media5 corporation

Mediatrix Management Tools

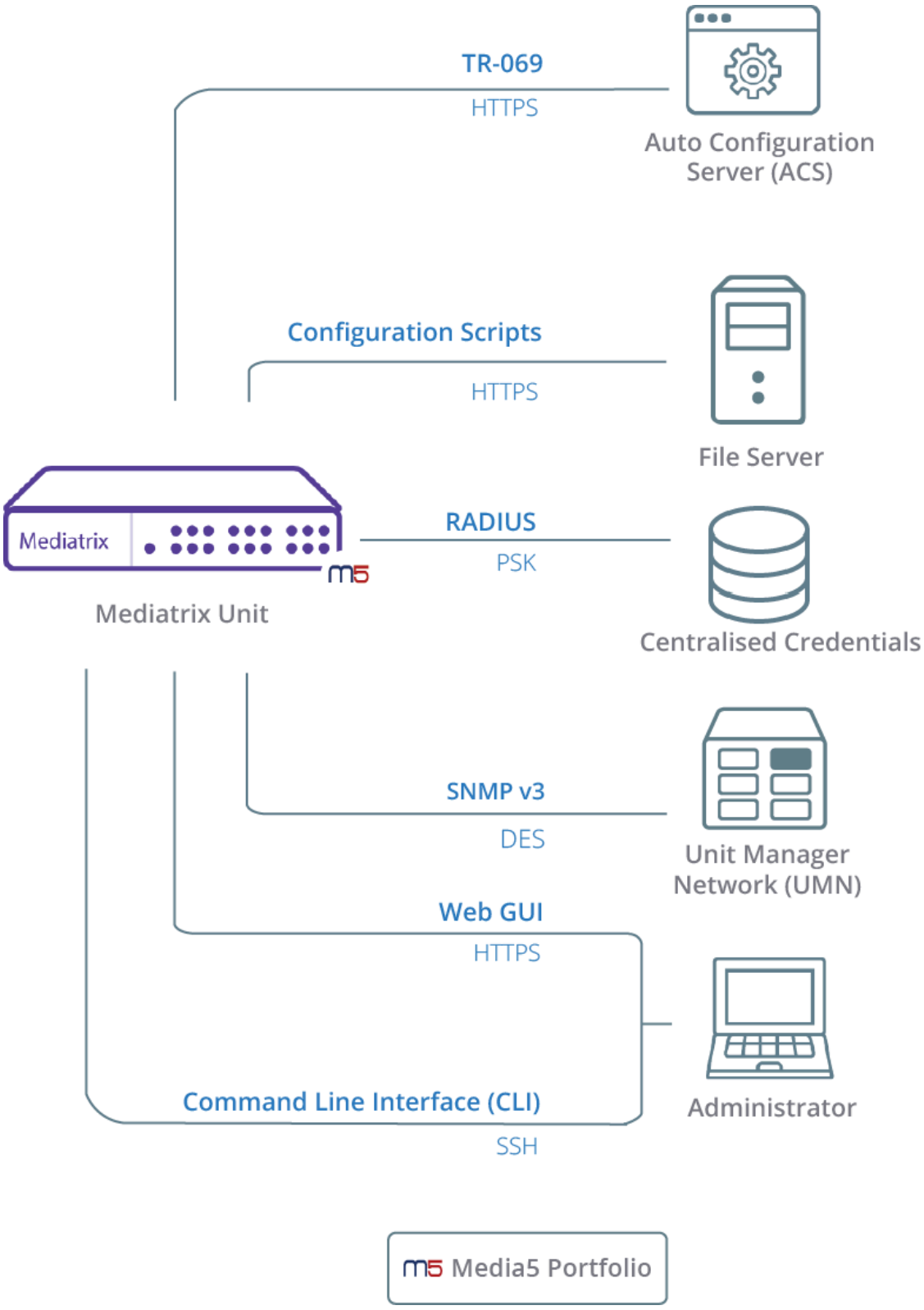
Table of Contents

1 Provisioning a CPE for VoIP Deployments

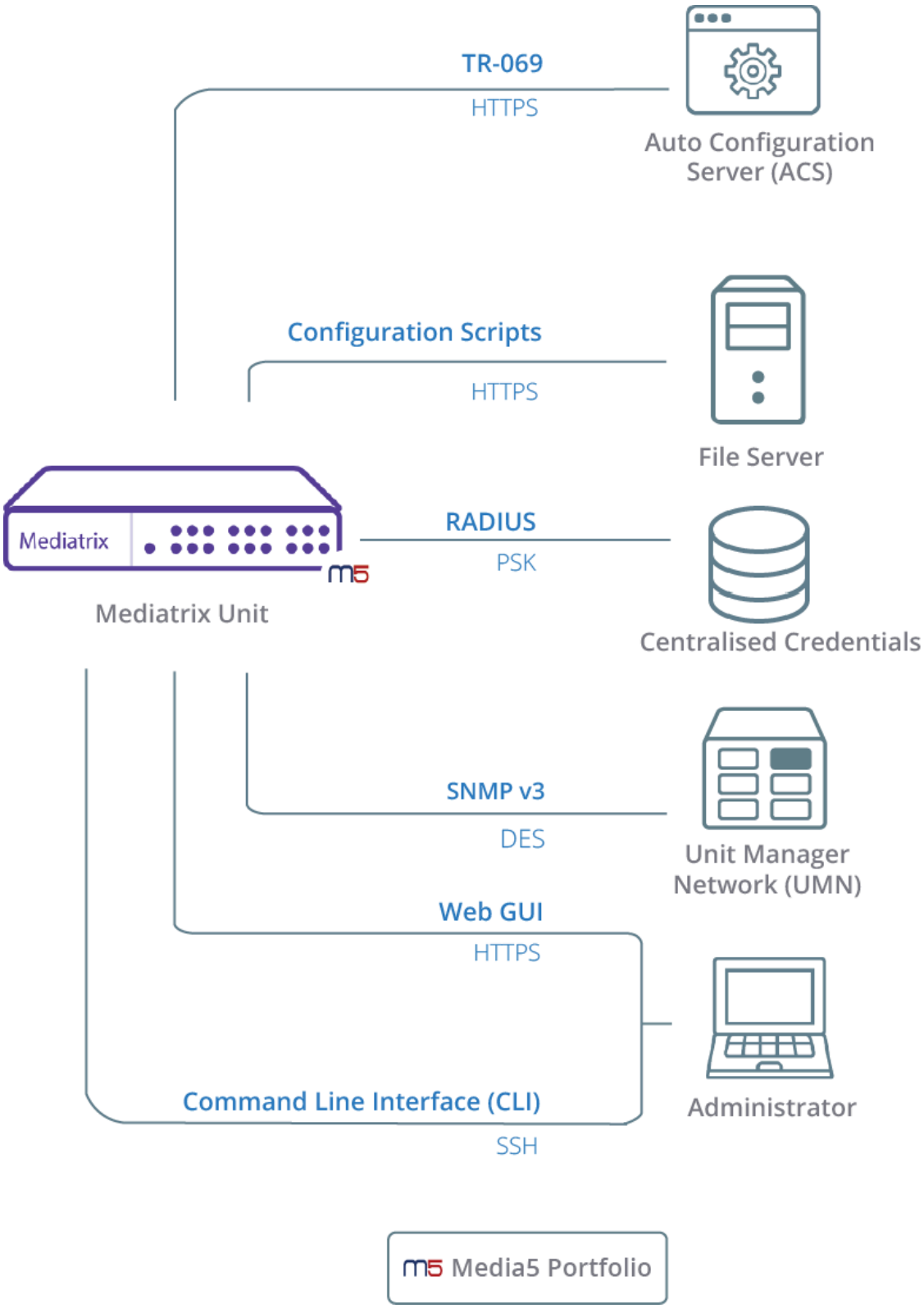
Over the last decade, the telecom industry initiated an intense migration from legacy networks to Voice Over IP (VoIP). VoIP brings numerous benefits such as reducing communication costs for end users, reducing operation and maintenance costs for carriers, and introducing a large variety of new applications such as instant messaging, file sharing, video conference and much more.

