

Securing a Mediatrix Unit
All Mediatrix Units

DGW 49.2.2941
2023-08-09

Table of Contents

Management Interfaces	3
Associating the Network Interface to the System Management Services	3
Stopping Services - Web Interface	3
Securing SNMP Interface	3
Forcing the Use of HTTPS	4
SIP	5
Configuring the Local Firewall	5
Enabling TLS Transport for SIP	6
Enabling Secure Media (SRTP) on All Endpoints	6
Enabling Secure Media (SRTP) on a Specific Endpoint	8
Configuration Files	10
Disabling DHCP Server Download	10
Configuring a Privacy Key	10
Disabling Partial Reset - ResetButtonManagement	11
Requirements	12
Online Help	13
DGW Documentation	14
Copyright Notice	15

Management Interfaces

Associating the Network Interface to the System Management Services

Steps

- 1) Go to **Management/Misc.**
- 2) From the **Network Interface** selection list, select the Network Interface you wish to bound to the system management services.
- 3) Click **Apply**.

Result

The user will access the System Management through the selected Network Interface.

Next Step

[Stopping Services - Web Interface](#) (p.3)

Stopping Services - Web Interface

Steps

- 1) Go to **System/Services**.
- 2) In the **User Service** table, click ☐ next to the service you want to disable.
- 3) Click **Apply**.

Next Step

[Securing SNMP Interface](#) (p.3)

Securing SNMP Interface

Steps

- 1) Go to **Management/SNMP**.
- 2) In the **SNMP Configuration** table, set the following parameters:
 - a) Set **Enable SNMP V1** to **Disable**.
 - b) Set **Enable SNMP V2** to **Disable**.
 - c) Set the **Privacy Protocol**.
 - d) In the **Privacy Password** field, enter a password of your choosing.
- 3) Click **Apply**.

Result

SNMP Configuration	
General Configuration	
SNMP Port:	161
SNMP Protocol	
Enable SNMP V1:	Disable
Enable SNMP V2:	Disable
Enable SNMP V3:	Enable
Authentication Protocol:	MD5
Privacy Protocol:	DES
Privacy Password:	
Community:	public
SNMP Trap	
Enable SNMP Trap:	Disable
Trap Destination(s):	192.168.10.10:162

Next Step

[Forcing the Use of HTTPS \(p.4\)](#)

Forcing the Use of HTTPS

Steps

- 1) Open CLI (Command Line Interface).
- 2) Set **Web.HttpMode** to **Secure**.

Result

The unit will now be forced to use HTTPS.

Next Step

[Configuring the Local Firewall \(p.5\)](#)

SIP

Configuring the Local Firewall

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Rules** table, complete the fields as required.
- 3) In the **Local Firewall Configuration** table, from the **Default Policy** selection list, select **Drop**.

IMPORTANT: Before setting the **Default Policy** to **Drop**, i.e. to apply the local firewall rules and to drop any incoming call that does not match a rule, review your rules to make sure that at least one rule accepts incoming packets for management, otherwise the communication with the Mediatrix Sentinel will be lost.

Note: For example, if the Web interface is used for management (HTTP port 80) via the unit's LAN interface (default IP address = 192.168.0.10), then the following rule could be added: **Activation=Enable / Destination Address=192.168.0.10 / Destination port=80 / Protocol=TCP / Action=Accept**

Note: For blacklisting to be used, at least one firewall rule must have the **Black listing enable** box checked.

Note: Before setting the **Default Policy** to **Drop**, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mediatrix Sentinel will be lost.

- 4) Click **Save**.



Caution: Take the time to carefully review your rules before continuing to the next step.

- 5) Click **Save & Apply** to apply all changes to the configuration.
- 6) Click **restart required services**, located at the top of the page.

Result

The Local Firewall will drop packets without any notification message.

If a rule with the **Black listing enable** box checked matches a packet and no **Rate Limit Value** was set, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration of the **Blacklist Timeout**.

If a rule with the **Black listing enable** box checked matches a packet and the **Rate Limit Value** has been reached, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration set for the **Blacklist Rate Limit Timeout**.

Next Step

[Enabling TLS Transport for SIP](#) (p.6)

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**.

Next Step

[Enabling Secure Media \(SRTP\) on All Endpoints](#) (p.6)

Enabling Secure Media (SRTP) on All Endpoints

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose **Default**.

3) In the **Security** table,

- a) From the **Mode** drop box, select **Secure** or **Secure with fallback**.
- b) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDES** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDES** protocol will add the **a=crypto** line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the **a=key-mgmt:mikey** line within the SDP Session Attributes.

