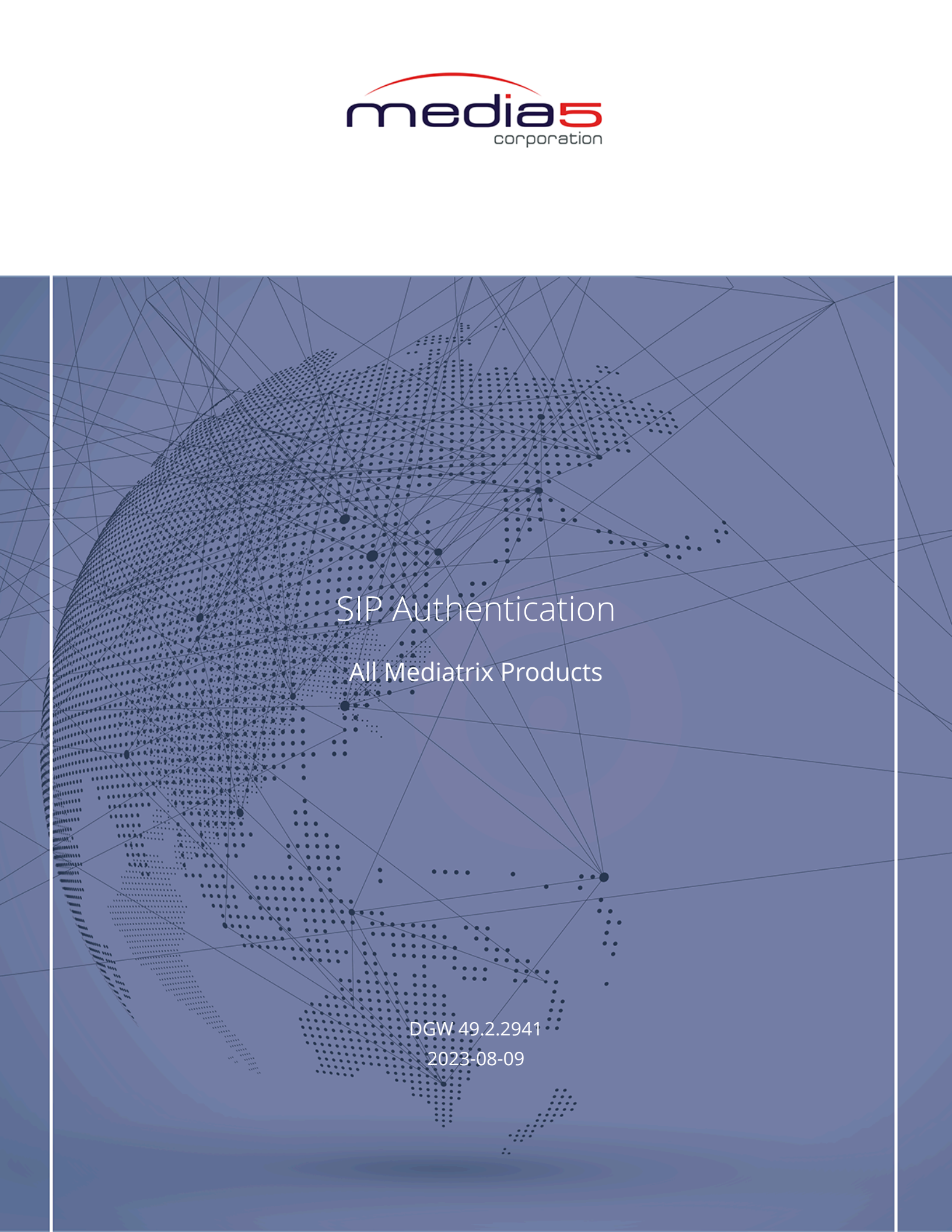


The background of the slide is a dark blue gradient with a complex, abstract graphic. It consists of a dense network of thin, light blue lines connecting numerous small, dark blue dots. These dots are arranged in a way that suggests a global map, with higher concentrations of dots in the Americas and Europe. The overall effect is a sense of global connectivity and data flow.

