



Administration Manual

Unit Manager Network

Product Version 3.2

Document Revision 34

Septembre 25, 2019

Media5 Corporation
4229 Garlock Street
Sherbrooke, Québec, Canada J1L 2C8

Unit Manager Network Administration Manual

© 2019, Media5 Corporation

All rights reserved. No part of this publication may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the express written permission of the publisher.

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.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Preface

Welcome	xi
Intended Audience	xi
Using this Manual	xi
Using the Online Help System	xi
Symbols	xi
Screen Captures	xii
Moving Through the UMN	xii
SCN vs PSTN	xii
Related Documentation	xii

Installation & Configuration

Chapter 1

Installation	3
Platform Requirements	3
Installation Procedure	3
Software License Key	4
If the Procedure Did Not Work	5
Installing the UmnMibPack	5
Modifying an Existing Installation	6
Upgrading Program Components	6
Service	7
Uninstalling the UMN	7

Chapter 2

Configuring the UMN	9
Configuration Window	9
User / Password Information	9
Units Selection	10
Global SNMP Preferences	11
GetBulk Settings	12
SNMPv3 Security Settings	12

Chapter 3

Introduction	15
Overview	15
Versions	15
Opening the Administrator Module	16
Connection on Startup Behaviour	17

Modules	18
Machine ID Key	18
Editing Mediatrix Units Parameters	19
Direct Edit Method	19
SNMP Edit Method	19
Collection Process	19
Protocols and Ports	20

Internal Editor

Chapter 4

Using the UMN	23
Introduction	23
Tool Bar	23
Server Properties	24
Unit Types	24
Analog Mediatrix Units	24
Digital Mediatrix Units	25
Managing the List of Mediatrix Units	25
Autodetecting New Units	25
Opening a SSH/Telnet Session	28
Telnet Session Settings	28
Opening the SSH/Telnet Session	29
Opening a Unit's Web-Based Configuration Interface	30
Internet Browser Settings	30
Opening the unit's Web-Based Configuration Interface	30
Deleting Units from the List	31
States of Units	31
Polling Units On-line Status	31
Toggling the Unit Information	32
Viewing Options	32
OID Cache	34
Managing Mediatrix Units	34
Setting Unit Properties	34
Using IP Addresses	35
Parameters Categories	36
Searching for a Unit	38
Setting Multiple Units	39
Reports	40
Saving a Report to File	40
Detailed Report	41
Summary Report	41

Chapter 5

Using Groups, Hierarchies, and Filters	43
Groups	43
Virtual Groups	43
Creating a Virtual Group	43
Associating Units to an Instance	44
Editing a Virtual Group	46

Deleting a Virtual Group	46
Static Groups	46
Hierarchies	47
Creating a New Hierarchy	47
Applying a Hierarchy	48
Modifying a Hierarchy	48
Copying a Hierarchy	49
Deleting a Hierarchy	50
Filters	50
Filter Logical Expressions	50
Creating a New Filter	51
Applying a Filter	53
Modifying a Filter	54
Copying a Filter	55
Deleting a Filter	55

Chapter 6

Performing Actions on Mediatrix Units 57

Downloading a Software Version	57
Software Download – Analog Units	57
Version SIP 2.x Units Software Download	57
Version SIP/MGCP 4.x/5.x Units Software Download	57
Software Download – Digital Units	58
Software Download – Dgw 1.1/2.0 Units	59
Downloading a Configuration File	60
Configuration Download – Analog Units	60
Startup Configuration Download – Digital Units	61
Uploading a Configuration File	62
Configuration Upload – Analog Units	62
Startup Configuration Upload – Digital Units	62
Saving a Configuration File to XML Format	64
Saving a Configuration File to Dgw Config Script Format	65
Restarting a Unit	66
Synchronizing vs Refreshing the List	66
Synchronizing the List	66
Refreshing the List	66
Removing all DHCP Options	67

Chapter 7

Administration Parameters 69

Administration Overview	69
Administration Window	69
IP Configuration	70
Software and Emergency Download	71
Syslog Daemon	72
Unit Manager Server	72
SNTP	73
Administration Window (Dgw v1.1/2.0 Units)	73
Uplink (Wan) Configuration	74
Host Configuration	75
SNTP Configuration	75
Default Gateway Configuration	76
DNS Configuration	77

Chapter 8

Dial Map Parameters	79
Dial Map Overview	79
Dial Map Window	79
Creating a Dial Map	82
Using the Dial Map Special Characters	82
How to Use a Dial Map	83
Combining Several Expressions	83
Using the “#” and “*” Characters	83
Using the Timer	83
Using a Dial Map for Calls Outside the Country	84
Example	84
Validating a Dial Map	84

Chapter 9

Gateway Parameters	85
Gateway Overview	85
Gateway Permissions Window	85
Using Permissions	88
How to Set Proper Permissions	88
Examples	89
Local Call, Same AC	89
Local Call, Different AC	89
Long Distance Call, Same AC	89
Long Distance Call, Different AC	89
Long Distance Call, Different CC	90

Chapter 10

Ports Parameters	91
Port Overview	91
Port Configuration Window	91
Codec Activation	94
Codec Activation Overview	94
Codec Activation Configuration Window	94

Chapter 11

Signalling Protocols Parameters	97
H.323 Parameters	97
H.323 Configuration Window	97
Direct Gateway Call	99
MGCP Parameters	101
MGCP Configuration Window	101
NCS Parameters	103
NCS Configuration Window	104
SIP Parameters	106
SIP Configuration Window	106
SIP Authentication	108
CorNet-IP Parameters	110
CorNet-IP Configuration Window	110

System Services	112
CorNet-IP Fault Management Parameters	114
Fault Management Window	114
Fault Management Events	115

Chapter 12

Configuration File Fetching Parameters	119
Before Downloading	119
Configuring the TFTP Server	119
Configuring the SNTP Server	119
Configuring the HTTP Server	119
Configuration File Fetching Overview	120
Configuration File Fetching Window	121
Server Settings	122
Auto-Update Settings	124
Privacy Settings	126

Chapter 13

Software Download Parameters	127
Before Downloading	127
Configuring the TFTP Server	127
Configuring the SNTP Server	127
Configuring the HTTP Server	127
Extracting the Zip File	127
Software Download Overview	128
Software Download Window	129
Server Settings	129
Download Settings	130
Example	131
Auto-Update Settings	132
Software Download Window (Dgw v1.1/2.0 Units)	135
Transfer Configuration	135
Firmware Packs Configuration	136

Chapter 14

STUN Parameters	139
Introduction	139
SIP Outbound Proxy	139
Restrictions on the Media5 STUN Implementation	139
STUN Overview	140
STUN Window	140

Chapter 15

Subscriber Services Parameters	143
Subscriber Services Overview	143
Subscriber Services Configuration Window	144
Call Hold	145
Call Waiting	145

Second Call	146
Call Transfer – Blind Transfer	146
Call Transfer – Attended Transfer	146
Conference Call	147
Call Forward	147
Call Forward – Unconditional	147
Call Forward – On Busy	149
Call Forward – On No Answer	151

Chapter 16

Telephony Attributes Parameters..... 155

Telephony Attributes Overview	155
Telephony Attributes Configuration Window.....	156
Call Direction	156
Automatic Call	157
Hook Flash Processing	158

Chapter 17

Working with SNMP 161

Introduction	161
SNMPv3 Services	161
SNMP Behaviour	162
Non-Secure Management Mode	162
Secure Management Mode	163
Setting Unit SNMP Preferences	163
GetBulk Settings.....	164
SNMPv3 Security Settings	164
Notes	165
SNMPv3 Unit Settings	166
Cloning a User.....	166
Modifying a User	167
Deleting a User.....	168

Chapter 18

Troubleshooting Tips..... 169

General Problems	169
------------------------	-----

Edit SNMP Window

Chapter 19

Edit SNMP Window 173

Edit SNMP Window	173
Toolbar	174
MIB File.....	175
MIB File Icons.....	175

Mx Experimental MIBs	175
MIB Cache.....	175
Performing SNMP Operations	176
Performing a GET Operation.....	176
Automatic GET	176
Performing a SET Operation	176
Performing a Walk Operation	178
SNMP Table Viewer	178
Options	179
Performing a GET Operation in a Table	180
Performing a SET Operation in a Table	180
Forcing a SET	180
Performing a Walk Operation in a Table	180
Miscellaneous Options.....	180
Using the Find Option.....	180
Expanding and Collapsing the MIB Tree.....	181
Message Log	181

