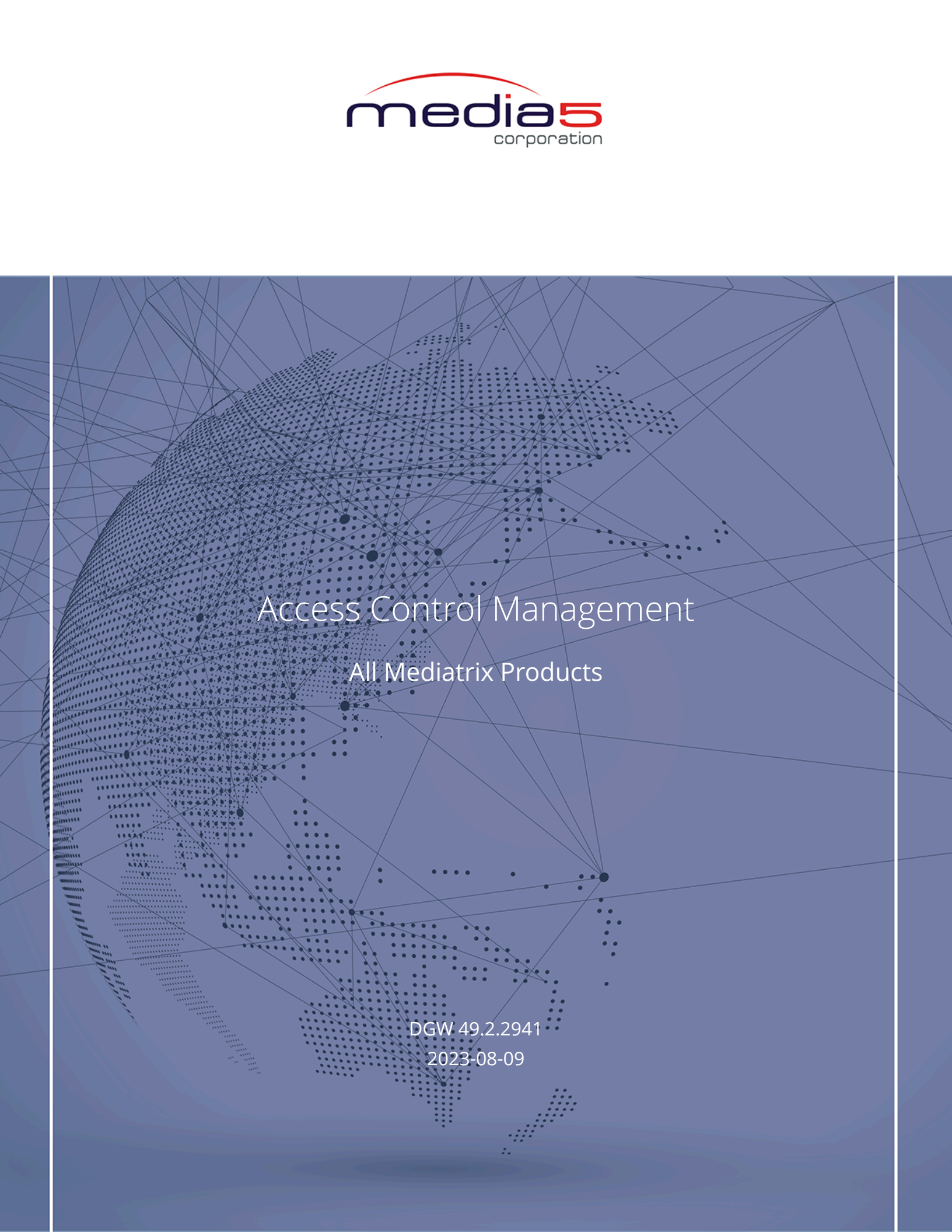


The background of the slide is a dark blue gradient. It features a complex, abstract graphic of a globe or sphere on the left side, composed of a dense grid of small dots. A network of thin, light blue lines connects various points across the entire slide, creating a web-like pattern that suggests global connectivity or data flow.