With a large variety of functions, different Customer Premise Equipment (CPE) are used by providers to deliver telecom services to residential and enterprise subscribers. CPEs represent a significant component into the network to secure communications between parties and ensure quality of service. CPEs also permit adapting the connection between legacy and IP based systems, and fulfill advanced features in compliance with the evolving environment of modern communications. For service providers, CPEs represent an important element of the capital and operation expenditures. It becomes of major concern for CPE vendors selecting a product design that will offer a competitive pricing structure, but also efficient management tools that will facilitate enabling new services. The following sections provide an overview of Mediatrix Product Line benefits and advantages for VoIP services deployments

2 Management Interfaces



2.1 Management Interfaces



2.2 TR-069 or CPE WAN Management Protocol (CWMP)

The Technical Report 069 (TR-069), also known as CWMP, is a Broadband Forum technical specification. This protocol can be used to monitor and update the Mediatrix unit configurations and firmware. In other words, when using TR-069, the Mediatrix unit can get in contact with an Auto Configuration Server (ACS) to initiate a configuration script transfer/execution and a firmware upgrade.

The first time the Mediatrix unit is connected to the network, it will attempt to contact the Auto Configuration Server (ACS), which is the entry point for the administrator. The Mediatrix unit will obtain the URL of the ACS using either the DHCP server with option 43 or by retrieving the information directly from the Customer's Profile. Therefore, upon start-up, the Mediatrix unit will contact the ACS, which in return will send the required configuration files and initiate, if necessary, a firmware update. This automated sequence is what is referred to as zero-touch, as the Mediatrix unit is automatically configured by the ACS according to the instructions given by the administrator without manual intervention on the unit.

The administrator can determine a schedule for the Mediatrix unit to periodically contact the ACS. These contacts will allow the Mediatrix unit to:

- verify if new configurations are available,
- verify if a new firmware update is available and
- send notifications for monitoring purposes.

Monitoring is achieved by regularly sending notifications to the ACS, through the mean of "Inform" requests, which can be:

- Passive: the information is sent according to the schedule.
- Active: the information is sent immediately when a parameter status changes, regardless of the periodic schedule.

Because the Periodic Informs are initiated by the Mediatrix unit, they have no problem passing through residential or enterprise NAT and firewalls.

Furthermore, the administrator can initiate a connection to the Mediatrix unit to perform immediate maintenance or monitoring. This will only be possible if the NAT firewall has been configured to allow communications initiated by the ACS.

The TR-069 protocol can be activated on units that are already deployed with a licence key (For more details on licences refer to theTechnical Bulletin - How to activate a licence on a Mediatrix unit published on the Media5 Documentation Portal). However, it can be enabled/disabled for a specific configuration via the Management interface.

TR-069 methods supported by the Mediatrix unit include:

- SetParameterValues
- GetParameterValues
- AddObject
- DeleteObject

- Download
- Reboot
- Upload
- FactoryReset

2.3 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) can be used to configure all the parameters available in the Mediatrix CPE, to perform firmware updates, to import a configuration and to monitor the Mediatrix CPE.

To configure the Mediatrix CPE parameters with the SNMP, a secure SNMPv3 or a non-secure SNMPv1 connexion can be used. The CPE does not grant an SNMPv3 access without authentication and privacy. Because the connexion is initiated by the Management Server, the communication is usually unable to go through the NAT Firewall.

Unit monitoring is possible with SNMP because it provides access to all the status parameters of the CPE. Furthermore, the CPE can send notifications, called traps, to the Management Server, that will allow the administrator to monitor specific events. Because it is the CPE that sends the notifications, the communication is usually able to go through the NAT Firewall however the SNMP protocol, based on UDP, does not insure reliable delivery of notifications.

The Mediatrix CPE supports the following SNMP methods:

- GetRequest
- SetRequest
- GetResponse
- SetResponse
- Trap
- GetWalk

The following Management Servers are certified to be used with our Mediatrix units:

- UMN
- HP Openview

The DGW Configuration Guide - Reference Guide published on the Media5 Documentation Portal provides the list of all available parameters.

2.4 Command Line Interface (CLI)

The Command Line Interface (CLI) provides an access to interactively configure all the Mediatrix unit parameters.

IMPORTANT: Although it is possible to configure existing ruleset parameters via the CLI, it is not possible to create or edit a ruleset from the CLI: it must be either imported or directly created or edited in the DGW Web interface.

The CLI is accessed through either a secure SSH session (default) or an unsecure TELNET session. When using a secure SSH session, all communications between Client and server are encrypted before being sent over the network, thus packet sniffers are unable to extract user names, passwords, and other potentially sensitive data. This is the default and recommended way to access the Command Line Interface.