Appendices

Appendix A

Managing Large Scale Deployment of Numerous Units.....	185
Before Configuring.....	185
Choice # 1: Use GUI (Dialog Boxes and/or Edit SNMP)	185
Choice # 2: Use Configuration Files	185
Modify the Existing Configuration File	186
Create a New Configuration File	186
Use the Default Configuration File as a Template.....	187

Appendix B

Unit Collection Methods	189
Introduction	189
MIB Parameters to Set	189
MIB Parameters for SIP v2.x Units	189
MIB Parameters for SIP/MGCP v4.x/5.x Units	190
MIB Parameters for Dgw v1.1/v2.0 Units	191
Automatic Collection Method (MIB)	192
Collection Method for SIP v2.x Units	192
Collection Method for SIP/MGCP v4.x/v5.x Units	193
Collection Method for Dgw v1.1/v2.0 Units	194
Manual Collection Method (Autodetect).....	195
Using a Configuration File	197
Traplog.txt File	197

Appendix C

Glossary 199

Appendix D

List of Acronyms 205

The Unit Manager Network (UMN) manages networks of Mediatrix units within an Intranet to provide end-to-end IP Telephony solutions.

Intended Audience

This **manual** explains how to install and use the UMN with Mediatrix products. It is intended for network administrators who are responsible for installing and setting up network equipment; consequently, it assumes the administrator has a basic working knowledge of LANs (Local Area Networks).

Using this Manual

This **manual** includes task-related information to help you use the UMN as quickly as possible.

Using the Online Help System

The UMN offers a built-in online help system that you can peruse at will.

► **To get help in a dialog box:**

1. Press the <F1> key while this window is opened.
The corresponding information is displayed.

Symbols

The following information provides an explanation of the symbols which appear in the UMN documentation.



Warning: Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Waarschuwing: Dit waarschuwingssymbool betekent gevaar. U overtreedt in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus: Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Attention: Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung: Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst.

Avvertenza: Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel: Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso: Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Advertencia! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Warning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.



Caution: Caution indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury and/or damage to the equipment or property.



Note: Note indicates important information about the current topic.

► This represents steps to perform to accomplish a particular task.

Screen Captures

This **manual** includes sample screen captures. Your actual screen can look slightly different from the sample screen. This is normal and not a cause for concern.

Moving Through the UMN

Moving through the UMN is like moving through any other Windows program. You can use your mouse to point and click or you can use the <Tab> key to move from field to field.

You can also use short-cut keys. These keys are used in menus and dialog boxes where an alternate keystroke sequence is available. These shortcut keys are shown underscored like Help. To use this shortcut key, press and hold the <ALT> key and press the <H> key. For more information about using shortcut keys and other Windows conventions, see the Microsoft Windows help.

SCN vs PSTN

In Media5's and other vendor's documentation, the terms SCN and PSTN are used. A SCN (Switched Circuit Network) is a general term to designate a communication network in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. The Public Switched Telephone Network (PSTN) or a Private Branch eXchange (PBX) are examples of SCNs.

Related Documentation

For more information, refer to the available documentation published on the Media5 documentation portal at <https://documentation.media5corp.com>

Installation & Configuration

Page Left Intentionally Blank

This [chapter](#) describes how to install the UMN.

Platform Requirements

- ▶ **Server module:** PC with Windows 2000, XP, Server 2003, Vista, 7 and Server 2016.
- ▶ **Administrator module:** PC with Windows 2000, XP, 2003, Vista, 7, and 10.

Installation Procedure

This section describes the steps required to install the UMN. You must install it by using a login with Administrator privileges in order to permit installation of the service. Media5 recommends to close all software applications and background programs such as firewalls, antivirus, etc. to avoid conflict during installation.

If you have a previous version already installed on your system, you have the choice between:

- ▶ Uninstalling the previous version ("[Uninstalling the UMN](#)" on [page 7](#))
- ▶ Upgrading the previous version to the new version ("[Upgrading Program Components](#)" on [page 6](#))

Depending on the version currently installed, you may not be able to perform an upgrade. Please refer to the *readme.txt* file on the installation CD for more information on version compatibility.



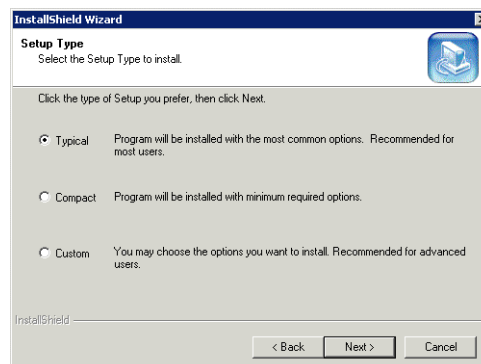
Caution: The installation will fail if there is another SNMP service running on port 162. If installation fails or if there is another SNMP service running on port 162, refer to the "[UMN application cannot be installed or UMN service cannot start on a Windows machine.](#)" on [page 4](#) section

▶ To install the UMN:

1. Choose a Windows machine to host the UMN.
2. In the directory where the installation program is located, select the *setup.exe* file and start it.
3. After reviewing the instructions in the Welcome dialog box, keep the preset installation folder, or click *Browse* and specify the pathname of a different folder.

The following window opens.

Figure 1: Installation Wizard



4. Specify the type of installation to use.

Table 1: Installation Options

Choice	Description
Typical	The UMN will be installed with the most common options. Recommended for most users.
Compact	The UMN will be installed with minimum required options.
Custom	You may select the options you want to install. Recommended for advanced users.

5. If you are using the Custom installation, select which parts of the UMN to install. Options with a check mark are installed. Click to the left of an item to select it.
6. Click *Next* to begin the installation.
When the installation is complete, restart your computer.

► **UMN application cannot be installed or UMN service cannot start on a Windows machine.**

1. Check that your firewall allows access to port 162.
2. Disable your anti-virus software to determine if it is causing interference.
3. Run the `netstat -ano | findstr ":162"` command to determine if there is another application running.
`C:\>netstat -aon | findstr ":162"`
 UDP 0.0.0.0:162 : 3968
 UDP [::]:162 : 3968

The numbers at the End of the Line are PID numbers that can be looked up in the Task manager to see which service is currently holding the port. If another application is holding the port, that application will need to be stopped.

Software License Key

Once installed, the UMN can manage up to three (3) units without a license key. To manage more than three units requires purchasing and installing a license key.

► **To get your license key:**

1. Double-click the *Administrator* icon or access the *Start > Programs > Unit Manager Network 3.2 > Unit Manager Network* option.
2. In the Administrator login window, enter the IP address of the computer running the UMN, and then click *OK*.
The *Unit Manager Client* window opens.
3. In the *Help* menu, select the *License Key Request* task.
The following window opens:

Figure 2: License Key Request Window

The Machine ID key of the server running the Unit Manager service (not necessarily the machine hosting the Administrator) is displayed in the *Machine ID Key* field.

4. Enter the Product Key that is located on the CD case in the *Product ID Key* field.
5. Enter the company name to which register the license in the *Company Name* field.
If the Product Key is valid, the *Send email* button becomes available.
6. Click *Send email*.
This starts your default email application. The information in the *Message* section of the *License Key Request* window is copied into the body of the email.
7. Add the register@media5corp.com email address in the *To* field of your email application.
Media5 also recommends that you put a meaningful subject such as *License Key Request*.
8. Send the email.
Some firewall settings prohibit emails with attached executable programs. If that is your case, mention it in the email and Media5 will send the file by another means.
9. Media5 will send back a license key as an executable program. Run this program to install your license key.
You are now ready to use the UMN with the number of units requested.

Note that if you uninstall and reinstall the UMN:

- ▶ you can use the same license key if you are installing the UMN on the same computer.



Caution: The machine ID key is generated according to the hardware of your computer. If a hardware component of your machine fails, it may be possible that the license key will not work.

- ▶ you shall ask a new license key if you are installing the UMN on a different computer.

If the Procedure Did Not Work

Copy the following information from the *Message* section of the *License Key Request* window and send it to the register@media5corp.com email address:

- ▶ Product Key (located on the CD case)
- ▶ the company name to which register the license
- ▶ the machine-specific ID key listed in the *Machine ID Key* field

Installing the UmnMibPack

The UmnMibPack is a single installable package that updates the MIB definition of the UMN. It does not contain any modification to the UMN software program application. A UmnMibPack is cumulative, which means it also includes the contents of all its predecessors.

