

Transport Layer Security

For all Mediatrix units

DGW 49.2.2941

2023-08-09

Table of Contents

Transport Layer Security (TLS)	3
X-509 Certificates	3
Hypertext Transfer Protocol Secure (HTTPS)	4
TR-069 or CPE WAN Management Protocol (CWMP)	4
Authentication	5
SIP over TLS	6
Basic Tasks	8
Preparing the Unit to Use TLS for SIP	8
Enabling TLS Debugging on Wireshark	10
Selecting the SIP TLS Server Certificate Security Level	11
Advanced Parameters	12
Transport Layer Security (TLS) Parameters	12
Online Help	14
DGW Documentation	15
Copyright Notice	16

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.12).

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)

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.

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 the [Technical 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

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.

SIP over TLS

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.

TLS Persistent Connections

Transport Layer Security (TLS) Persistent Connections are associated with the SIP servers (outbound proxy, registrar, and home domain proxy).

TLS connections are currently only supported with SIP Trunk gateways. The TLS Persistent Connections statuses are available under **SIP/Servers** of the DGW Web interface.

Note: The **Status** table is not displayed if the persistent connections are not activated.

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.

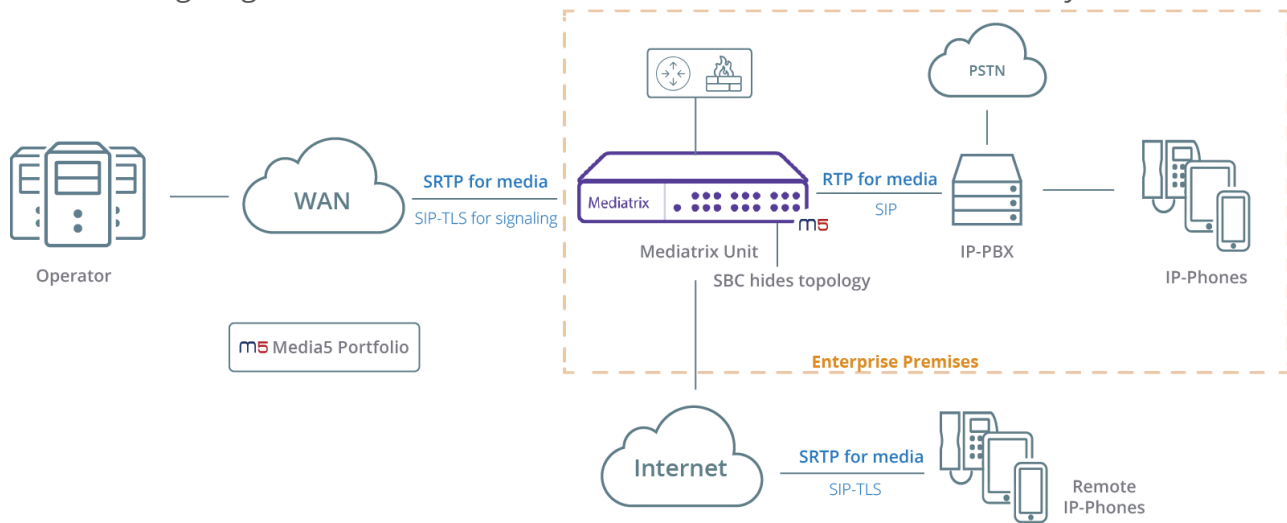
Communications Security

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.



Basic Tasks

Preparing the Unit to Use TLS for SIP

Information

These steps should be performed first when using Transport Layer Security (TLS) as they are mandatory for all TLS based applications (TR-069, SIP over TLS, 802.1X, HTTPS file transfer, etc.)

Steps

- 1) Make sure the unit is able to retrieve current Time/Date information from a NTP server, either from a NTP server learnt from DHCP or static NTP servers.
- 2) Make sure the time zone of your unit is adjusted properly. Refer to [Selecting the Unit's Time Zone](#) (p.9)

Note: This step is mandatory for the unit to have the proper date/time, otherwise the TLS communication cannot be validated.

- 3) Upload all the trusted CA certificates required for server validation. Refer to [Technical Bulletin -Using Trusted CA and Host Certificates](#) published on the [Media5 Documentation Portal](#).
- 4) If the respective pop-up message appears, click **restart required services**.

Enabling Secure Signaling (TLS)

Information

.

Steps

- 1) Go to **SIP/Transport** tab.
- 2) In the **Protocol Configuration** table, from the **TLS** dropbox, select **Enable**.

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

- 3) Click **Apply**.
- 4) Follow the link located at the top of the Web page to start the appropriate service.

Result

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable ▾		Disable ▾		Enable ▾	

Apply

The Ready LED will turn to a steady green. The SipEp Notification messages #303 and #310 are sent once the TLS connection is established. For example:

Syslog message: USER.INFO: SipEp: 1400-SIP Endpoint: 303-TLS connection with remote host 10.5.128.14:5063 is now ready to be used for SIP gateway default.