The command interpreter interface of the CLI allows the user to browse the unit parameters, write the command lines, and display the system's notification log.

2.4.1 Command Line Interface Parameters

For more details on the scripting language, refer to the DGW Configuration guide - Configuration Scripting Language Syntax published on the Media5 Documentation Portal.

2.5 Configuration Manager Service

The Configuration Manager (Conf) service allows executing configuration scripts as well as performing the backup/restore of the CPE's configuration. Configuration scripts are files containing textual commands that are downloaded from a file server over the network to a Mediatrix CPE. Scripts can be downloaded using the FTP, TFTP, HTTP and HTTPS protocols. All available parameters used to configure the Mediatrix CPE are supported by the configuration scripts.

Written by the system administrator, scripts can be used to assign values to parameters or execute configuration commands such as:

- Automate recurrent configuration tasks
- Batch-apply configuration settings to multiple devices
- Initiate firmware upgrade

The administrator can chose to trigger the execution of scripts in different ways:

- Scheduled to be executed once
- Scheduled to be executed periodically at a specified time interval
- When the CPE is restarted

It is possible to generate a configuration script from the configuration running on the Mediatrix CPE. This script can be used as a:

- Starting point to create a variation of the configuration for another CPE
- Troubleshooting tool to view the content of a faulty configuration

- Back-up in case the CPE needs to be reset

The automated importation of configuration scripts can be performed using a Customer Profile or using a DHCP server indicating the location of the file server with options 66 or 67. The automated importation to a CPE is what is referred to as zero-touch, as the CPE is automatically updated with the latest configuration scripts without manual intervention. Because the importation is initiated by the Mediatrix CPE, scripts have no problem passing through residential or enterprise NAT and Firewalls.

3 Configuration Elements

3.1 Configuration Parameters

Mediatrix offers a very detailed level of configuration. This provides a powerful flexibility to adapt the configuration to almost any SIP implementation. SIP is a technology based on a list of RFC and 3GPP recommendations that SIP vendors address diferently. These differences led to interoperability issues that demanded frequent adaptations when deploying servers and endpoints from different vendors. The large list of configuration parameters available with Mediatrix CPEs make these adaptations possible.

The configuration database of Mediatrix devices is organised into services. Each service:

- Implements a set of related features
- Defines a set of configuration parameters (read-write) and status parameters (read-only), organized as single elements or in tables
- Defines a set of commands for performing interactive management actions (adding/deleting rows in table, initiating a file transfer, forcing re-registration, etc.)

Parameters configure every aspect of the Mediatrix CPE behaviour including:

- Networking parameters
- Telephony services activation
- Security policies
- Interoperability adaptations

Access to parameters is granted according to administrator credentials, 3 access levels are supported. This is customizable in Customer Profiles. Manually accessing to configuration parameters is available though a web GUI, SNMP management servers and Command Line Interface.

3.2 Configuration Scripts

Carriers and service providers usually define a configuration that will apply to a large number of units in compliance with the network architecture. It is the commands and the parameter values grouped in a text file that produce the Configuration Scripts.

To enforce security, configuration scripts can be encrypted and only Mediatrix units with the matching encryption key will be capable of decrypting and applying the configuration settings. Furthermore, configuration scripts can be downloaded and uploaded using HTTPS.

Configuration Script files are fetched by Mediatrix units from the network through any of the management interfaces available. Upon receiving the file, the Mediatrix unit executes each command line in sequence and assigns the values to the configuration parameters.

3.2.1 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is a transfer protocol widely used to secure communications over Internet telephony networks.

HTTPS allows for communications over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS). HTTPS is mainly used to secure the content of a Web site and securely transfer files.

A communication using HTTPS reasonably guaranties that the targeted peer is the proper one, not an impostor, and that media cannot be read or tampered by any third-party.

3.2.1.1 Transport Layer Security (TLS)

The Transport Layer Security protocol provides data privacy and integrity for computer network communications.

In other words, it provides signaling security and communication security. TLS is a widely used security protocol that allows for:

- Server and Client authentication
- Data confidentiality
- Data integrity

TLS is used for:

- DGW Web Access
- HTTP-based Configuration/Firmware File Transfer
- 802.1X
- SIP communications
- TR-069 (CWMP)

When a certificate is authenticated, a secure TLS connection is established with a peer. Then SIP, HTTPS, and TR-069 can be used over the TLS connection. TLS connections also prevents man-in-the-middle attacks.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. Once TLS is enabled, it is enabled for all configured SIP gateways.