Each UmnMibPack has its own specific version number that is incremented after each new release. This version number is displayed in the main Administrator window in the right pane's title and in the *Server properties* window.

The latest Unit Manager Network Mib packs can be found on the Media5 documentation portal at <https://documentation.media5corp.com/display/DGWLATEST/Unit+Manager+Network>

► **To install a UmnMibPack:**

1. Start the UmnMibPack installation by double-clicking the installer file.
The installation procedure starts.
2. Follow the instructions on screen.

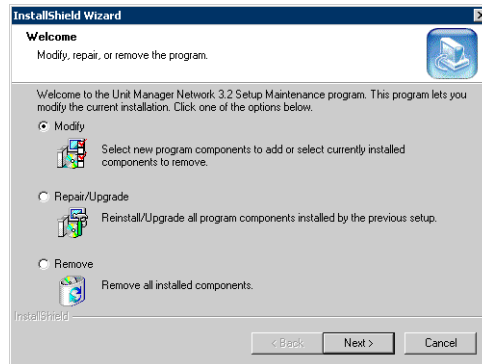
Modifying an Existing Installation

You can modify a previous installation of the UMN.

► **To modify an already installed version of the UMN:**

1. In the directory where the installation program is located, select the *setup.exe* file and start it.
The following window opens:

Figure 3: Installation Wizard



You have the following choices:

Table 2: Installation Wizard Choices

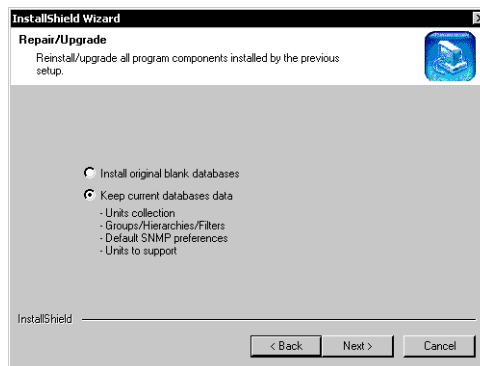
Choice	Description
Modify	You can select new program components to add or select currently installed components to remove.
Repair/Upgrade	Reinstalls/Upgrades all program components installed by the previous setup. See "Upgrading Program Components" on page 6 for more details.
Remove	Removes all installed components.

2. Proceed with the rest of the procedure.

Upgrading Program Components

Upon selecting the *Repair/Upgrade* choice when modifying an installation, the following window opens:

Figure 4: Repair/Upgrade



The repair/upgrade feature allows you to define how to handle the databases the UMN uses.

Table 3: Repair/Upgrade Choices

Choice	Description
Install original blank databases	Overwrites your current databases with the ones provided with the installation. You will lose any information you currently have.
Keep current databases data	The following information is kept: • Units collection • Groups/Hierarchies/Filters • Default SNMP preferences • Units to support

Service

After the computer has restarted, you can verify that the service is properly installed and started by accessing the following window:

- ▶ On Windows 2000/XP/2003, the *Administrative Tools/Services* window of the *Control Panel*.

There should be one (1) service installed and started:

- ▶ Unit Manager Network 3.2

If the service is not started, you can access the Event Viewer to look at any error message the service might have logged. This will help you determine why the service has not started.

Uninstalling the UMN

The following describes how to uninstall the UMN.

▶ To uninstall the UMN:

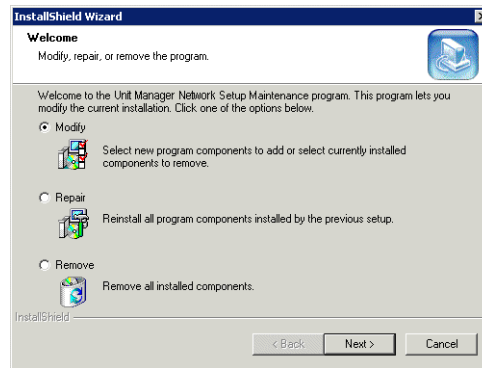
1. Backup any files if this is only a temporary uninstall. Make sure you have Administrator privileges. The following directories contain the files that you should back up:

- CfgFile: Contains the units' configuration
- Filters: Contains the filters defined by the administrator
- Hierarchies: Contains the units' hierarchy as defined by the administrator

You should also back up the *Database\MxUnitManagerUserData.umn*, which contains the client database of the units detected by UMN.

2. In the directory where the installation program is located, select the *setup.exe* file and start it. The following window opens:

Figure 5: Installation Wizard



3. Select the *Remove* option, and then click *Next*.
This removes all installed components of the UMN.
4. Follow the instructions on screen.

Configuring the UMN

The following [chapter](#) describes how to configure the UMN.

Configuration Window

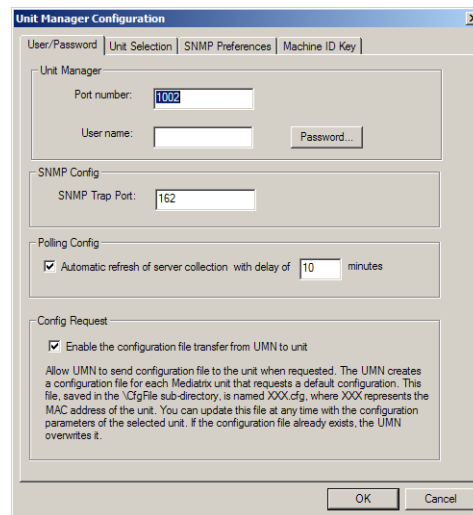
The *Unit Manager Configuration* window allows you to modify the parameters that define how the UMN works.

► **To configure the UMN:**

1. Select the *Start > Programs > Unit Manager Network 3.2 > Configuration > Unit Manager Configuration* option.

The following window opens.

Figure 6: Unit Manager Configuration Window



The *Unit Manager Configuration Window* contains four tabs to set various information:

- User / Password
- Unit Selection
- SNMP Preferences
- Machine ID Key (see [“Software License Key” on page 4](#) for more details)

User / Password Information

The *User / Password* tab allows you to set a minimum of protection for your UMN. The user name and password entered here must be the same as those set in the UMN login window. See [“Opening the Administrator Module” on page 16](#) for more details.

Figure 7: User / Password Tab

The screenshot shows the 'Unit Manager Configuration' dialog box with the 'User/Password' tab selected. The dialog has four sub-sections: 'Unit Manager', 'SNMP Config', 'Polling Config', and 'Config Request'. In the 'Unit Manager' section, the 'Port number' is set to 1002, and there are fields for 'User name' and 'Password...'. In the 'SNMP Config' section, the 'SNMP Trap Port' is set to 162. In the 'Polling Config' section, the checkbox 'Automatic refresh of server collection with delay of' is checked, with a delay of 10 minutes. In the 'Config Request' section, the checkbox 'Enable the configuration file transfer from UMN to unit' is checked. A detailed description of this option is provided below the checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

Unit Manager Configuration

User/Password | Unit Selection | SNMP Preferences | Machine ID Key

Unit Manager

Port number: 1002

User name: Password...

SNMP Config

SNMP Trap Port: 162

Polling Config

☒ Automatic refresh of server collection with delay of 10 minutes

Config Request

☒ Enable the configuration file transfer from UMN to unit

Allow UMN to send configuration file to the unit when requested. The UMN creates a configuration file for each Mediatrix unit that requests a default configuration. This file, saved in the \CfgFile sub-directory, is named XXX.cfg, where XXX represents the MAC address of the unit. You can update this file at any time with the configuration parameters of the selected unit. If the configuration file already exists, the UMN overwrites it.

