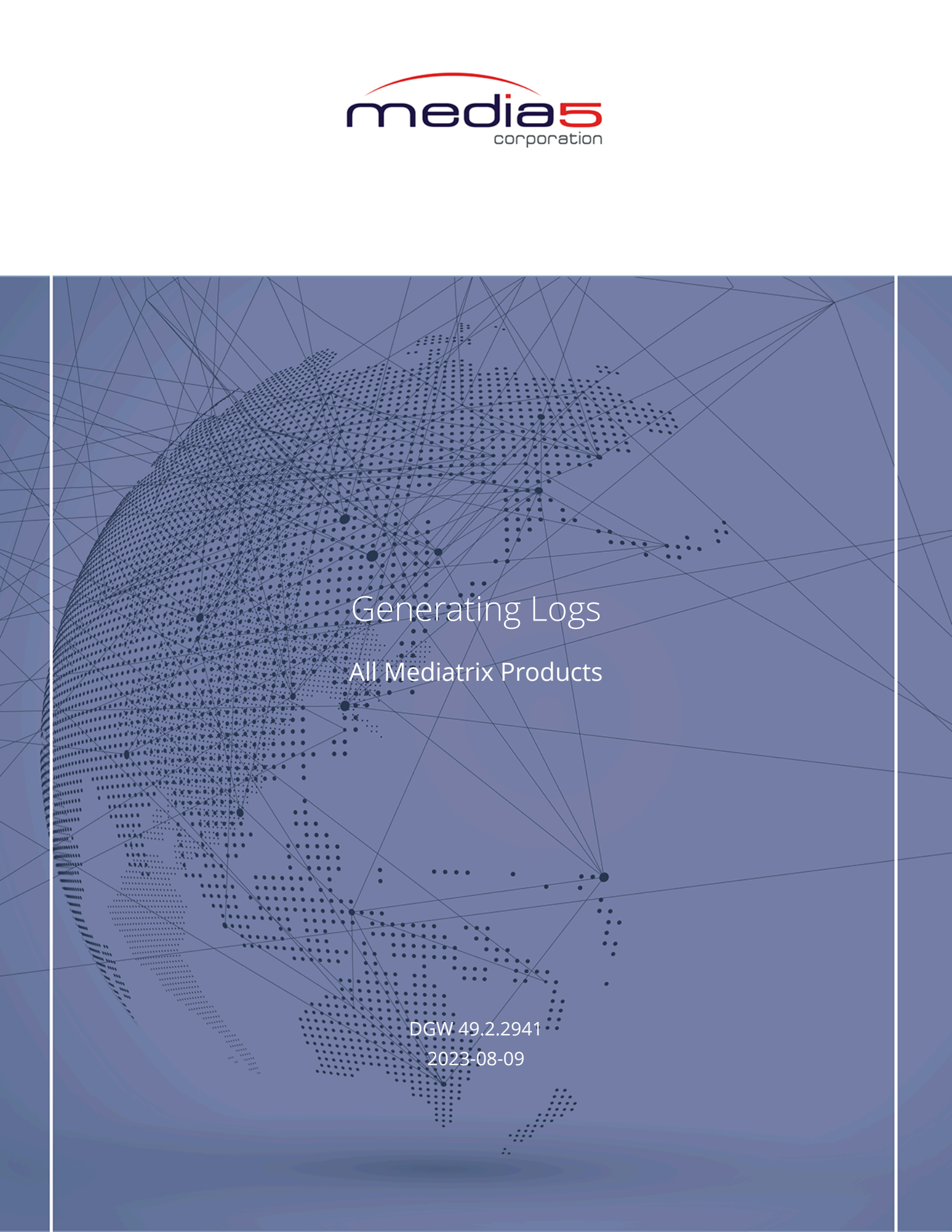


The background of the slide is a dark blue gradient with a complex, abstract graphic. It features a network of thin, light blue lines connecting various points, creating a web-like structure. Overlaid on this is a large, semi-transparent globe or sphere composed of a dense grid of small dots. The globe is tilted and appears to be part of the network structure.