Access Control Management

All Mediatrix Products

DGW 49.2.2941

2023-08-09

Table of Contents

Basic Concepts	3
Important Information	3
Access Right Permissions	3
Protection Against Brute Force Login Attempts	4
Service Access Control Type	4
Radius Servers used For Authentication	4
Radius Servers used For Accounting	4
Basic Tasks	6
Adding a User to DGW	6
Changing the Rights of a DGW User	6
Changing the Login Password	7
Deleting a User from DGW	7
Protecting User Accounts Against Brute Force Attacks	8
Setting the Access Control Type of the CLI Service	8
Setting the Access Control Type of the Snmp Service	9
Setting the Access Control Type of the Web Service	10
Advanced Access Control Parameters	12
Online Help	13
DGW Documentation	14
Copyright Notice	15

Basic Concepts

Important Information

- The **Management/Access Control** page is only accessible if you have **admin** Access Rights.
- A maximum of 10 users can be added in the **Users** table.
- When a partial reset is triggered,
 - the default accounts are restored, with their default values and access rights.
 - the Radius authentication is disabled.
- The password is case sensitive. All characters are allowed.
- The username is case sensitive.
- The Mediatrix unit's Radius server settings do not support IPv6.

Access Right Permissions

Access Right	Observer	User	Admin
Read Configuration Parameters	√	√	√
Modify Configuration Parameters		√	√
Read/Write Passwords, Secrets, Secret Keys			√
Change Access Rights			√
Execute Configuration Scripts		√	√
Export Configuration		√	√
Backup/Restore Configuration			√
Firmware Updates and Rollback			√

Protection Against Brute Force Login Attempts

Mediatrix units have a protection against brute force login attempts.

When this protection is enabled, a user account is temporarily locked after repetitive login failures. The protection is enabled by default. The maximum number of login attempts before locking the user's account and the duration of the lock are configurable.

Service Access Control Type

It is possible to define the type of authentication and accounting to use for the CLI, SNMP, and Web services. In other words, it is possible to decide if authentication or accounting requests are sent to a RADIUS server or validated against the username and password stored locally in the **Users** table of DGW.

- Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted.
- Accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session.

Radius Servers used For Authentication

A radius server can be used for Authentication for the CLI and the Web services

The first authentication attempt is sent to the Radius server with the highest priority. When authentication fails or the request reaches the timeout set in the **Server Request Timeout** field, the next server with the highest priority is used.

Note: As long as there are Radius servers available to try, they are tried, even if one of the servers has rejected authentication.

When all servers have failed to reply because the request has reached the timeout set in the **Server Request Timeout** field or when no servers are configured for the service asking for authentication, authentication is attempted against local user names and passwords as a fallback strategy.

Note: If one of the servers in the list of Radius servers rejects the authentication, the fallback strategy will not occur.

Radius Servers used For Accounting

A radius server can be used for Accounting Requests for the CLI, Snmp, and Web services

It is possible to use up to three Accounting Radius servers for each of the CLI, the Snmp, and Web services.

The first accounting attempt is sent to:

- the Priority #1 Radius server. If the accounting fails or the request reaches the timeout, the accounting request is sent to:
- the Priority #2 Radius server. If the accounting request fails or the request reaches the timeout, the accounting request is sent to:
- Priority #3 Radius server. If the accounting request fails or the request reaches the timeout, the accounting request is dropped.

Basic Tasks

Adding a User to DGW

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, complete the **User Name** and **Password** fields.

Note: The user name is case sensitive.

Note: Passwords are not exported to a configuration script, unless the user has admin access rights

- 3) Click **+**
- 4) From the **Access Rights** selection list, choose the appropriate rights.
- 5) From the **Lock Protection**, enable de protection, if required.
- 6) Click **Apply**.

Result

Users					
User Name	Password	Access Rights	Lock Protection		
NewUser	*****	Observer ▾	Enable ▾	—	
admin	*****	Admin ▾	Enable ▾	—	
public	*****	Admin ▾	Enable ▾	—	
				+	

Changing the Rights of a DGW User

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, from the **Access Rights** selection list, choose the appropriate rights.
- 3) Click **Apply**.

Result

The user will have the selected DGW access rights.

Changing the Login Password

Before you start

You must have administrator rights.

Information

For security reasons, it is a best practice to change the Default Login Password.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, enter a new password for the user.

Note: The password is case sensitive. All characters are allowed.

- 3) Click **Apply**.

Deleting a User from DGW

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, click  next to the user to delete.

Note: If all users are deleted from the **Users** table, the profile's default user(s) will be used upon unit restart.

- 3) Click **Apply**.
- 4) Click **Reboot**.

Result

The current activities of the deleted user are terminated only once the system has been restarted.