OK Cancel

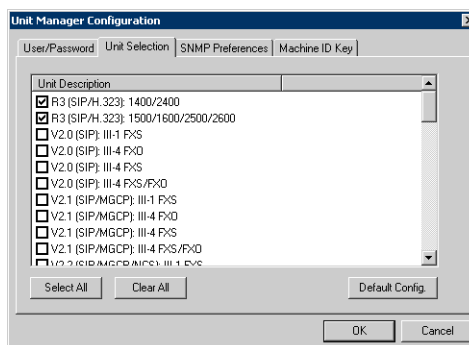
► **To set User / Password information:**

1. Specify the port number, user name and password of the UMN.
2. Define the SNMP Trap Port.
This is the port on which the UMN listens for SNMP traps.
3. If applicable, enable and define the automatic refresh time (in minutes) of server polling in the *Polling Config* section.
This parameter specifies that the server periodically checks for the status of all its Mediatrix units collection. The status may either be on or off. This information is used by the UMN to refresh its own list of units. See ["Polling Units On-line Status"](#) on page 31 for more details. Available values are between 1 and 1440.
4. If applicable, check the *Enable the configuration file transfer from UMN to the unit* option.
This parameter allows the UMN to send a configuration file to the unit when requested. The UMN creates a configuration file for each Mediatrix unit that requests a default configuration. This file, saved in the \CfgFile sub-directory, is named XXX.cfg, where XXX represents the MAC address of the unit. You can update this file at any time with the configuration parameters of the selected unit. If the configuration file already exists, the UMN overwrites it.
5. Click *OK* to apply the changes.

Units Selection

The *Unit Selection* tab allows you to select which type of units you want to be displayed in the UMN.

Figure 8: Unit Selection Tab



This window lets you select the type of units according to their software version. Not all unit types are selected by default.

If you deselect one type of unit, all units of this type are not displayed in the UMN and you don't know that they exist. These settings are also used when finding new Mediatrix units on the network. See [“Autodetecting New Units” on page 25](#) for more details.

You can revert to the list of units selected by default at any time by clicking the *Default Config* button.

Click *OK* to apply the changes.

Global SNMP Preferences

The *SNMP Preferences* tab allows you to define the SNMP preferences per unit type, i.e. v2.x (SIP), v4.x (SIP/MGCP), v5.x (SIP/MGCP) or Dgw units.



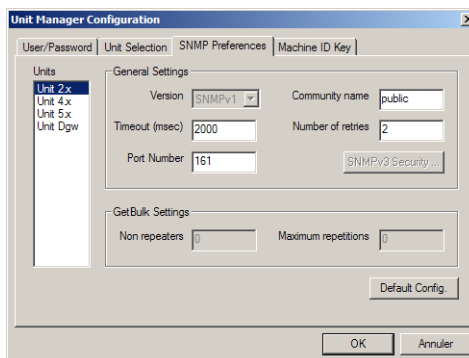
Note: The SNMP preference for Dgw units has been changed for the following:

- SNMPv3 with authentication and without privacy
- username =admin
- password =administrator

When updating from UMN v3.2r31.66/67 to v3.2r31.68 and if you keep your old database, the SNMP preference is not updated. This means that a Dgw unit cannot be reached if it has firmware Dgw v2.0r13.240 or higher. You should thus manually change the SNMP preference after updating UMN. This operation is not required with UMN v3.2r31.68 and higher.

To define SNMP preferences for individual units, see [“Setting Unit SNMP Preferences” on page 163](#).

Figure 9: SNMP Preferences Tab



► **To set SNMP preferences:**

1. Select the type of units for which to set the SNMP preferences.
The information available differs depending on whether you have v2.x, v4.x, v5.x or Dgw units.
2. In the *General Settings* section, select the *Version* of SNMP used.
Supported values are SNMPv1, SNMPv2c, and SNMPv3. They may or may not be available depending on the unit type selected.
3. Set the *Timeout* in milliseconds.
When a SNMP request is sent to the remote unit, an answer must be sent back from the unit within a specified period of time. This is the Timeout. If no answer is received within the Timeout value, the UMN sends the SNMP request again to the remote unit. If the unit still does not answer after the defined Number of retries, the UMN considers it as being off-line.
4. Define the *Port Number* on which the remote unit listens for SNMP requests.
5. Define the *Community name*.
Media5 recommends not to change this value and keep *public*.
6. Define a *Number of retries*.
Number of times the UMN sends a SNMP request to the remote unit in case it does not answer within the specified Timeout. If the remote unit still does not answer after the defined Number of retries, the UMN considers it as being off-line.
7. Click *OK* to apply the changes.
You can revert to the default settings of a unit type at any time by selecting this unit type and clicking the *Default Config* button.

GetBulk Settings

The GetBulk operation is used to efficiently retrieve large blocks of data, such as multiple rows in a table. GetBulk settings are specific to SNMPv2c and SNMPv3. They are used by the GetTable and GetWalk commands.

► **To set GetBulk settings:**

1. In the *SNMP Preferences* tab, select the unit type *Unit 4.x*.
2. Set the *Version* to *SNMPv2c* or *SNMPv3*.
3. Set the following GetBulk settings.

Table 4: GetBulk Parameters

Parameter	Description
Non repeaters	Number of pairs in the variable binding list array for which a single instance should be returned.
Maximum repetitions	Maximum number of repetitions to return.

4. Click *OK* to apply the changes.

SNMPv3 Security Settings

Set SNMPv3 security settings to successfully connect to a unit that supports SNMPv3.



Note: Create a user in the remote unit or SNMPv3 agent prior to defining the following settings or you will not be able to connect to this remote unit or SNMPv3 agent.

► To set **SNMPv3 security settings**:

1. In the *SNMP Preferences* tab, select the unit type *Unit 4.x*.
2. Set the *Version* parameter to *SNMPv3*.
3. Click the *SNMPv3 Security* button.

The following window opens.

Figure 10: SNMPv3 Security window

The image shows a dialog box titled "SNMPv3 Security". It has three main sections. The "Identification" section contains a "User name" field with the text "McDesUse" and a "Context name" field. The "Security Level" section has three radio buttons: "No authentication or privacy", "Authentication without privacy", and "Authentication with privacy", with the third one selected. The "Authentication" section has a "Protocol" dropdown menu set to "MD5" and a "Change Password ..." button. The "Privacy" section has a "Protocol" dropdown menu set to "DES" and a "Change Password ..." button. At the bottom are "OK" and "Cancel" buttons.

You can specify security information required to successfully connect to a SNMPv3 agent.

4. Set the following information:

Table 5: Security Settings Parameters

Parameter	Description
User name	Human-readable alphanumeric string representing a user or a group of users. It is passed as a parameter in all of the SNMP operations. This field cannot be empty.
Context name	SNMPv3 context name. A MIB context is a named subset of the object instance in the local MIB.
Security level (radio buttons)	SNMPv3 security level at which SNMP messages can be sent or processed, expressed in terms of whether or not authentication and/or privacy are provided. Available values are: - No authentication or privacy - Authentication without privacy - Authentication with privacy All options are mutually exclusive.
Authentication protocol (drop-down list)	SNMPv3 authentication protocol. Available values are <i>MD5</i> or <i>SHA</i> .
Change Password - Authentication (button)	Opens the <i>Change Password</i> window to specify the SNMPv3 authentication password. You must have the proper rights granted by the SNMPv3 agent to proceed. Note: SNMPv3 Passwords should not have repeating blocks of characters and must have at least 8 characters.
Privacy protocol (drop-down list)	SNMPv3 privacy protocol, for instance, DES.
Change Password - Privacy (button)	Opens the <i>Change Password</i> window to specify the SNMPv3 privacy password. You must have the proper rights granted by the SNMPv3 agent to proceed. Note: SNMPv3 Passwords should not have repeating blocks of characters and must have at least 8 characters.



Note: The Mediatrix units support Basic and Digest authentication as per RFC 3261.

5. Click *OK* when all changes are done.

This [chapter](#) introduces the UMN and explains the collection process concept.

Overview

The UMN manages networks of Mediatrix units within an Intranet to provide end-to-end IP Telephony solutions.

In particular, the UMN helps to:

- ▶ Control configuration parameters of all Mediatrix units on the network.
- ▶ Field-upgrade all Mediatrix units.
- ▶ Display firmware release of any Mediatrix unit.
- ▶ Permit controlled implementation of new software.
- ▶ Keep track of all the configuration options of the Mediatrix units on the network.
- ▶ Know the state of each Mediatrix unit (power off/on).

Versions

Once installed, the UMN can manage up to three units without a license key. To manage more than three units requires purchasing and installing a license key. See [“Software License Key” on page 4](#) for more details.

The number of units the UMN supports is displayed in the main Administrator window in the right pane’s title.

Opening the Administrator Module

The Administrator module is a Graphical User Interface (GUI) that allows you to set all information pertaining to the Mediatrix units collection.

► **To open the Administrator:**

- 1. Access the *Start > Programs > Unit Manager Network 3.2* section and select one of the following options.