SIP Authentication

All Mediatrix Products

DGW 49.2.2941
2023-08-09

Table of Contents

Basic Concepts	3
SIP Authentication	3
Important Information To Know before Using Sip Authentication	4
Authentication Table Entries - Order is Important	4
Basic Tasks	8
Defining Authentication Credentials for a Gateway	8
Defining Authentication Credentials for an Endpoint	9
Defining Authentication Credentials for the Unit	9
Defining Authentication Credentials for a Username	10
Selecting the Priority Level of an Authentication	11
Erasing Authentication Credentials	11
Online Help	12
DGW Documentation	13
Copyright Notice	14

Basic Concepts

SIP Authentication

SIP authentication is a security feature that allows a SIP server to validate the authenticity of the sender, and to accept only the requests when they have the proper credentials.

To authenticate a SIP request, the server issues an authentication challenge to which the SIP client must respond with the proper username/password credentials. The Mediatrix unit can be configured with the authentication information needed to respond to the authentication challenges issued by SIP servers.

The authentication information is configured in the **Authentication** table. Each entry of the table has a **Criteria** and a **Realm**, if it is enabled, that define when it is appropriate to use this entry.

There are 4 criteria categories:

- **endpoint-specific:** Applies only to challenges received for SIP requests related to a specific endpoint. For instance, the registration associated with the endpoint in the user agent table or the INVITE sent to initiate a call from the endpoint.
- **gateway-specific:** Applies only to challenges received for SIP requests on a specific SIP gateway.
- **user-name specific:** Applies only to challenges for a context that uses a specific user name.
- **global to the whole unit:** Applies to all challenges received for SIP dialogs. The defined user names and passwords will apply to all the endpoints of the unit.

IMPORTANT: If authentication credentials are required for several realms, create a separate table entry for each realm.

The **Authentication** table may have between 20 and 100 rows. If you have less than 20 rows, the Mediatrix unit automatically adds new rows up to the minimum of 20.

When a challenge occurs (either 401 Unauthorized or 407 Proxy Authentication Required), the first entry in the **Authentication** table having a criteria that matches the challenge is used to reply to the challenge. The username and password of a criteria can be configured in the Web interface in the **SIP/Authentication/ Authentication** table. The entries of the **Authentication** table are tried from the first row to the last row. To have a match, the realm in the **Authentication** table entry must match the realm in the challenge or the **Validate Realm** field of the entry must be set to **Disable**. For each entry matching certain criteria (described below), the challenge is replied with the entry's user name and password. If authentication fails, the SIP server may issue another authentication challenge, provided it has been configured to do so. (Because of the increased risks of hacking, servers usually give only a single chance). In that case, the next entry in the table having a matching criteria is used to reply to this new challenge. This can be repeated until no more matching entry is found. If no entry matches the criteria, the authentication fails. To match the authentication request, the entry must also meet one of the following criteria:

- The challenge needs to be for a SIP request related to the endpoint specified in the **Endpoint** column if the corresponding **Criteria** column is set to **Endpoint**.
- The challenge needs to be for a SIP request performed on the SIP gateway specified in the **Gateway** column if the corresponding **Criteria** column is set to **Gateway**.
- The challenge needs to be for a context that uses the user name specified in the **User Name** field if the corresponding **Criteria** column is set to **username**. The user name associated with a context is:
 - the user name of the FROM if the context sent the original SIP request, or
 - the user name of the request URI if the context received the original SIP request
- The challenge applies to a unit if the corresponding **Criteria** column is set to **Unit**.

Important Information To Know before Using Sip Authentication

Access Rights

The **SIP /Authentication** page is not accessible if you have the User or Observer access right.

Naming

The SIP username (i.e. the one in the username criteria) is checked against SIP username syntax of RFC3261.

Authentication

The **Authentication** table (under **SIP /Authentication**) may have between 20 and 100 rows. If you have less than 20 rows, the Mediatrix unit automatically adds new rows up to the minimum of 20.

Authentication Order

The order of the tried entries in the **SIP/Authentication** table is from the first row to the last row. The row sequence is important. Refer to [Authentication Table Entries - Order is Important](#) (p.4) .

Endpoint Authentication

- Several usernames/passwords can be defined for a single Endpoint.
- Endpoint Authentication can be defined for all types of endpoints i.e. E1T1/FXS/FXO/BRI/PRI.