Generating Logs

All Mediatrix Products

DGW 49.2.2941
2023-08-09

Table of Contents

Event Notifications	4
Logging Event Notifications	4
Logging Specific Event Notifications	5
Destinations for Event Notifications	7
Send via Syslog	7
Send via SIP	7
Log Locally	7
Log to File	8
Send via SNMP	8
Diagnostic Traces	9
Logging Diagnostic Traces	9
Basic tasks	10
Clearing the Local Logs	10
Updating the Local Logs	10
Disabling Event Notification Reporting for a Service	10
Modifying the Severity Level Triggering the Reporting of a Notification	10
Command Line Interface (CLI)	12
Advanced Log Parameters	12
Online Help	13

Table of Contents

DGW Documentation	14
Copyright Notice	15

Event Notifications

An event is something that happens in the system and that needs to be reported. Event notifications are formatted text messages issued by the DGW software to signal something of interest to the unit administrator.

Event Notifications are used to generate alarms in the customer's system and to monitor the system. It is possible to control:

- for which service event notifications will be reported;
- which event notifications will be reported based on the severity level of the event;
- if a specific event notification should be reported or not;
- where the event notifications will be logged.

For example, it is possible to log all event notifications raised for the Call Router (Crout) service, or to log only one specific event notification for the Certification (Cert) service.

IMPORTANT: Unit performance is affected by the quantity of events that are reported.

Event Notifications can be sent to different destinations to be logged:

- Internal destination
 - [Log to File](#) (p.8) to a file in the DGW File management system (not available on the 4102S and the Mediatrix C7 series).
 - [Log Locally](#) (p.7) to the [Local Logs](#) page of the DGW Web interface.
- External destination
 - to a [SIP server via NOTIFY](#).
 - to a [Syslog](#) server via syslog transport.

Logging Event Notifications

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, click + located next to **Services**.
- 3) For each service, choose the **Severity** level that will trigger the notifications.

Note: if you do not wish to log the event notifications of a service, select **Disable**.

Note: At this point, you have only enabled the possibility to log event notifications.

- 4) In the **Criteria** field, enter **All**.

- 5) From the **Action** drop-down list, select where and how the event notifications will be logged.
 - a) Choose [Log Locally](#) (p.7) to display the event notifications in the Local Log.
 - b) Choose [Log to File](#) (p.8) to send the event notifications to the DGW file management system (not available on the Mediatrix 4102S and C7 Series).
 - c) Choose [Send via Syslog](#) (p.7) to send the event notifications to a Syslog server.
 - d) Choose [Send via SNMP](#) (p.8) to send the event notification via the SNMP transport.

Note: You cannot choose **Send Via SIP** if you wish to log all event notifications, as this may overload the SIP gateway. The system will indicate **Not Supported**.

- 6) If you selected [Send via Syslog](#) in the previous step, make sure you have configured the address of the syslog server under **Syslog Configuration/Remote Host** field.
- 7) Click [+](#).
- 8) Click **Apply**.

Result

All event notifications with the appropriate selected **Severity** level of each selected service will be logged to the chosen destination.

Notification Events							
#	Activation	Criteria	Service	Notification	Action	Config Status	
1	Enable ▾	All	Service ▾	--- Suggestion --- ▾	Send Via Syslog ▾	Valid	-
3	Enable ▾	All	Service ▾	--- Suggestion --- ▾	Send Via SIP ▾	Valid	-
4	Enable ▾	All	Service ▾	--- Suggestion --- ▾	Send Via SNMP ▾	Valid	-
5	Enable ▾	All	Service ▾	--- Suggestion --- ▾	Log Locally ▾	Valid	-
6	Enable ▾	All	Service ▾	--- Suggestion --- ▾	Log To File ▾	Valid	-
							+

Logging Specific Event Notifications

Information

Instead of logging all the event notifications, as specified in [Logging Event Notifications](#), the **Criteria** can be refined to a subset of events.