Syslog message: USER.INFO: SipEp: 1400-SIP Endpoint: 310-Server 10.5.128.14:5063 is now reachable for SIP gateway default.

Selecting the Unit's Time Zone

Information

Time Servers should be configured under Network/Host/SNTP Configuration. For more details refer to the [DGW Configuration Guide - Vlan Configuration](#) published on the [Media5 Documentation Portal](#).

Steps

- 1) Go to **Network/Host**.
- 2) In the **Time Configuration** table, in the **Static Time Zone** field, specify the time zone in which the Mediatrix unit is located.

Note: If preceded by a minus sign (-), the time zone is east of the prime meridian, otherwise it is west, which can be indicated by the preceding plus sign (+). For example, New York time is GMT 5.

- 3) Click **Apply**.

Result

Any DGW parameter referring to a time value will use the local time described by this time zone reference. The **Hoc.SystemTime** will return the unit local time in accordance with the configured time zone.

Enabling TLS Debugging on Wireshark

Before you start

To configure Wireshark for TLS packet capture, the private key associated with the server certificate are needed to decrypt TLS packets.

Steps

- 1) Go to **Edit/Preferences**.
- 2) Click + next to **Protocols**.
- 3) Select SSL.
- 4) Fill the **RSA keys list** field.

Note: The field specifies the binding between an IP address, a port, a protocol, and a RSA decryption key. Enter the IP address of the server, the SIP port, and the path to the file containing the server private key. Several such bindings may be specified by separating them with a semi-colon ";".

- 5) Start the Wireshark capture.

Note: TLS sessions using Diffie-Hellman based ciphers (DHE, ECDH, ECDHE) cannot be decrypted by Wireshark.

- 6) Restart the SipEp service on the Mediatrix unit or restart the unit.
- 7) Once the unit is restarted and the "Ready" LED is lit on the Mediatrix unit, stop the packet capture.
- 8) Using the "ssl" filter in the capture should show the SIP packets between the two endpoints.

Result

No.	Time	Source	Destination	Protocol	Info
757	15.	192.168.120.12	192.168.120.11	TLSv1	Application Data
759	15.	192.168.120.11	192.168.120.12	TLSv1	Application Data
783	15.	192.168.120.12	192.168.120.11	TLSv1	Application Data
832	15.	192.168.120.11	192.168.120.12	TLSv1	Application Data
862	15.	192.168.120.12	192.168.120.11	TLSv1	Application Data
889	16.	192.168.120.12	192.168.120.11	TLSv1	Application Data
895	16.	192.168.120.11	192.168.120.12	TLSv1	Application Data
956	16.	192.168.120.11	192.168.120.12	TLSv1	Application Data
1024	16.	192.168.120.12	192.168.120.11	TLSv1	Encrypted Alert
1025	16.	192.168.120.11	192.168.120.12	TLSv1	Encrypted Alert
1297	18.	192.168.120.12	192.168.120.11	SSL	Client Hello
1300	18.	192.168.120.11	192.168.120.12	TLSv1	Server Hello, Certificate, Server Hello Done
1303	19.	192.168.120.12	192.168.120.11	TLSv1	Client Key Exchange, Change Cipher Spec, Finished
1305	19.	192.168.120.11	192.168.120.12	TLSv1	Change Cipher Spec
1306	19.	192.168.120.11	192.168.120.12	TLSv1	Finished
1329	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1349	19.	192.168.120.11	192.168.120.12	SIP	Status: 401 Unauthorized (0 bindings)
1381	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1405	19.	192.168.120.11	192.168.120.12	SIP	Status: 401 Unauthorized (0 bindings)
1424	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1473	19.	192.168.120.11	192.168.120.12	SIP	Status: 200 OK (2 bindings)
1514	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1556	19.	192.168.120.11	192.168.120.12	SIP	Status: 200 OK (2 bindings)

File: "C:\DOCUME~1\magagne\LOCALS~1\Temp\wireshark\XXXXa18584" 1520 KB 00:00:24 Packets: 1848 Displayed: 23 Marked: 0 Dropped: 0

Selecting the SIP TLS Server Certificate Security Level

Information

The security level used to validate the TLS server certificate has no effect on the TLS client authentication when the unit is acting as a TLS server. Refer to the [SipEp.InteropTlsClientAuthenticationEnable](#) parameter.

Only the setting for SIP over TLS transport is available over the Web GUI. For others, like file transfer or TR-069, settings are available with the script. And the levels of support are different. SIP over TLS security level has one more level (Trusted Certificate level) which other services do not have.

Steps

- 1) Go to **SIP/Interop**.
- 2) In the **TLS Interop** table, select the security level used to validate certificates.

Advanced Parameters

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**

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