Authentication Table Entries - Order is Important

The priority of an entry in the **Authentication** table is important. The most specific authentication credential must be set before the more generic ones, otherwise the challenges will be responded with the generic credentials rather than the specific ones. If authentication fails with the credentials found in the **Authentication** table, the SIP server may issue another authentication challenge. In that case, the next entry in the table having a matching criteria is used to reply to this new challenge. This can be repeated until no more matching entry is found.

For example

✦ Authentication

Authentication										
Priority	Criteria	Endpoint	Gateway	Username	Criteria	Validate	Realm	Realm	User Name	
1	Endpoint	Slot4/FXS1				Disable			User1	    
2	Endpoint	Slot4/FXS3				Disable			User3	    
3	Gateway		gateway_1			Disable			gw1	    
4	Gateway		gateway_2			Disable			gw2	    
5	Unit					Disable			Unit1	    

- Three gateways are defined in the **Gateway** table (under **SIP/Gateways**)
 - **gateway_1**
 - **gateway_2**
 - **gateway_3**
- The unit has 4 endpoints:
 - **Slot4/FXS1**
 - **Slot4/FXS2**
 - **Slot4/FXS3**
 - **Slot4/FXS4**
- The SIP requests related to **Slot4/FXS1**, **Slot4/FXS3**, and **Slot4/FXS4** are sent via **gateway_2**
- The SIP requests related to **Slot4/FXS2** are sent via **gateway_3**

Table 1: Scenario 1

Step	Description
1	Endpoint Slot4/FXS3 needs to register to the SIP server.
2	A SIP REGISTER request is sent to the SIP server.
3	The SIP server must authenticate the request, so it challenges the request with a 401 Unauthorized challenge response.
4	Upon reception of this challenge, the Mediatrix unit searches the Authentication table to find the first matching Criteria entry.
5	Entry #1 of the Authentication table has a Criteria that matches endpoint Slot4/FXS1 , but because the REGISTER was issued for Slot4/FXS3 , the match fails.
6	Entry #2 of the Authentication table has a Criteria that matches endpoint Slot4/FXS3 and because the REGISTER was issued for Slot4/FXS3 , the match succeeds, and the credentials of this entry are used to respond to the challenge.
7	If the credentials configured in entry #2 are good, the SIP server accepts to handle the REGISTER request.

Table 2: Scenario 2

Step	Description
1	Endpoint Slot4/FXS4 must register to the SIP server.
2	A SIP REGISTER request is sent to the SIP server.
3	The SIP server must authenticate the request, so it challenges the request with a 401 Unauthorized challenge response.
4	Upon reception of this challenge, the Mediatrix unit searches the Authentication table to find the first matching Criteria entry.
5	Entry #1 of the Authentication table has a Criteria to match endpoint Slot4/FXS1 but because the REGISTER was issued for Slot4/FXS4 , the match fails.
6	Entry #2 of the Authentication table has a Criteria to match endpoint Slot4/FXS3 but because the REGISTER was issued for Slot4/FXS4 , the match fails.
7	Entry #3 of the Authentication table has a Criteria to match gateway gateway_1 but because the REGISTER was issued via gateway_2 , the match fails.
8	Entry #4 of the Authentication table has a Criteria to match gateway_2 and because the REGISTER was issued via gateway_2 , the match succeeds, and the credentials of this entry are used to respond to the challenge.
9	If the credentials configured in entry #4 are good, the SIP server accepts to handle the REGISTER request.

Table 3: Scenario 3

Step	Description
1	Endpoint Slot4/FXS2 must register to the SIP server.
2	A SIP REGISTER request is sent to the SIP server.
3	The SIP server must authenticate the request, so it challenges the request with a 401 Unauthorized challenge response.
4	Upon reception of this challenge, the Mediatrix unit searches the Authentication table to find the first matching Criteria entry.
5	Entry #1 of the Authentication table has a Criteria to match endpoint Slot4/FXS1 , but because the REGISTER was issued for Slot4/FXS2 , the match fails.
6	Entry #2 of the Authentication table has a Criteria to match endpoint Slot4/FXS3 , but because the REGISTER was issued for Slot4/FXS2 , the match fails.
7	Entry #3 of the Authentication table has a Criteria to match gateway gateway_1 , but because the REGISTER was issued via gateway_3 , the match fails.
8	Entry #4 of the Authentication table has a criteria to match gateway gateway_2 , but because the REGISTER was issued via gateway_3 , the match fails.
9	Entry #5 of the Authentication table has a criteria to match the whole unit, so the match succeeds, and the credentials of this entry are used to respond to the challenge.
10	If the credentials configured in entry #5 are good, the SIP server accepts to handle the REGISTER request.