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, click + located next to **Services**.
- 3) From the **Severity** drop-down list, for each service, choose the severity level that will trigger the notification.

Note: If you do not wish to log the event notifications of a service, select **Disable**.

Note: At this point, you have only enabled the possibility to log event notifications.

- 4) In the **Notification Events** table, select a **Service** for which Event Notifications must be issued.
- 5) From the **Notification** drop-down list, select one, or several, specific service notifications you wish to log.

Note: The **Criteria** field will be auto populated with the selection made in the **Notification** field.

Note: To log all the notifications of a specific service enter in the **Criteria** field the service code with all separated by a coma. For example: 200.all to log all the notifications of the Bni service. (The code can be found in the **Service** drop-down list.)

- 6) From the **Action** drop-down list, select where and how the event notifications will be logged.
 - a) Choose [Log Locally](#) (p.7) to display the event notifications in the Local Log.
 - b) Choose [Log to File](#) to send the event notifications to the DGW file management system. (not available on the Mediatrix 4102S and C7 Series).
 - c) Choose [Send via Syslog](#) (p.7) to send the event notifications to a Syslog server.
 - d) Choose [Send via SIP](#) (p.7) to send the event notifications to a SIP server.
- 7) This step is not necessary if you chose **Log To File** in the previous step. In **Syslog Configuration** table, in the **Remote Host** field, enter the IP address of the server.
- 8) Click **+**.
- 9) Repeat steps 4 to 7 for each notification you wish to publish.
- 10) Click **Apply**.

Result

The selected service notifications with the corresponding **Severity** level will be published to the selected destination.

Notification Events							
#	Activation	Criteria	Service	Notification	Action	Config Status	
1	Enable	Criteria of chosen notification	Service	Choose Notification	Log Locally	Valid	-
2	Enable	Criteria of chosen notification	Service	Choose Notification	Send Via SIP	Valid	-
3	Enable	Criteria of chosen notification	Service	Choose Notification	Send Via Syslog	Valid	-
4	Enable	Criteria of chosen notification	Service	Choose Notification	Log To File	Valid	-
			--- Suggestion ---				+

Destinations for Event Notifications

Send via Syslog

Event notifications can be logged by a Syslog server.

The event notifications will be sent over UDP in the syslog format, to the syslog server specified in the configuration. Alternatively, the syslog server address can be provided through DHCP. It is important to understand that if no syslog server address is provided by a DHCP server or specified by the administrator, no messages are sent.

IMPORTANT: In some cases, Mediatrix devices can generate more information than the syslog server can handle. In these cases, it is preferable to capture the information with Wireshark.

Send via SIP

It is possible to send the event notifications to a SIP server.

The event notifications sent to a SIP server are included in the SIP Notify messages. When choosing to send event notifications to a SIP server, it is not allowed to send all notifications, i.e. select the **All** criteria when configuring event notifications. This has been implemented to avoid sending high volumes of traffic and risking the overload of the SIP server.

The destination can be configured with the **sipEp.sipNotificationsGateway** parameter and the **sipEp.maxNotificationsPerNotify** parameter is used to define how many messages can be sent in a single "SIP NOTIFY" request the

For more details, refer to [DGW Configuration Guide - Reference Guide](https://documentation.media5corp.com) published on the Media5 documentation portal at <https://documentation.media5corp.com>

Log Locally

The DGW Local Log displays the Event Notifications related to the events occurring on the Mediatrix unit that are generated by the Mediatrix Notifications and Logging Manager (Nlm) service.

Notifications will be displayed in the **Local Log Entries** table of the DGW Web interface provided the issuing of events for a service is enabled, and if the event meets the selected severity level chosen to be reported.

The **Local Log Entries** table has the following characteristics:

- Number of displayed event notifications is limited
- Newer notifications replace older ones.