Although some parameters are available through the Web GUI, many parameters are not accessible through the Web GUI:

- Cipher Suite
- TLS version
- Certificate validation and trust level

For more details on advanced parameters, refer to Transport Layer Security (TLS) Parameters (p.15).

3.2.1.2 Unit Signaling Security

Signaling is the protocol that activates a device located in the network and establishes calls between peers.

To provide security to signaling, the Mediatrix unit will connect to the network via SIP over TLS. The network is then authenticated by a certificate that guaranties that the Mediatrix unit is connected to a "safe" network.

The network will then authenticate the device with the username and password to make sure the device is part of the network's subscriber list. This authentication is done with the digest authentication. The result of these authentications and verifications provides private and reliable communications between the network and the device. Calls will be established without leaving any possibility to a third party to identify the called or callee number, or to be able to interfere with the communication in any way.

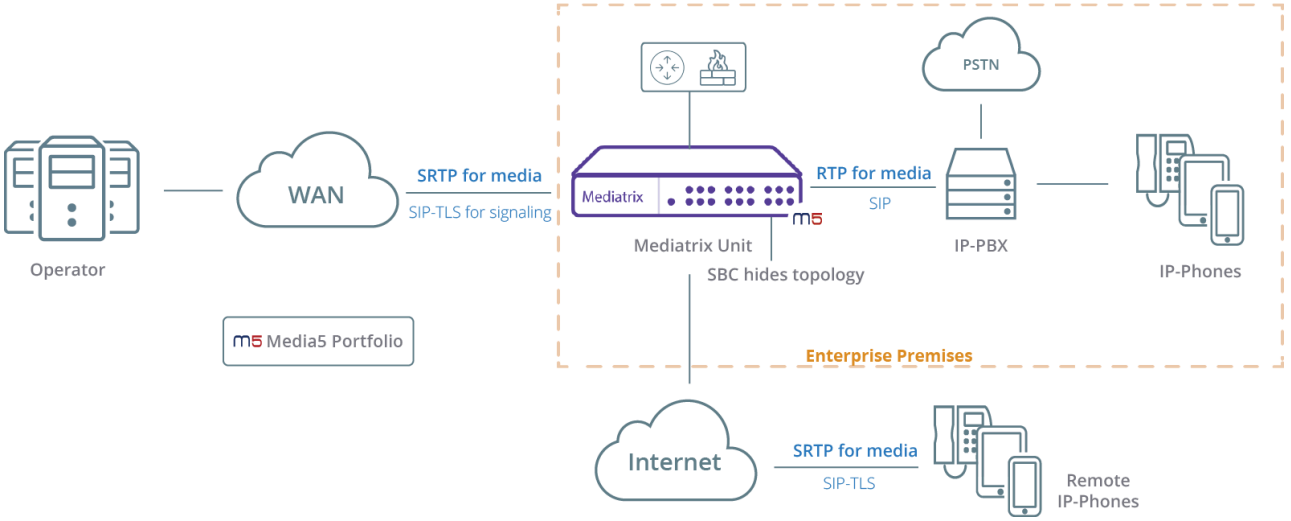
3.2.1.3 Communications Security

An important aspect of communications security, is that data sent and received from one endpoint to another remains secured, reliable, and private at all times.

When configured for complete security, signaling is performed with TLS with the use of a certificate and the unit transports the audio and video through Secure RTP (SRTP). The Mediatrix unit will make sure that the certificate specifically encrypted for the session and issued by the end user is valid, e.g.:

- the date and hour are not expired
- the certificate was issued by a recognised authority and configured within the unit
- the certificate was issued for the proper IP address or specific FQDN

The following diagram combines several use cases of communications security.



3.2.1.4 X-509 Certificates

The Mediatrix unit uses digital X-509 certificates which are based on the international X.509 public key infrastructure (PKI) standard. The certificates are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

X.509 certificates provide guaranties on confidentiality, authentication, integrity, and non-repudiation. It is the Public Key Infrastructure (PKI) which includes hardware, procedures, and software than manages the certificates. The PKI also provides public-key encryption. Therefore, the Public Key Infrastructure provides information that can guaranty that the signed certificates can be trusted.