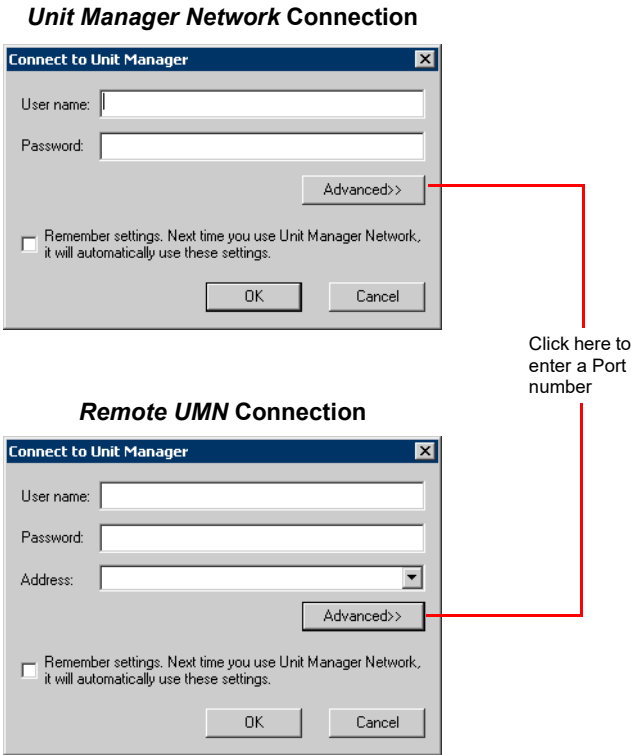
There are two ways to open the UMN:

Table 6: UMN Login Options

Menu Option	Description
Remote UMN	Opens a UMN session on another, i.e., remote, machine. You need to enter a user name and a password, as well as the IP address of the remote computer on which the UMN you want to open is installed.
Unit Manager Network	Opens the UMN on the local machine, i.e., on the computer where you are currently working. You only need to enter a user name and a password.

The Administrator login window opens.

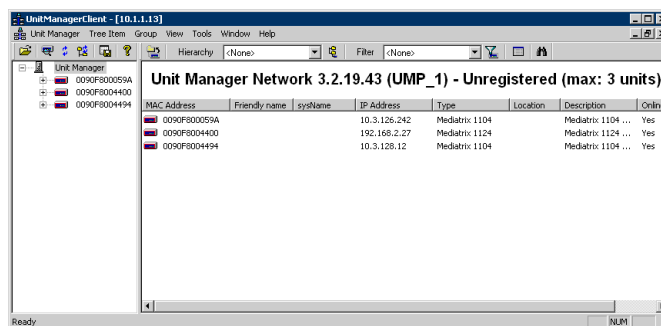
Figure 11: Administrator Login



- 2. Enter a valid user name and password.
The user name and password entered here must be the same as those set in the UMN configuration window. If you are connecting to a remote UMN, you must use the user name and password set in the remote UMN application. See ["Chapter 2 - Configuring the UMN"](#) on page 9 for more details.
- 3. If you are connecting to a remote UMN, enter the IP address of the remote computer running the UMN.

4. If required, click the *Advanced* button to enter a Port number.
It must be the same as the Unit Manager port number. If you are connecting to a remote UMN, you must use the port number set in the remote UMN application. See [“Chapter 2 - Configuring the UMN” on page 9](#) for more details.
5. If you want the UMN to automatically use the settings you just entered the next time you open it, click the *Remember settings* option.
The *Connect to Unit Manager* window will not display the next time you open the UMN. If you want to remove the automatic settings option, you must specify it in the *Settings* window, option *Restore last connection on startup*, as described in [“Connection on Startup Behaviour” on page 17](#).
6. Click *OK*.
The Administrator window opens.

Figure 12: Administrator Graphical Interface



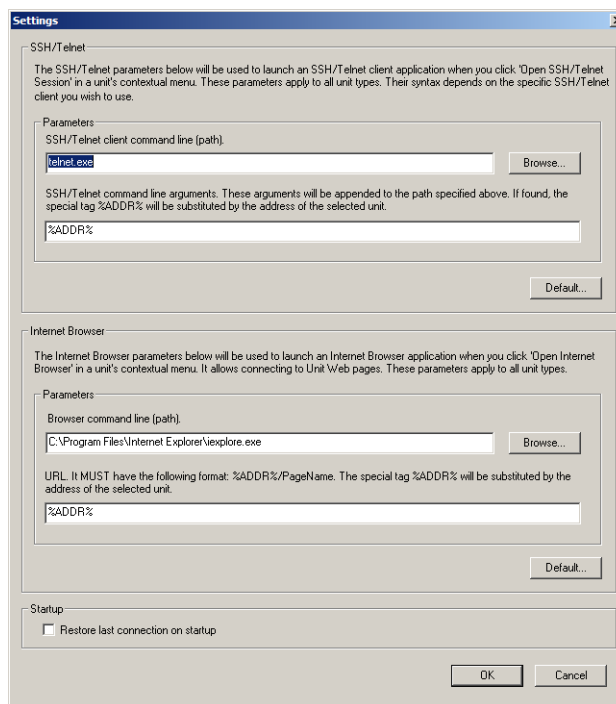
Connection on Startup Behaviour

After opening the Administrator module for the first time, the opening behaviour will not be the same the next time you open the UMN. It will automatically try to reconnect with the last server to which it was connected upon closing it. If this is successful, you will not see the *Connect to Unit Manager* dialog box.

You can change this behaviour.

- **To change the connection on startup behaviour:**
 1. In the *Tools* menu, select the *Settings* task.
The following window opens:

Figure 13: Settings Window



2. If you want to see the *Connect to Unit Manager* dialog box each time you restart the UMN, uncheck the *Restore last connection on startup* option.
3. Click *OK*.

Modules

The UMN contains the following modules.

Table 7: UMN Modules

Modules	Description
Unit Manager	Used to configure and deploy a large number of Mediatrix units. The Unit Manager Network: - Keeps track of all the configuration options of the Mediatrix units on the network. - Automatically detects new Mediatrix units connected to the administrative domain. - Allows to remotely configure the Mediatrix units. - Knows the state of each Mediatrix unit (online/offline).
Administrator	Unit Manager graphical user interface.

See also "Platform Requirements" on page 3.

Machine ID Key

You can access the *Machine ID Key* window in the *Help* menu. This window displays the ID key of the server running the Unit Manager service (not necessarily the machine hosting the Administrator). This menu item is only available if the Unit Manager module is properly started.

Once installed, the UMN can manage up to three units without a license key. To manage more than three units requires purchasing and installing a license key.

Send the following information to the register@media5corp.com email address:

- ▶ Product Key (located on the CD case)
- ▶ Company name to which register the license
- ▶ Machine-specific ID key

Media5 will send a license key as an executable program. Run this program to install the license key.

See [“Software License Key” on page 4](#) for more details.

Editing Mediatrix Units Parameters

There are two ways to remotely configure the Mediatrix units connected to your administrative domain:

- ▶ Directly in the UMN.
- ▶ By editing the values stored in the Management Information Base (MIB).

Direct Edit Method

The direct edit method is performed in the UMN itself with dialog boxes that allow you to set the various parameters relevant to the selected category. See [“Internal Editor” on page 21](#) for more details on this method.

SNMP Edit Method

The UMN has an integrated MIB browser (called the *Edit SNMP* window) that allows you to change parameter values directly in the corresponding MIB. See [“Chapter 19 - Edit SNMP Window” on page 173](#) for more details on this method.

Refer to the *MIB Reference* manual for a complete list of variables that can be set.



Note: It is assumed that you have basic knowledge of TCP/IP network administration and SNMP.

Collection Process

The UMN lists the units present on an administrative domain. These units can be listed in two ways:

- ▶ The UMN lists the Mediatrix units it can find in a specified range of IP addresses, for instance within your administrative domain. See [“Autodetecting New Units” on page 25](#) for more details.
- ▶ If properly set up, the Mediatrix units contact the UMN to let it know they are on-line. See [“Unit Collection Methods” on page 189](#) for more details.

Protocols and Ports

The following describes which protocols with which ports are used for the communication between the UMN and the managed units. This information is necessary to configure firewalls located between the components. Please note that the ports below are the default ports and they can vary depending on the UMN's and the units' configuration.

