



SIP Transport

All Mediatrix Units

DGW 49.2.2941

2023-08-09

Table of Contents

Basic Concepts	3
Important Information to Know Before Configuring SIP Transport	3
Basic Tasks	4
Preparing the Unit to Use TLS for SIP	4
Selecting the Unit's Time Zone	4
Enabling TLS Transport for SIP	5
Enabling UDP Transport for SIP	5
Enabling TCP Transport for SIP	5
Configuring SIP Transport Parameters	6
Advanced SIP Transport Parameters	7
Online Help	8
DGW Documentation	9
Copyright Notice	10

Basic Concepts

Important Information to Know Before Configuring SIP Transport

- For SIP signaling, UDP and TCP are mutually exclusive with TLS. Activating TLS automatically disables these unsecure protocols.
- The TLS Persistent Connections Status table is not displayed if the TLS transport is not activated.
- Secure transport (TLS) requires to:
 - Synchronise the time in the unit (Refer to [Selecting the Unit's Time Zone](#) (p.4)).
 - Install the security certificates used to authenticate the server to which you will connect. Refer to [Technical Bulletin - Using Trusted CA and Host Certificates](#) published on the [Media5 Documentation Portal](#).
 - Configure the unit so that a “transport=tls” parameter is added to the Contact header of your SIP requests. (**SIP/Transport/General Configuration** table, **Add SIP Transport in Contact Header**).

If secure media (SRTP) is used, it is highly recommended to also use secure SIP signaling (TLS), otherwise the security of the media could be easily compromised by an attacker looking at the SIP signaling.

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.4)

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**.

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 Transport for SIP

Before you start

A TLS certificate must be installed on the Mediatrix unit.

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **Protocol Configuration** table, set **TLS** to **Enable**.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. Once TLS is **enabled**, all configured gateways will use TLS, and all other protocols will be disabled.

- 3) Click **Apply**.

Enabling UDP Transport for SIP

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **Protocol Configuration** table, set **UDP** to **Enable**.

IMPORTANT: The unit does not support a mix of both TLS and non-TLS links. If TLS is enabled and you want to enable UDP, you must first disable TLS. This will apply to all gateways.

- 3) Click **Apply**.

Enabling TCP Transport for SIP

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **Protocol Configuration** table, set **TCP** to **Enable**.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. If TLS is enabled and you want to enable TCP, you must first disable TLS. This will apply to all gateways.

- 3) Click **Apply**.

Configuring SIP Transport Parameters

Before you start

Some servers implementation may require to explicit the transport type in the SIP Contact header. If that's the case, see the following steps.

Steps

- 1) Go to **SIP/Transport**.
- 2) Enable one or both of the **Add SIP Transport in Registration** or **Add SIP Transport in Contact Header** parameters, depending on what is required.
- 3) **Apply**.

Result

In the following example, the transport parameter is added in the Contact header of the REGISTER request and includes the supported transport (UDP, TCP or TLS) for that gateway.

General Configuration		
Add SIP Transport in Registration:	Enable ▾	
Add SIP Transport in Contact Header:	Enable ▾	
Persistent Base Port:	16000	
Failback Interval:	15	
TLS Certificate Trust Level:	Locally Trusted ▾	
TCP Connect Timeout:	127	
Add rport:	Disable ▾	

Advanced SIP Transport 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 configuration parameters by either :

- 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](#).

- To set transport TLS Cipher Suite settings: refer to the [DGW Configuration Guide - Transport Layer Security](#) document published on the Media5 documentation portal.
- To set whether or not the unit uses the symmetric source port feature when Sending SIP traffic over UDP: **SipEp.InteropSymmetricUdpSourcePortEnable**.
- To set TLS authentication: refer to the [DGW Configuration Guide - Transport Layer Security](#) document published on the Media5 documentation portal.
- To set whether or not to force a DNS NAPTR request: **SipEp.InteropForceDnsNaptrInTls**.
- To set the proper SIP failover conditions: **SipEp.defaultSipFailoverConditions** and **SipEp.GwSpecificFailover.SipFailoverConditions**.
- To select the SIP gateway on which failover conditions will be applied: **SipEp.gwSpecificFailover.EnableConfig**.
- To set the failover conditions on a specific gateway: **SipEp.gwSpecificFailover.SipFailoverConditions**.
- To set the persistent port interval: **SipEp.TransportPersistentPortInterval**.

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