To enable a TLS connection on Mediatrix units, at least one CA certificate is needed to validate that the certificate presented by the server is valid. This certificate must be uploaded to the Mediatrix units. The Mediatrix unit then checks the server's 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. 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)

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 (TlsClient or TlsServer)
- whether or not the certificate is owned by a Certification Authority (CA)

3.2.1.5 Authentication

As defined in the Oxford Dictionary, authentication is the process or action of verifying the identity of a user or process.

In an Internet telephony network environment, authentication will allow the Mediatrix unit to make sure the peer it is communicating with is the proper network or endpoint (unit or end-user device). This provides a level of security for communications as no communication will be allowed if the authentication is not confirmed.

3.2.1.6 SIP Transport Types

You can globally set the transport type for SIP all the endpoints of the Mediatrix unit to either UDP (User Datagram Protocol), TCP (Transmission Control Protocol), or TLS (Transport Layer Security).

Please note that RFC 3261 states the implementations must be able to handle messages up to the maximum datagram packet size. For UDP, this size is 65,535 bytes, including IP and UDP headers. However, the maximum datagram packet size the Mediatrix unit supports for a SIP request or response is 5120 bytes excluding the IP and UDP headers. This should be enough, as a packet is rarely bigger than 2500 bytes.

3.2.1.7 Transport Layer Security (TLS) Parameters

Although the services can be configured in great part in the Web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the DGW Configuration Guide - Reference Guide published on the Media5 Documentation Portal. The Reference Guide contains all the parameters used in the DGW software with their description, default values, and interactions.

For certificate transfert

- To set the HTTPS transfer cipher suite for certificate transfer: **Cert.TransferHttpsCipherSuite**
- To set the HTTPS transfer Tls Version for certificate transfer:: **Cert.TransferHttpsTlsVersion**
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

For file transfer

- To set the HTTPS transfer cipher suite for file transfer: **File.TransferHttpsCipherSuite**
- To set the HTTPS transfer Tls Version configuration for file transfer: **File.TransferHttpsTlsVersion**

For DGW Web access

- To set the Https Cipher Suite for secure DGW Web access: **Web.HttpsCipherSuite**.
- To set the Http Mode used for DGW Web access: **Web.HttpMode**
- To select the Secure Server Port used to access the DGW Web interface: **Web.SecureServerPort**
- To set the HTTPS Cipher Suite for secure DGW Web access: **Web.HttpsCipherSuite**
- To set the Tls Version used for secure DGW Web access: **Web.TlsVersion**

For SIP TLS transport

- To set the TLS transport cipher suite used for secure SIP transport: **SipEp.TransportTlsCipherSuite**
- To set Transport Tls Version used for secure SIP transport: **SipEp.TransportTlsVersion**
- To set TLS client authentication: **SipEp.InteropTlsClientAuthenticationEnable**

For TR-069 (CWMP) establishment

- To set the HTTPS transport cipher suite configuration for TR-069 (CWMP): **Cwmp.TransportHttpsCipherSuite**
- To set the HTTPS Transport Tls Version configuration for TR-069 (CWMP): **Cwmp.TransportHTTPSTlsVersion**
- To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS: **Cwmp.TransportCertificateValidation**

3.3 Rulesets

Mediatrix CPEs offering session border controller capabilities address a large variety of applications such as network demarcation, SIP firewall, SIP normalization and survivability. To facilitate the implementation of these applications, Mediatrix session border controller provisioning is based on a catalog of configuration templates named Rulesets. Rulesets define one or several rules used to filter, manipulate or route inbound or outbound requests.

For example, they can manage:

- NAT Traversal
- Media anchoring
- SIP normalization

By selecting these Rulesets, administrators will manage service activations following a few steps procedure and saving valuable operation time. A Ruleset editor available with Mediatrix session border controllers enables administrators to create new Ruleset or modify existing ones to adjust settings to different deployment scenarios.

3.4 Security Certificates

Security Certificates are files used to authenticate a Mediatrix CPE to other network elements and vice versa. In other words, they establish a secure connection, using TLS or HTTPS, between the Mediatrix CPE and the network elements. Security certificates contain attributes that identify a network element or an organisation. They also include a public or private encryption key.