Basic Tasks

Defining Authentication Credentials for a Gateway

Before you start

- Administrator access rights are required to access this page.
- The **Mediatrrix** unit can support up to 5 gateways.

Steps

- 1) Go to **SIP/Authentication**.
- 2) Click  located on the first row.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click , to add a new row at the bottom of the table.

- 3) In the **Authentication** table, from the **Criteria** selection list, select **Gateway**.
- 4) From the **Gateway** selection list, select a gateway.
- 5) Enter a password and username for the gateway.

Note: You can optionally enable realm validation, if needed.

- 6) Click **Apply**.

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to the gateway specified in the **Gateway** column. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Gateway		Gateway_Name_gw		Disable		username	*****

Defining Authentication Credentials for an Endpoint

Before you start

You will not be able to access this page if you have a User or Observer access right.

Information

If different usernames/passwords are needed for different realms, use multiple table entries.

Steps

- 1) Go to **SIP/Authentication**.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click **+**, to add a new row at the bottom of the table.

- 2) Click **Edit** located on the first row.
- 3) From the **Criteria** selection list, select **Endpoint**.
- 4) From the **Endpoint** selection list, select an endpoint.
- 5) Enter a password and username for the endpoint.

Note: You can optionally enable realm validation, if needed.

- 6) Click **Apply** or **Apply and Refresh Registration**

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to the endpoint specified in the **Endpoint** column. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Endpoint	Endpoint_Name			Disable		Username	*****

Defining Authentication Credentials for the Unit

Before you start

- You will not be able to access this page if you have a User or Observer access right.

- The challenge applies to a unit if the corresponding **Criteria** column is set to **Unit**.

Steps

- 1) Go to **SIP/Authentication**.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click , to add a new row at the bottom of the table.

- 2) Click **Edit** located on the first row.
- 3) From the **Criteria** selection list, select **Unit**.
- 4) Enter a password and username for the unit.

Note: You can optionally enable realm validation, if needed.

- 5) Click **Apply** or **Apply and Refresh Registration**

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to any gateway or endpoint of the unit. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Unit				Disable		Username	*****

Defining Authentication Credentials for a Username

Before you start

You will not be able to access this page if you have a User or Observer access right.

Steps

- 1) Go to **SIP/Authentication**.

Note: By default, 20 unconfigured entries are included in the **Authentication** table. If the first 20 entries are configured, click , to add a new row at the bottom of the table.

- 2) Click  located on the first row.
- 3) From the **Criteria** selection list, select **User Name**.
- 4) In the **Username Criteria**, enter the name of a username.
- 5) Enter a password and username for the username.

Note: You can optionally enable realm validation, if needed.

- 6) Click **Apply** or **Apply and Refresh Registration**

Result

The username and password will be used to respond to authentication challenges received for SIP requests related to a specific username. If they do not match the specified credentials, the communication will fail.

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Username ▾	▾	▾	UserName1	Enable ▾		UserName	*****

Selecting the Priority Level of an Authentication

Steps

- 1) Go to **SIP/Authentication**.
- 2) Use the arrows to move an authentication entry up or down the table.

Note: Search is performed from the first entry of the table down to the last.

- 3) Click **Apply** or **Apply and Refresh Registration**

Result

The Authentication table will be searched in the selected order to find which credentials to use.

Erasing Authentication Credentials

Before you start

Administrator access rights are required to access this page.

Steps

- 1) Go to **SIP/Authentication**.
- 2) Click  located at the end of the row containing the credential to erase.
- 3) Click **Refresh Registration**.

Result

The entry will be permanently erased from the unit.

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