaWE1MQwwCgYDVQQLDANUQUxhZjAUBG9NVBAMMDTE5Mi4xNjguMS4y
MjYxITAfBgkqhkiG9w0BCQEWEnRuZ0BtZWRpYTVjb3JwLmNvbTAeFw0xNTEyMDEx
MTQ4MTI0aFw0yNTEyMDExMTQ4MTI0aHIGKMqswCQYDVQQGEwJDQTEPMA0GA1UECAwG
```

```
UXVLYmVjMREwDwYDVQQHDAhNb250cmVhbDEPMA0GA1UECgwGTWVkaWE1MQwwCgYD
VQQLDANUQUUMxFTATBgNVBAMMDDE5Mi4xNjguMS4zMTEhMB8GCSqGSIb3DQEJARYS
dGFjQG1lZGlnNWNvcnAuY29tMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKC
AQEAuxKDO66oK0igcHQ1r1lnXLIQT9R0oQkE/pp0Do9vXZVsc8D6uyFldRoDnm6w
BHbbrhLgBfsZ5nVHwZ2KCsJJB2THEhDXUskLS/4EWMveLcrzGygH+qjHArwYmYQd
EQRyrd/RqkDgnR2j9gocZBRXBfAWYtLgacJe4xLPy317JyR7YrLLQfv2hZAXqSdu
tmYJCys04050Ev1Dv7kfIDQvxP74Qsh0JgmW4Kq0eQdkfo+XkwLppIdYyIHi+5Tg
Wz4YoMRbZHZfKF+Vdw0GAeSy2X+QCmHP81GR+SPefHzzn9oUk0HaDpjAPgKWUaaJ
PHrC8k+gsu6Wi0+dCRcUWnX47QIDAQABozkwNzAJBgNVHRMEAjAAMAsGA1UdDwQE
AwIEsDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwdQYJKoZIhvcNAQEL
BQADggEBAEX1sxk/Ad4aV0rPk2oE/dz0mFmq4LeucYw9uJ6F7SdewAU8pghXMvBu
c0wvToFdEmRTvPmsDghsPmxSgTyL4DBwfJ2YbPfoFK6BDnZAmU3gw37+WXY0w7tW
1ea+kWN4v6Dv/Ga0uBxQ4pAN2lQaDc99fMSp3G3TCFW4lh0lBEeBxvZ0pHwuLrcd
1IbdPNy7z13Ko0639B935Lj1CRGpzEvgSgGtcMhkLifLAL7dhLVcU7fLIA0z5Kov
A70ESnlj8V8DuVirBTNUKGqgY/36g87e7n8g84Xse86vEFhpkzCcZtDIKQ5KvTv
+iLgQLs9mjHAUruNV9+JJx1spv8FZp0=
-----END CERTIFICATE-----
```

Next Step

[Importing a Host Certificate through the Web Page \(p.10\)](#)

[Importing any Certificate through a Configuration Script \(p.11\)](#)

Importing a Host Certificate through the Web Page

Before you start

You must have an SNTP server for current date and time.

Steps

- 1) Go to **Management/Certificates**.
- 2) Click **Activate unsecure certificate transfer**.
- 3) From the **Type** selection list, select **Host**.
- 4) Click **Browse** and select the Host certificate.
- 5) Click **Apply**
- 6) In the **Host Certificate Associations** table, select the services that Host Certificate should be associated with.

Note: A Host certificate is by default associated with all services. Several Host Certificates can be imported and associated with one or several services.

- 7) Click **Import**.
- 8) Click **Apply**.

Result

This is an example of the result of a Host Certificate imported and associated with all services.

✦ Certificates

Host Certificates					
File Name	Issued To	Issued By	Valid From	Valid To	Usage
FQDN_Unit192.168.27.103.pem	192.168.27.103	192.168.1.27	2017-03-15 13:36:13	2027-03-15 13:36:13	TlsClient, TlsServer

Other Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA
Cert_MxDefault001.der	Media5 Corporation - Mediatix Primary CA	Media5 Corporation - Mediatix Primary CA	2015-03-06 15:06:40	2065-03-06 15:06:40	TlsClient, TlsServer	Yes

Host Certificate Associations											
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert	Nlm	SBC	CWMP	
FQDN_Unit192.168.27.103.pem	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	

Certificate Authorities	
File Name	Override the OCSP URL for issued Certificates
Cert_MxDefault001.der	

Certificate Import Through Web Browser	
Type	Path
Host	FQDN_Unit192.168.27.103.pem
	Import

Importing any Certificate through a Configuration Script

Information

To use the `Cert.InstallCertificate` command, the provided content must be a valid certificate file encoded in Base64.

Under Linux system: `base64 --wrap=0 myCertificate.crt > myBase64File.txt`

With OpenSSL tool: `openssl base64 -A -in myCertificate.crt -out myBase64File.txt`

Steps

- 1) Prepare the configuration script file with the wanted `Cert.InstallCertificate` command line to execute.

IMPORTANT: The *FileContent* argument requires the Base64 encoding of the whole certificate file, including the portions that may be already in Base64.

IMPORTANT: Double quotes must be used around the Base64 value of the *FileContent* argument.

```
Cert.InstallCertificate
  Name="MyCertificate.crt" Type="Host"
  FileContent="LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQ
pNSU1Fb3dJQkFBS0NBUEVudXhLRE82Nm9LT2lnY0hRMXlxbG5YTGlRVD
lSMG9Ra0UvcHBPRG85dlhaVnNjOEQ2CnV5RmxkUm9E...RESUtRNUt2V
HYKK2lMZ1FMczltakhBVXJ1TlY5K0pKeDFzcHY4RlpwMD0KLS0tLS1FT
kQgQ0VSVElGSUNBVEUtLS0tLQ=="
```

Note: For more details about the `Cert.InstallCertificate` command, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

Note: For more details on size limitation with configuration script file, refer to the [DGW Configuration Guide - Limitations of DGW Platforms](#) document published on the [Media5 Documentation Portal](#)

- 2) Go to **Management/Configuration Scripts/Execute**.
- 3) If you are not using HTTPS, click **Activate unsecure file importation from the Web browser**.
- 4) In the **Upload Script Through Web Browser** table, browse to the location of the file you wish to import.
- 5) Click **Upload and Execute**.

Result

The certificate will be inserted in the **Management/Certificates** page.

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the [Media5 Documentation Portal](#).

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes:** Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes:** These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins:** These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide:** They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide:** The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide:** This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com