Table 8: Protocols and Ports

Protocol	TCP/ UDP	Traffic to UMN	Traffic from UMN	Configurable
Corba (UMN client-server communication)	TCP	1002	1002	Yes ("User / Password Information" on page 9)
SNMP	UDP	161	161	Yes ("Autodetecting New Units" on page 25)
SNMP Trap	UDP	162	N/A	Yes ("User / Password Information" on page 9)
TFTP (Config. File transfer)	UDP	69	69	No
TFTP temporary data port	UDP	1-65535	1-65535	No
HTTP (Unit's Web page access)	TCP	80	80	Yes ("Opening a Unit's Web-Based Configuration Interface" on page 30)
SSH (Unit's CLI access)	TCP	22	22	Yes ("Opening a SSH/Telnet Session" on page 28)

Some features of the UMN may not work when a NAT is present. Media5 recommends to avoid using NAT with the UMN.

Internal Editor

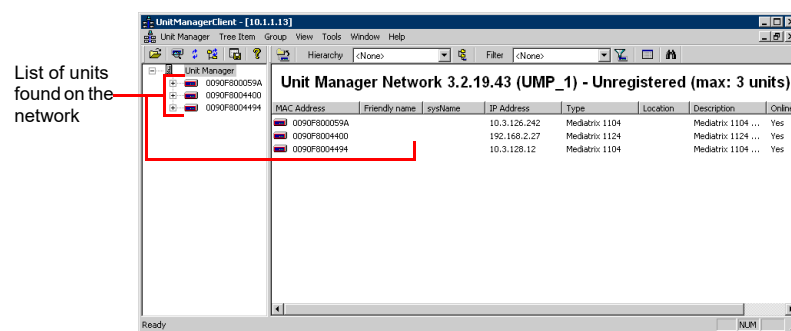
Page Left Intentionally Blank

This [chapter](#) introduces the UMN graphical user interface (GUI) and explains how to manage the Mediatrix units collection.

Introduction

The UMN's GUI allows you to easily configure and deploy a large number of analog and digital Mediatrix units.

Figure 14: UMN – Administrator Window



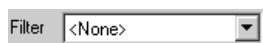
Tool Bar

The following tools help you manage remote units.

Table 9: Tool Bar Icons

Tool	Description
	Connects to the UMN.
	Launches the <i>Unit Detection</i> window. See “Autodetecting New Units” on page 25 for more details.
	Refreshes the display. See “Refreshing the List” on page 66 for details.
	Refreshes the tree hierarchy display. See “Refreshing the List” on page 66 for details.
	Opens the <i>Reports</i> window. See “Reports” on page 40 for more details.
	Displays basic information about the UMN.
	Opens the <i>Virtual Groups Management</i> window. See “Virtual Groups” on page 43 for more details.
Hierarchy <None>	Selects an existing hierarchy and applies it to the list of units. See “Applying a Hierarchy” on page 48 .
	Opens the <i>Hierarchies Management</i> window. See “Hierarchies” on page 47 .

Table 9: Tool Bar Icons (Continued)

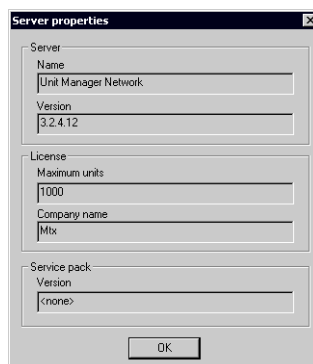
Tool	Description
	Selects an existing filter and applies it to the list of units. See “Applying a Filter” on page 53 .
	Opens the <i>Filter Management</i> window. See “Filters” on page 50 .
	In the right pane, toggles between the list of units and the on-line/off-line status of these units for the selected level. See “Toggling the Unit Information” on page 32 .
	Opens the <i>Find Units</i> window. See “Searching for a Unit” on page 38 .

Server Properties

The *Server properties* window gives read-only information about the server name and version, the license installed and the service pack.

► **To display the server properties:**

1. Right-click the *Unit Manager* level.
2. Select the *Properties* option in the context sensitive menu that opens.
You can also select the *Properties* task of the *Tree Item* menu.
The following window opens:

Figure 15: Server Properties Window

Unit Types

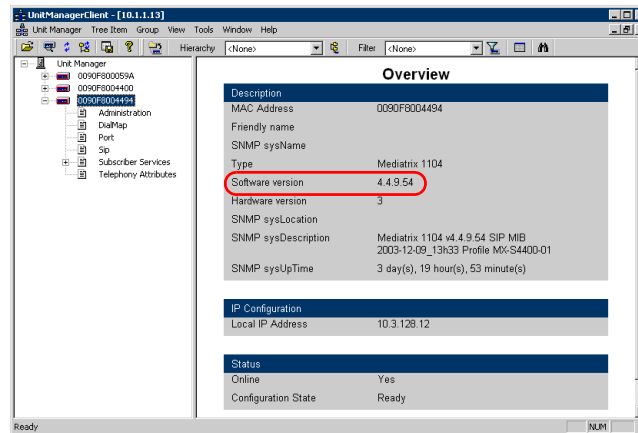
The UMN lists two types of Mediatix units:

- Analog Mediatix units.
- Digital Mediatix units.

Analog Mediatix Units

The UMN lists the analog Mediatix units from all signalling protocols and software versions. The software versions support different signalling protocols. To only display units from a specific version, see [“Units Selection” on page 10](#). The Overview page of the selected unit displays the software version.

Figure 16: Software Version



Depending on the software version and protocol used by a selected unit, the information available varies. See [“Parameters Categories” on page 36](#) for more details.

Digital Mediatrix Units

The UMN lists all the digital Mediatrix units. To only display units from a specific version, see [“Units Selection” on page 10](#).

Refer to your digital Mediatrix unit’s documentation for more details on how to configure and use it.

Managing the List of Mediatrix Units

This section explains how to add, delete, and manage Mediatrix units in the UMN.

You can also define which units you want displayed at one time and in which fashion. This is possible by using groups, hierarchies, and filters. See [“Chapter 5 - Using Groups, Hierarchies, and Filters” on page 43](#) for more details.

Autodetecting New Units

You can automatically find new analog and digital Mediatrix units on the network according to the unit versions you have selected in the *Unit Manager Configuration* window. See [“Units Selection” on page 10](#) for more details.

The UMN can detect analog units that are in normal operation mode as well as in recovery mode. For more information on the recovery mode, please refer to the analog unit’s Administration manual.

Refer to [“General Problems” on page 169](#) if you have problems with the autodetect feature.

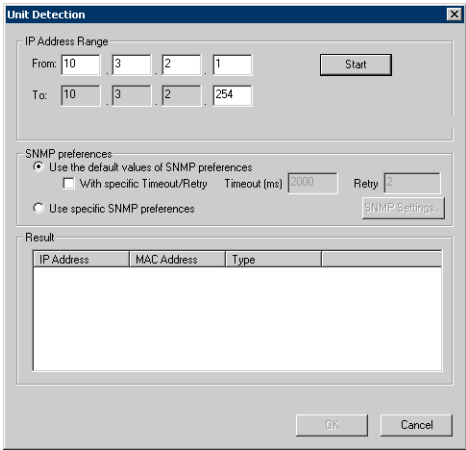
► To autodetect new Mediatrix units on the network:

1. Click the  icon in the UMN tool bar.

You can also right-click the *Unit Manager* level and select the *AutoDetect* option in the context sensitive menu that opens.

The *Unit Detection* window opens:

Figure 17: Unit Detection Window



- 2. Set the range of IP addresses within which to detect units.
- 3. Define the SNMP Preferences to use for units detection.
Only units having SNMP preferences compatible with those you define will be detected.