Users					
User Name	Password	Access Rights	Lock Protection		
admin	*****	Admin ▾	Enable ▾	—	
public	*****	Admin ▾	Enable ▾	—	
NewUser	(Deleted on next reboot)				
				+	

Protecting User Accounts Against Brute Force Attacks

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Users** table, from the **Lock Protection** selection list, choose **Enable**.

Note: For more details, refer to [Protection Against Brute Force Login Attempts](#) (p.4) and the [Advanced Access Control Parameters](#) (p.12) parameters.

- 3) Click **Apply**.

Setting the Access Control Type of the CLI Service

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Services Access Control Type** table, from the **Authentication Type** selection list, choose the appropriate type of authentication.
- 3) From the **Accounting Type** selection list, choose the appropriate type of Accounting.
- 4) If you chose to use Radius servers for authentication and/or accounting, from the **Select a Service** selection list, choose CLI.
- 5) In the **CLI Radius Server** table, complete the fields as required.

Note: As defined by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866, the RADIUS standard ports are 1812 for authentication and 1813 for accounting. However, by default, many access servers use for authentication requests port 1645 and 1646 for accounting requests.

- 6) Click **Apply**.

Result

For example:

Services Access Control Type			
Service	Authentication Type	Accounting Type	
Cli	Radius	Radius	
Snmp	Local	Radius	
Web	Radius	Radius	

Select a Service:

Cli Radius Servers			
	Priority #1	Priority #2	Priority #3
Authentication			
Host:	hostname1:port	hostname2:1812	hostname3:1645
Server Secret:			
Accounting			
Host:	hostname1:port	hostname2:181	hostname3:1646
Server Secret:			
General (Applied to all services)			
Server Request Timeout (s)	5		
Radius Users Access Rights	Admin		

Setting the Access Control Type of the Snmp Service

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Services Access Control Type** table, from the **Accounting Type** selection list, choose the appropriate type of Accounting.

Note: The use of a Radius server for Authentication is not allowed for the Snmp Service

- 3) If you chose to use Radius servers for accounting, from the **Select a Service** selection list, choose **SNMP min**.
- 4) In the **SNMP Radius Servers** table, complete the fields as required.

Note: As defined by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866, the RADIUS standard ports are 1812 for authentication and 1813 for accounting. However, by default, many access servers use for authentication requests port 1645 and 1646 for accounting requests.

- 5) Click **Apply**.

Result

For example:

Services Access Control Type			
Service	Authentication Type	Accounting Type	
Cli	Radius	Radius	
Snmp	Local	Radius	
Web	Radius	Radius	

Select a Service: Snmp

Snmp Radius Servers			
	Priority #1	Priority #2	Priority #3
Authentication			
Host:			
Server Secret:			
Accounting			
Host:	hostname1:port	hostname2:1813	hostname3:1646
Server Secret:			
General (Applied to all services)			
Server Request Timeout (s)	5		
Radius Users Access Rights	Admin		

Setting the Access Control Type of the Web Service

Before you start

You must have administrator rights.

Steps

- 1) Go to **Management/Access Control**.
- 2) In the **Services Access Control Type** table, from the **Authentication Type** selection list, choose the appropriate type of authentication.
- 3) From the **Accounting Type** selection list, choose the appropriate type of Accounting.
- 4) If you chose to use Radius servers for authentication and/or accounting, from the **Select a Service** selection list, choose **Web**.
- 5) In the **Web Radius Servers** table, complete the fields as required.

Note: As defined by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866, the RADIUS standard ports are 1812 for authentication and 1813 for accounting. However, by default, many access servers use for authentication requests port 1645 and 1646 for accounting requests.

- 6) Click **Apply**.

Result

For example:

Services Access Control Type			
Service	Authentication Type	Accounting Type	
Cli	Radius ▾	Radius ▾	
Snmp	Local ▾	Radius ▾	
Web	Radius ▾	Radius ▾	

Select a Service: Web ▾

Web Radius Servers				
	Priority #1	Priority #2	Priority #3	
Authentication				
Host:	hostname1:port	hostname2:1812	hostname3:1645	
Server Secret:				
Accounting				
Host:	hostname1:port	hostname2:1813	hostname3:1646	
Server Secret:				
General (Applied to all services)				
Server Request Timeout (s)	5			
Radius Users Access Rights	Admin ▾			

Advanced Access Control 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 :

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

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

- To set the maximum login attempts allowed before locking the account:
Aaa.LoginLockedMaxRetry
- To set how much time the account will remain locked: **Aaa.LoginLockedTimeout**

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