- c) From the drop box, select the **AES_CM_128** encryption algorithm.
- d) From the **Allow Unsecure T.38 with Secure RTP** selection, choose if unsecure **T.38** is allowed with RTP.

Note: **T.38** packets will never be encrypted. The setting **Allow Unsecure T.38 with Secure RTP** will make possible to use **T.38**, otherwise it will be rejected. If not using **T.38** for faxing, to avoid an impact on the number of simultaneous calls a Mediatrix unit can handle in SRTP, set the **Allow Unsecure T.38 with Secure RTP** parameter to **No** and refer to the [Standard Fax Configuration](#) document to disable **T.38** Fax Transmission.

4) In the **SRTP Preferences** table,

- a) From the **Crypto Mode When Sending Offer** drop box, select the preferred mode.
- b) From the **Crypto Mode When Sending Answer** drop box, select the preferred mode.
- c) From the **Crypto Context Behavior** drop box, select the preferred behavior.

Note: For more information about the recommended **SRTP Preferences**, please refer to [Recommended SRTP Preferences for a Typical VoIP Network](#) section of the [Setting the Security Parameters of the RTP Stream](#) document.

Note: For troubleshooting the SRTP interoperability, please refer to the [SRTP Troubleshooting](#) document.

5) Click **Apply**.**Result**

All new SIP exchanges will contain RTP/SAVP negotiation elements.

Select Endpoint: Default ▾

Security	
RTP	
Mode:	Secure ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾
T.38	
Allow unsecure T.38 with secure RTP:	No ▾

SRTP Preferences	
Crypto Mode When Sending Offer:	Mode when sending SDP offer with SRTP ▾
Crypto Mode When Sending Answer:	Mode when sending SDP answer with SRT ▾
Crypto Context Behavior:	Behavior of the SRTP Context ▾

Next Step[Disabling DHCP Server Download](#) (p.10)

Enabling Secure Media (SRTP) on a Specific Endpoint

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose an endpoint.

Note: The list of available endpoints will vary depending on the type of unit being used.

- 3) In the **Security** table, from the **Mode** drop box, select **Secure** or **Secure with fallback**.
- 4) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDS** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDS** protocol will add the a=crypto line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the a=key-mgmt:mikey line within the SDP Session Attributes.

- 5) From the drop box, select the **AES_CM_128** encryption algorithm.
- 6) Click **Apply**.

Result

All new SIP exchanges going through the specified endpoint will contain RTP/SAVP negotiation elements.

Select Endpoint: Chosen Endpoint 

Security	
RTP	
Endpoint Specific:	Yes 
Mode:	Secure 
Key Management Protocol:	Key Management Protocol for SRTP 
Encryption:	AES_CM_128 

Configuration Files

Disabling DHCP Server Download

Steps

- 1) Go to **Management/Configuration Scripts**.
- 2) In the **Automatic Script Execution** table, set **Allow DHCP to Trigger Scripts Execution** to **Disable**.
- 3) Click **Apply**.

Result

Ensures that no one can send a new configuration file to the unit if the DHCP server is compromised.

Automatic Script Execution		
Execute On Startup:	Disable	
Execute Periodically:	Disable	
Time Unit:	Hours	
Period:	1	
Time Range:		
Allow DHCP to Trigger Scripts Execution:	Disable	

Next Step

[Configuring a Privacy Key \(p.10\)](#)

Configuring a Privacy Key

Steps

- 1) Go to **Management > Configuration Scripts**.
- 2) In the **Execute Scripts** table, set a privacy key of your choosing in the **Privacy Key** field.

Result

The unit will only accept scripts that have been encrypted with this privacy key. The privacy key also ensures that the files are encrypted when using unsecure transfer mode (HTTP,TFTP,FTP).

Next Step

[Disabling Partial Reset - ResetButtonManagement \(p.11\)](#)

Disabling Partial Reset - ResetButtonManagement

Steps

- 1) Open CLI (Command Line Interface).
- 2) Set **ResetButtonManagement** to **DisablePartialReset**.

Result

The Mediatrix unit will no longer partially reset the unit.

Requirements

CLI

Make sure the Telnet access is disabled. You can look at the `Cli.EnableTelnet` variable to verify if Telnet connections are allowed. The access is disabled by default.

Additional considerations

- In the initial configuration of the unit, review the users and change their passwords and access rights according to your security policy.
- On FXS devices, the Vocal Unit Information allows a caller on an FXS port to dial codes to get information on the unit like the IP addresses and the MAC address. It is recommended to turn this feature off to prevent attackers from gaining information on the Mediatrix unit setup.

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