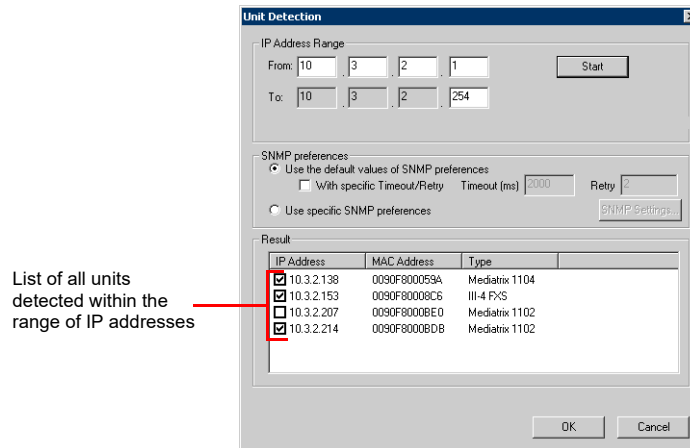
Table 10: Autodetect SNMP Preferences

Choice	Description
Use the default values of SNMP preferences	Units having SNMP preferences compatible with the generic SNMP preferences as defined in “Global SNMP Preferences” on page 11 will be listed. You can define a specific timeout and retry count when autodetecting units by checking the <i>With specific Timeout/Retry</i> option. These will override the default values. Enter the information in the appropriate fields. This may be useful when, for instance, you are scanning a large range of IP addresses and you want to reduce the time it takes to do so.
Use specific SNMP preferences	Click the <i>SNMP Settings</i> button to define specific SNMP preferences. These settings are the same as in unit-specific SNMP preferences described in “Setting Unit SNMP Preferences” on page 163 . Units having SNMP preferences compatible with the specific ones you set will be listed.



Note: The digital Mediatrix units only support SNMPv1.

- 4. Click the *Start* button.
The UMN goes through all IP addresses within the specified range and lists the Mediatrix units detected in the *Result* section.

Figure 18: Results of Autodetect

Units with a check mark were not present in the previous autodetect process. You can check/uncheck units as you want.

5. Click **OK** to add units with a check mark.
The list of Mediatrix units in the UMN is automatically refreshed.

Opening a SSH/Telnet Session

You can launch a SSH/Telnet client session to configure the parameters of digital Mediatrix units.

Telnet Session Settings

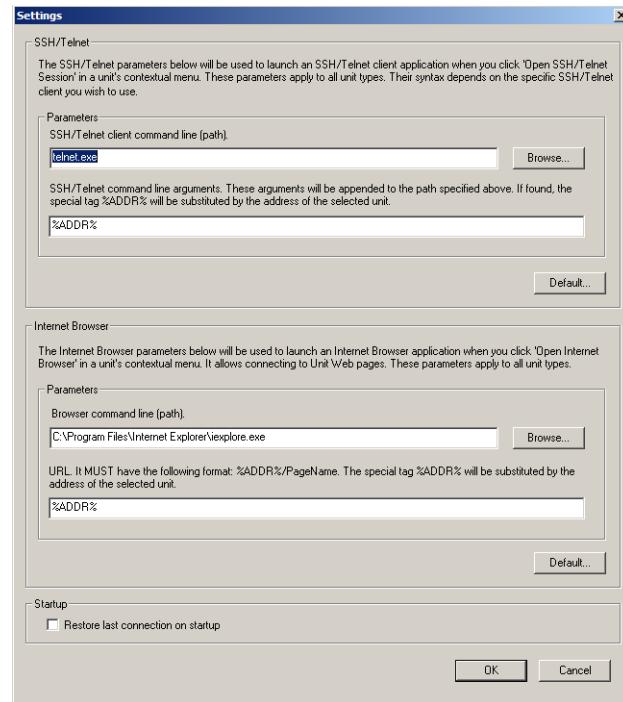
The parameters used to open a SSH/Telnet session are global and apply to all digital Mediatrix units.

► **To set SSH/Telnet session parameters:**

1. In the *Tools* menu, select the *Settings* task.

The following window opens:

Figure 19: Settings Window



2. In the *SSH/Telnet* section, set the file name and path of the SSH/Telnet application to use in the *SSH/Telnet client command line (path)* field.

You can use the *Browse* button to locate the SSH/Telnet application. The default value is "telnet.exe", which is the Windows Telnet client. Note that this application is not the same between different Windows versions. Windows 2000's Telnet application is text-based (runs in command prompt).

If you do not want to use the default Windows Telnet client, you can specify the SSH/Telnet client to use.

3. If applicable, enter SSH/Telnet command line arguments.

These arguments will be appended to the path specified in the previous step. The default value is *%ADDR%*, which represents the IP address of the unit.

An example of SSH/Telnet command line argument could be:

```
-p -s %ADDR%
```

The syntax of the arguments depends on the SSH/Telnet client you are using. Please refer to your SSH/Telnet client's documentation for more details on the syntax to use.

4. Click *OK* when all changes are done.

For information on the *Restore last connection on startup* option, see ["Connection on Startup Behaviour" on page 17](#).

Opening the SSH/Telnet Session

Once the SSH/Telnet session settings are configured (see [“Telnet Session Settings” on page 28](#)), you can open the session.

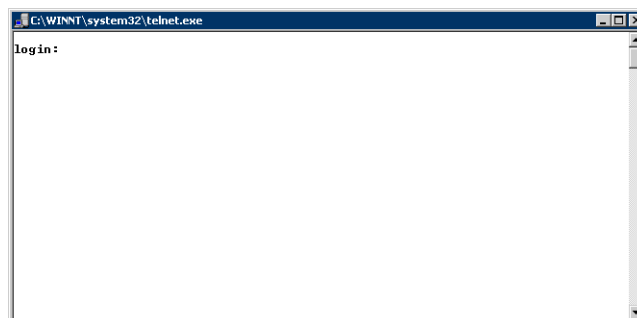
The SSH/Telnet session is opened from the PC where the client application is installed. It thus establishes a direct connection to the unit. This could cause some problems if the client PC cannot directly access the unit because of a firewall, restrictions, etc.

► **To open a SSH/Telnet session:**

1. Right-click the unit for which to open a SSH/Telnet session.
2. Select the *Open SSH/Telnet Session* option in the context sensitive menu that opens.

The following window opens:

Figure 20: Telnet Session Login



This window may differ if you are not using the default Windows Telnet client.

Refer to your digital Mediatrix unit's documentation for informations on how to access it via a Telnet session.

Opening a Unit's Web-Based Configuration Interface

You can launch the web-based configuration interface of a unit to configure its parameters.

Internet Browser Settings

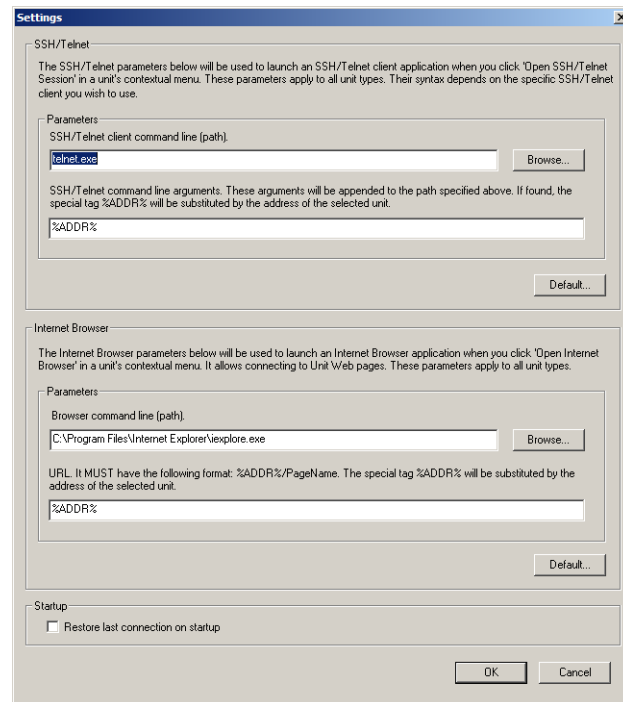
The parameters used to open the Internet browser and the web-based configuration interface are global and apply to all the related Mediatrix units. This feature is not available for all unit types.

► **To set Internet browser parameters:**

1. In the *Tools* menu, select the *Settings* task.

The following window opens:

Figure 21: Settings Window



2. In the *Internet Browser* section, set the file name and path of the Internet browser to use in the *Browser command line (path)* field.
You can use the *Browse* button to locate the Internet browser. The default value is "C:\Program Files\Internet Explorer\iexplore.exe", which is the Windows Internet Explorer.
If you do not want to use the default browser, you can specify the browser to use.
3. Enter the URL of the web-based configuration interface in the *URL* field.
The URL must have the *%ADDR%/PageName* syntax. *%ADDR%* represents the IP address of the unit.
4. Click *OK* when all changes are done.
For information on the *Restore last connection on startup* option, see ["Connection on Startup Behaviour" on page 17](#).

Opening the unit's Web-Based Configuration Interface

Once the Internet browser settings are configured (see ["Internet Browser Settings" on page 30](#)), you can open the web-based configuration interface.