- The routing criteria should be designed to avoid overloading the log.
- The local log has no persistence. Its content is erased when the unit or the Nlm service is restarted.
- The local log does not accept messages from the SNMP service with a 'Debug' severity level. This is to prevent an issue when reading the local log with SNMP. The SNMP walk through the table would not catch up with the increasing index because of the DEBUG events generated by the SNMP service itself.

Log to File

The event notifications can be logged in a file saved in the DGW File Management system.

Event notifications logged to a file will be available in the DGW Web interface, under **Management/File** tabs. The log to file feature is not available on the Mediatrix 4102S and C7 Series as they do not have more than 1MB or more user storage. The number of files stored in the unit is limited. When the maximal number is reached, the oldest stored file is deleted. The limit is configured in the **LogFileMaxNb** Mib parameter.

Send via SNMP

The event notification can be sent via the SNMP transport.

The Send via SNMP entries have the following characteristics:

- The traps will be sent according to the Trap Destination(s) and SNMP Protocols configured in the Management/SNMP tab of the unit.
- By default, Notifications are only sent at severity level Warning or higher. This means you will only get traps in case of an error. To also get the recovery events for a particular service, set its severity to « Info » in System/Event Log/Service Notification Configuration.
- For SNMP traps, the notification queue is limited to 100 notifications per second for bandwidth limitation purposes.
- Newer traps replace older ones.
- The routing criteria should be designed to avoid overloading the queue

Diagnostic Traces

Diagnostic Traces are specifically used for troubleshooting purposes. As for Event Notifications, they report errors, warnings, or system information.

Diagnostic Traces do not need to be activated, except at the specific demand of Media5 Technical Assistance Center.

Logging Diagnostic Traces

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Remote Host** field, enter the static IP address or domain name and port number of the device that archives the log entries sent by syslog transport.

Note: Specifying no port, or port 0, sends notifications to port 514.

- 3) From the **Diagnostic Traces** field, select **Enable**.
- 4) Click **Edit**.
- 5) In the **Diagnostic Traces** table, select the level of severity an event should have to be reported by the syslog.

IMPORTANT: Enabling all the traces will reduce the performance of the Mediatrix unit and may cause it to no longer respond.

- 6) Click **Apply**.
- 7) Click **Apply** again.

Result

The traces generated by the Mediatrix unit with the selected severity level, will be sent to the specified address.

Syslog Configuration	
Remote Host:	IP address
Technical Assistance Centre	
Diagnostic Traces:	Enable ▾
Filter:	Edit

Basic tasks

Clearing the Local Logs

Steps

- 1) Go to **System/Local Log**.
- 2) Click **Clear Local Log**.

Result

The entries in the **Local Log Entries** table will be permanently deleted.

Updating the Local Logs

Steps

- 1) Go to **System/Local Log**.
- 2) Click **Refresh Local Log**.

Result

All new entries generated by the Notifications and Logging Manager (NLM) of your Mediatrix unit will be displayed in the **Local Log Entries** table.

Disabling Event Notification Reporting for a Service

Steps

- 1) Go to **System/Event Log**.
- 2) In the **Service Notification Configuration** table, from the drop-down list located next to a service name, select **Disable**.

Result

No event notifications will be issued for the service.

Modifying the Severity Level Triggering the Reporting of a Notification

Steps

- 1) Go to **System/Event Log**.

- 2) In the **Service Notification Configuration** table, from the drop-down list located next to a service name, select the severity level an event should have to issue a notification.

Result

Notifications will be issued for the service only if the severity level matches the selection.

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.

Advanced Log Parameters

When using the [Send via Syslog](#) destination the following CLI parameters can be used:

- **sipEp.sipNotificationsGateway** to define the gateway that will be used.
- **sipEp.maxNotificationsPerNotify** to define how many messages can be sent in a single "SIP NOTIFY" request.

When using the [Log to File](#) destination, the following CLI parameter can be used:

- **LogFileMaxNb** to set the maximum number of files stored in the file management system.

For complete details on parameters, refer to the [DGW Configuration Guide - Reference Guide](#) published on the [Media5 Documentation Portal](#).

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