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)

Although Security Certificates are factory installed, it is possible to add new ones to an existing CPE.

4 Troubleshooting

The Mediatrix CPE provides several troubleshooting features such as notification messages, diagnostic traces and SIP signalling logs.

The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/ IP protocol. With this software, you can monitor useful messages coming from the Mediatrix CPE.

- **Diagnostic Traces** are sent using the Syslog to the Technical Assistance Centre to further assist in resolving some issues such as Interoperability.
- **PCM traces** are two different RTP streams made specifically to record all analog signals that are either sent or received on the analog or ISDN side of the Mediatrix device. PCM traces are an efficient tool to identify problems with:
  - Echo in your network
  - DTMF signals
  - Caller ID signals
  - Fax signals or false Fax detection
  - Message Waiting Indicator signals
  - Any other analog or digital signal
- **Statistics** are collected on each port of the PRI card, on Ping/Pingv6 on the CLI or on Media. Statistics are collected on:
  - Packet loss
  - Jitter
  - Latency
  - Packet count
  - Octet count
- **Live Network Captures** can be taken with the pcapture command and sent to Wireshark located on a separate terminal. The SBC can also capture the SIP/RTP traffic of a specific call, selected by rules. The Network Capture will gather information on:
  - Interoperability
  - Timing issues
- **Configuration scripts** can be generated from the configuration running on the Mediatrix CPE. This provides the content of your configuration that can be used by technical support to troubleshoot your faulty configuration.

5 Monitoring

Several features are available for monitoring.

- Event Notifications are sent to a Syslog server, a SIP server or saved in a local file, depending on the rules that are applied to the event. Notifications can be sent for events such as:
  - SIP registration failures
  - TLS authentication failures
  - Maximum number of calls reached on a PRI line
- SNMP traps (notifications) can be sent by the CPE to the Management server allowing the administrator to monitor specific events such as:
  - Cold start
  - Warm start
  - Link up
  - Link down
  - Authentication failure
- TR-069 notifications are regularly sent to the ACS. These periodic contacts, also called Periodic Informs, can be:
  - Passive: the information is sent according to the defined schedule.
  - Active: the information is sent immediately when the event occurs, regardless of the schedule, if a parameter value changes, because the administrator may want to be informed immediately.
- Call Details Record are sent by Syslog and the format can be customised. They contain information such as:
  - Source identities (points of origin)
  - Destination identities (endpoints)
  - Call duration
  - Total usage time for the billing period

6 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:

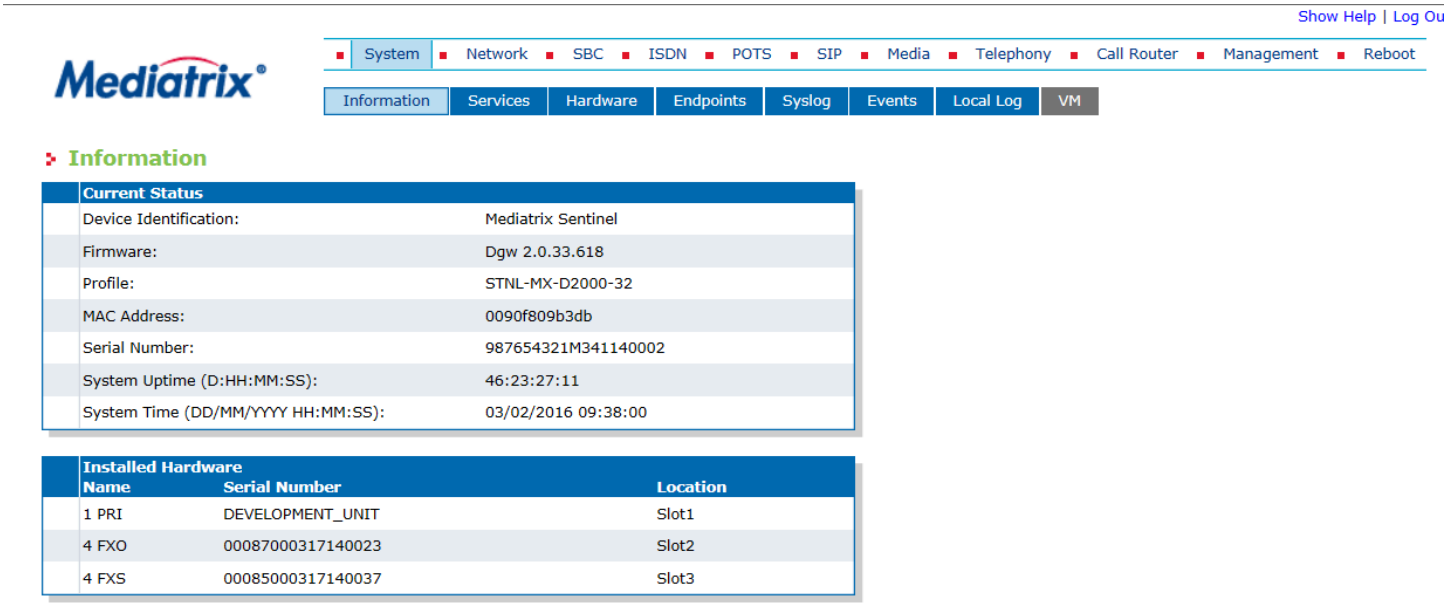
- **Release notes**: Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes**: These documents are created to facilitate the configuration of a specific use case. 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.

