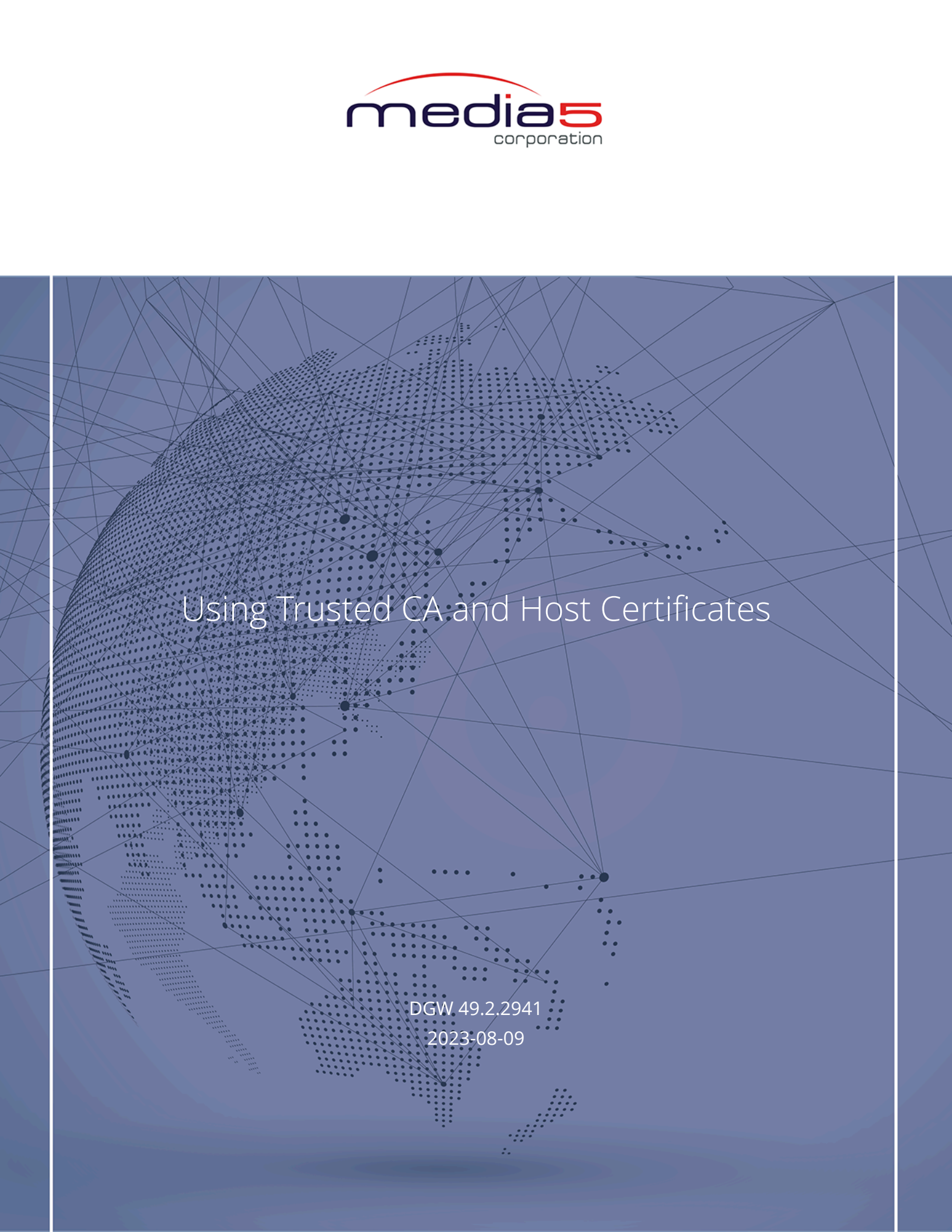




# Using Trusted CA and Host Certificates

DGW 49.2.2941  
2023-08-09

# Table of Contents

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| Certificates                                                          | 3  |
| Importing a Trusted CA or SIP Server Certificate through the Web Page | 4  |
| Importing a Host Certificate through the Web Page                     | 5  |
| Importing any Certificate through a Configuration Script              | 6  |
| Supported Certificate Types and Key Strength                          | 8  |
| Trusted CA Certificate Content Example                                | 9  |
| Online Help                                                           | 10 |
| DGW Documentation                                                     | 11 |
| Copyright Notice                                                      | 12 |

# Certificates

The Mediatrix unit uses digital certificates, which are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates such as:
  - **TlsClient:** The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
  - **TlsServer:** The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.
- whether or not the certificate is owned by a Certification Authority (CA)

Although certificates are factory-installed new ones can also be added. Since TLS certificates are validated in terms of time (certificate validation/expiration date, etc.), the use of NTP (Network Time Protocol) is mandatory when using the security features.

