Using Trusted CA and SIP Server Certificates

1 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 certificates have a validity period (start date and expiry date), 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).

To enable a TLS connection on Mediatrix units, no CA certificate needs to be installed if the respective parameters for each secure service (e.g. SIP, Conf, Cwmp, etc) has the NoValidation value. If the value is different than NoValidation, then at least one CA certificate needs to be installed. This certificate must be uploaded to the Mediatrix units. The Mediatrix unit then checks the server identity by validating the host name used to contact it against the information found in the server's certificate. If the validation fails, the Mediatrix unit refuses the secure connection. For the SIP over TLS service, we have four (4) levels of validation: HostName, trustedCertificate, DNSSRV, and NoValidation (for a complete description of the validation levels, refer to the Help of the DGW Web interface under SIP/Interop). The way that the remote peer is evaluated for secure connection differs for each level. Remember that the unit must be correctly configured with an SNTP server because the TLS server certificate is also validated in terms of time (certificate validation/expiration date, etc.).

For example in a setup for two Mediatrix gateways with no SIP proxy in the middle. At least one of the units will require a Host certificate. If only one unit has a Host certificate, the calls will be allowed in only one direction (Unit 1 calls Unit 2). For bi-directional calls, both Mediatrix units would require a Host certificate. 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.

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)
1.1 Importing a Trusted CA or SIP Server Certificate to the Mediatrix Unit

**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**

---

2 Trusted CA Certificate Content Example

```
-----BEGIN CERTIFICATE-----
MIICNTCCz6gAwIBAgIJANYsw8F6o0dbMA0GCSqGSIb3DQEBCwUAMQQxExzARBgogJ
kiaJk/IgEAzAZFgNgjB20xGTXBgoJkiaJk/IgEAzAZFgNgjB20xGTXBgoJkiaJk/IgEAzAZ
FgNgjB20xGTXBgoJkiaJk/IgEAzAZFgNgjB20xGTXBgoJkiaJk/IgEAzAZFgNgjB20xGTXBgoJ
kiaJk/IgEAzAZFgNgjB20xGTXBgoJkiaJk/IgEAzAZFgNgjB20xGTXBgoJkiaJk/IgEAzAZFg
-----END CERTIFICATE-----
```

3 Online Help
4 DGW Documentation

Mediatrix units are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the Documentation Portal at http://documentation.media5corp.com

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.

5 Copyright Notice

Copyright © 2019 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.