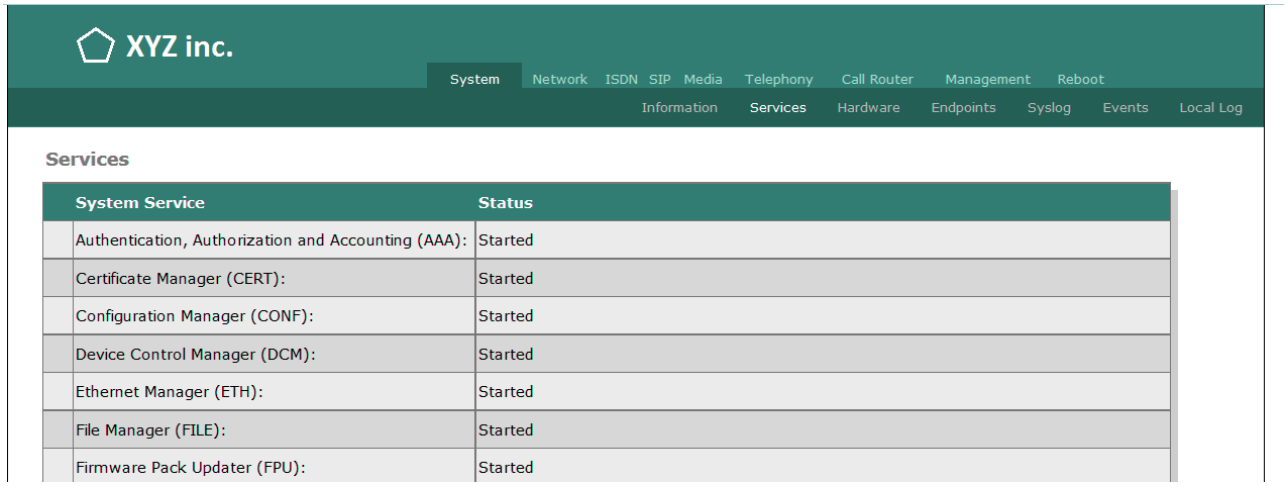
7 Customisation

7.1 Branding

Several aspects of branding can be configured through a customer profile.

- Web interface appearance (Logo, colour, and skin)





- Color of device

- Labels on device

- Custom Model names
- Customer provided Mac address and serial number

7.2 Customer Profile

A profile is a customer factory customisation where parameter values, skins, and branding are defined specifically for the customer.

Customer profiles can be uploaded via HTTPS/TLS to insure data integrity and confidentiality. The customer profile can include information on:

- security:
  - default administrator accounts and password policies
  - security parameters to be activated
  - specific services to activate or not
  - the installation of security certificates
  - the customisation of web pages
  - the installation of Rulesets used by the SBC
  - the installation of a VM image
  - the URL of the Auto Configuration Server (ACS) or of a configuration script
- configuration:
  - the installation of Rulesets used by the SBC
  - the installation of a VM image
  - the URL of the Auto Configuration Server (ACS) or of a configuration script
- branding:
  - the customisation of web pages

8 Copyright Notice

media5 corporation

media5corp.com