The Mediatrix unit uses two types of certificates:

- **Host Certificates:** used to certify the unit (e.g.: a web server with HTTPS requires a host certificate).
- **Others:** Any other certificate including trusted CA certificates used to certify peers (e.g.: a SIP server with TLS).

The Conf, Cwmp, Eth, Fpu, Nlm, Sbc, and SipEp services are considered secure as they require certificate validation to establish a secure connection to a remote host. The following parameters, available by the CLI, are used to determine whether or not the connection to the remote host should be validated with the service certificate. By default, the parameters are always set to a value requiring validation.

- `Conf.ScriptsTransferCertificateValidation`
- `Cwmp.TransportCertificateValidation`
- `Eth.Eap.CertificateValidation`
- `Fpu.MfpTransferCertificateValidation`
- `Nlm.PCcaptureTransferCertificateValidation`
- `Sbc.CertificateValidation`
- `SipEp.InteropTlsCertificateValidation` (also available in the DGW Web page under SIP/Interop)

The certificates must be uploaded to the Mediatrix units. They define how a Mediatrix unit will certify the remote host in order to mark it as secure and suitable for a TLS connection. If the Mediatrix unit does not trust the remote certificate (i.e. does not authenticate it with either one of the 3 methods: HostName, trustedCertificate, DnsSrv), then the Mediatrix unit will not establish the connection.

By default it is not possible to upload a Host certificate without first clicking on Activate unsecure certificate transfer. This is because the certificate upload will be done in clear text, which means the private key will be susceptible to interception. Establishing a connection without certificate validation, i.e. establishing an unsecure connection, should only be used :

- for testing purpose,
- if one cannot identify the required CA cert, or
- the CA cert has mismatched Common Name/Subject Alternate Name. (In this case there is no fallback, it will fail if the name does not match)

Certificates are used to secure the following connections:

- SIP
- Configuration Web pages
- File transfers (scripts, firmwares, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP (802.1x)

One common use of the host certificate is to allow HTTPS Web access to the unit (which in this case, the device is the TLS server). For more details refer to the [Technical Bulletins - Creating a Media5 Host Certificate with Open SSL](#) document on the [Media5 Documentation Portal](#).

## Importing a Trusted CA or SIP Server Certificate through the Web Page

### Before you start

You must have an SNTP server for time tracking.

### Steps

- 1) Go to **Management/Certificates**.
- 2) Click **Activate unsecure certificate transfer**.
- 3) In the **Certificate Import Through Web Browser** table, from the **Type** selection list, select **Other**.
- 4) Click **Browse** and select your certificate.

**Note:** The name of the certificate cannot have more than 50 characters.

- 5) Click **Import**.
- 6) Click **Apply**.

7) Click **restart required services** located at the top of the page.

## Result

| Host Certificates           |                     |                       |                     |                     |                      |   |
|-----------------------------|---------------------|-----------------------|---------------------|---------------------|----------------------|---|
| File Name                   | Issued To           | Issued By             | Valid From          | Valid To            | Usage                |   |
| 0090f80b1b9a_thomas_new.pem | 0090f80b1b9a        | Mediatix Units CA     | 2019-06-30 20:00:00 | 2069-06-30 20:00:00 | TlsClient, TlsServer | — |
| sentinel.pem                | s400.media5corp.com | ThomasNG CA Authority | 2017-08-08 22:22:09 | 2027-08-08 22:22:09 | TlsClient, TlsServer | — |

| Other Certificates                   |                                                              |                                    |                     |                     |                      |     |   |
|--------------------------------------|--------------------------------------------------------------|------------------------------------|---------------------|---------------------|----------------------|-----|---|
| File Name                            | Issued To                                                    | Issued By                          | Valid From          | Valid To            | Usage                | CA  |   |
| CAMedia5.crt                         | prod_ca.media5corp.com                                       | prod_ca.media5corp.com             | 2014-08-07 15:29:47 | 2058-05-28 15:29:47 |                      | Yes | — |
| DigiCertGlobalCAG2.crt               | DigiCert Global CA G2                                        | DigiCert Global Root G2            | 2013-08-01 08:00:00 | 2028-08-01 08:00:00 |                      | Yes | — |
| DigiCertGlobalRootG2.crt             | DigiCert Global Root G2                                      | DigiCert Global Root G2            | 2013-08-01 08:00:00 | 2038-01-15 07:00:00 |                      | Yes | — |
| DigiCertHighAssuranceEVRootCA.crt    | DigiCert High Assurance EV Root CA                           | DigiCert High Assurance EV Root CA | 2006-11-09 19:00:00 | 2031-11-09 19:00:00 |                      | Yes | — |
| Mediatix_IntermediateCA.crt          | Mediatix Units CA                                            | Media5 Corporation Root CA         | 2019-02-21 16:27:12 | 2043-11-26 11:25:46 | TlsClient, TlsServer | Yes | — |
| RootCA.pem.cer                       | DigiCert Global Root CA                                      | DigiCert Global Root CA            | 2006-11-09 19:00:00 | 2031-11-09 19:00:00 |                      | Yes | — |
| Symantec_SHA1_rootCA.cer             |                                                              |                                    | 1996-01-28 19:00:00 | 2028-08-01 19:59:59 |                      | No  | — |
| ThomasNg_CA.crt                      | ThomasNG CA Authority                                        | ThomasNG CA Authority              | 2017-08-08 22:06:46 | 2044-12-24 21:06:46 | TlsClient, TlsServer | Yes | — |
| Virtual_Root_CA.pem                  | Media5 Corporation Root CA                                   | Media5 Corporation Root CA         | 2018-11-26 11:15:47 | 2043-11-26 11:25:46 |                      | Yes | — |
| verisign_G5_primary_intermediate.cer | VeriSign Class 3 Public Primary Certification Authority - G5 |                                    | 2006-11-07 19:00:00 | 2021-11-07 18:59:59 | TlsClient, TlsServer | Yes | — |

| Host Certificate Associations |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |  |
|-------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--|
| File Name                     | SIP                                 | Web                                 | EAP                                 | Conf                                | Fpu                                 | File                                | Cert                                | Nlm                                 | SBC                                 | CWMP                                |  |
| 0090f80b1b9a_thomas_new.pem   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |  |
| sentinel.pem                  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |  |

**Note:** Make sure to associate the certificate to the appropriate service. If you are using SBC service, only 1 certificate should be associated to it.

## 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 - Mediatrix Primary CA | Media5 Corporation - Mediatrix 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   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |

| Certificate Authorities |                                               |
|-------------------------|-----------------------------------------------|
| File Name               | Override the OCSP URL for issued Certificates |
| Cert_MxDefault001.der   | <input type="text"/>                          |

| Certificate Import Through Web Browser |                                                          |
|----------------------------------------|----------------------------------------------------------|
| Type                                   | Path                                                     |
| Host                                   | <input type="text" value="FQDN_Unit192.168.27.103.pem"/> |

## 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
pNSU1Fb3dJQkFBS0NBUEVBdXhLRE82Nm9LT2lnY0hRMXIXbG5YTGlRVD
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.

# Supported Certificate Types and Key Strength

DGW supports the following certificate types and key strength for TLS connections:

- RSA certificates up to 4096-bit keys
- ECDSA certificates with the secp256r1, secp384r1, and secp521r1 curves
  - ECDSA is supported starting from DGW 47.0

And the following hashing algorithm:

- Up to SHA-512

# Trusted CA Certificate Content Example

```
-----BEGIN CERTIFICATE-----
MIICNTCCAZ6gAwIBAgIJANYsw8F6ocdbMA0GCSqGSIb3DQEBBQUAMEQxEzARBgoJ
kiaJk/IsZAEZFgNjb20xGTAXBgoJkiaJk/IsZAEZFglZWRpYXRyaXgxZjAQBgNV
BAMTCU1lZGlnNWRLdjAeFw0wODA4MzExNzQwMTBaFw0xODA4MzExNzQwMTBaMEQx
EzARBgoJkiaJk/IsZAEZFgNjb20xGTAXBgoJkiaJk/IsZAEZFglZWRpYXRyaXgx
ZjAQBgNVBAMTCU1lZGlnNWRLdjCBnzANBGMkqhkiG9w0BAQEFAAOBjQAwYkCgYEA
3TJm6UbpfidGJ/kURz3/kwr8lOLY+Fe280/Iq9Klq5m5G0NEbl8aF3+EbSPTV8GU
YlnzXdHHRAVDP5f3gPJU2+obWxbmQSlqvjx6QdxAhNcGTdPv7UGatQapCmQe1/Ct
2qtLqXrxG/bTPv+Vt/WKPmFEA+hjkVJ1hQgQLAUpD2MCAwEAAAMvMC0wDAYDVR0T
BAUwAwEB/zAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcN
AQEFBQADgYEALhFUmWUROV7UTf/Zy3hmZDwyjd8YcuAkb+TrdvK7yHJHTqC0DdvB
L10REHz6Ch7WCiydR8JLj0fAK+kXGYj9VdWj+qvlTnV4PBEvNzA3bbHBqVo0upJM
aDT7atCeNRJ8ipcy7MHN00FRbEW0XKhwnDxQnX2tz0myAeAnDHe5bsQ=
-----END CERTIFICATE-----
```

## 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](http://media5corp.com)