The Internet browser session is opened from the PC where the client application is installed. It thus establishes a direct connection to the unit. This could cause some problems if the client PC cannot directly access the unit because of a firewall, restrictions, etc.

► **To open an Internet browser session:**

1. Right-click the unit for which to open an Internet browser session.
2. Select the *Open Internet Browser* option in the context sensitive menu that opens.

Deleting Units from the List

You can remove Mediatrix units from the list in the UMN by selecting the specific unit to remove, and then pressing the key of the keyboard. You can also use the right-click context sensitive menu.

States of Units

Mediatrix units listed in the UMN can have four states, each one differentiated by the colour of the icon on the left.

Figure 22 illustrates the various states.

Figure 22: Units States

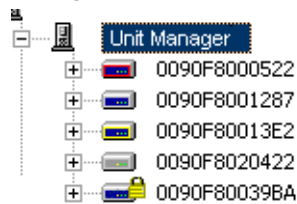


Table 11: Units States Description

Color	State
Red	The unit has been detected for the first time. The network administrator has not made any change to it yet.
Blue	The network administrator has edited some of the unit parameters.
Yellow	The unit has received its default configuration file. The network administrator has not made any change to it yet.
Grey	The unit has been previously detected, but it is currently off-line.

Furthermore, units currently using the SNMPv3 protocol are displayed with a lock icon.

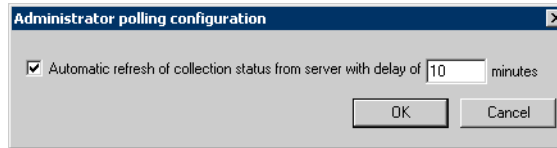
You can also use model-specific icons, as described in [“Viewing Options” on page 32](#)

Polling Units On-line Status

The Administrator window can periodically check for the status of all Mediatrix units it lists. The status may either be on-line or off-line. This information is taken from the UMN server, as defined in [“User / Password Information” on page 9](#).

► **To set polling information:**

1. In the *View* menu, select the *Polling* task.
The following window opens:

Figure 23: Administrator Polling Configuration

2. If applicable, define the automatic refresh time (in minutes) at which the Administrator looks into the server units status.

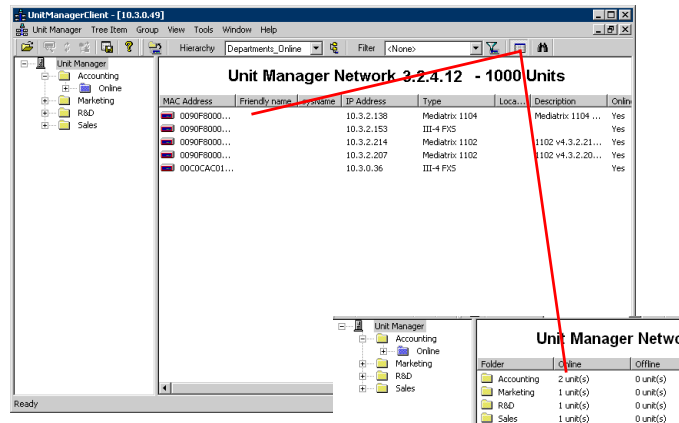
The result is displayed at various locations in the UMN, such as in the Status line of each unit's overview pane (see [“Managing Mediatrix Units” on page 34](#) for more details).

Toggling the Unit Information

In the right pane of the UMN, you can toggle between the list of units and the on-line/off-line status of these units.

► To toggle the unit information:

1. Select the level for which you want information.
For instance, this could be the top level of the tree list.
2. Click the  icon in the UMN tool bar.
You can also select the *Show Units* task of the *View* menu.
The information toggles between the list of units and the on-line/off-line status of these units.

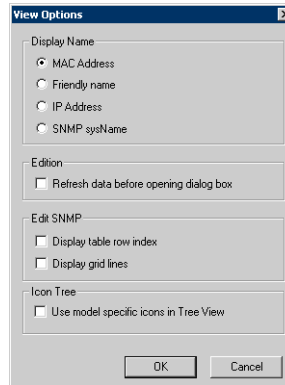
Figure 24: Toggling Information

Viewing Options

The following options allow you to define how to sort the Mediatrix units in the UMN.

► To set viewing options:

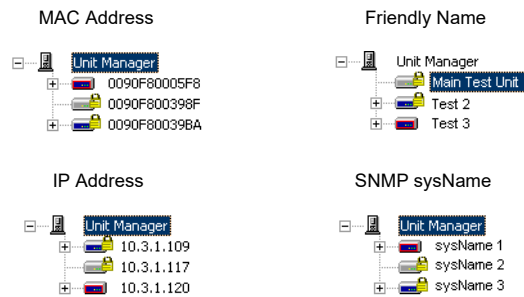
1. In the *View* menu of the UMN, select the *Options* task.
The following window opens:

Figure 25: View Options Window

2. Select how to sort the Mediatrix units.

You can sort the units according to their:

- MAC Address
- Friendly name
- IP Address
- SNMP sysName (see [“Setting Unit Properties” on page 34](#) for more details).

Figure 26: Display Name Options

3. In the *Edition* section, check the *Refresh data before opening dialog box* if you want the UMN to automatically refresh its data.
When opening a dialog box, the UMN retrieves the information it stored in its database. However, if another UMN changed this information, your application does not know it. Checking this option will avoid such confusion but may slightly slow access to dialog boxes.
4. In the *Edit SNMP* section, select if you want to show/hide the table row index and grid lines by checking/unchecking the proper choices.
This section relates to the *Edit SNMP* window of the UMN. See [“SNMP Table Viewer” on page 178](#) for more details.
5. In the *Icon Tree* section, select whether you want to use the standard icons to represent units in the tree list (option unchecked), or model-specific icons by checking the *Use model specific icons in Tree View* option.

Table 12: Model-Specific Icons Description

Icon	Description
	Represents a FXS unit.
	Represents a FXO unit.

Table 12: Model-Specific Icons Description (Continued)

Icon	Description
	Represents a Secure Enterprise Controller (Mediatrix 3300 series) unit.

The same colours to describe the unit's state apply as defined in [“States of Units” on page 31](#).

- Click *OK* to set the changes.

OID Cache

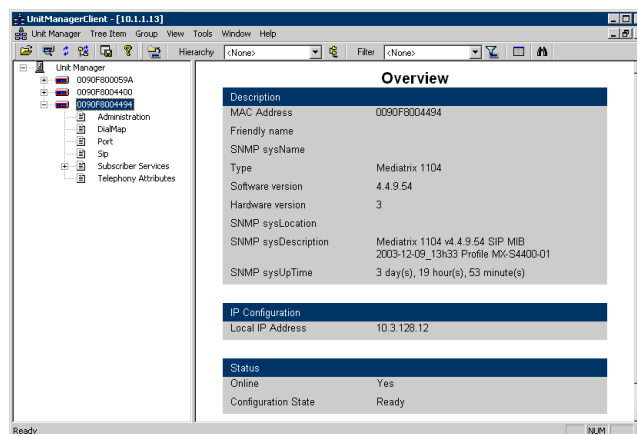
When working with SNMP tables, the UMN uses an OID cache to access the tables. If there is an error when accessing a table for the first time, it may be possible that the cache does not contain the proper information. This could happen, for instance, with a unit that does not display the proper number of ports.

► **To clear the contents of the OID cache:**

- In the *Tools* menu of the UMN, select the *Clear Server's OID Cache* task.

Managing Mediatrix Units

Upon selecting a Mediatrix unit, a general overview of this unit is displayed in the right pane of the Administrator window.

Figure 27: Mediatrix Unit Overview

The *Overview* section lists information for the selected Mediatrix unit such as:

- MAC address
- Friendly Name
- Type
- Software/Hardware version
- Local IP address
- etc.

Setting Unit Properties

You can set some basic properties of a selected Mediatrix unit.

► **To set unit properties:**

1. Double-click the unit for which to set the properties.
You can also right-click the unit and select the *Properties* option in the context sensitive menu that opens.
The following window opens:

Figure 28: Properties Window



Note: The *Save running configuration after setting values* option is available on Mediatrix digital units only.

2. Set the friendly name of the unit.
The friendly name is an alternative to the MAC address and is displayed if you select it in the viewing options. See [“Viewing Options” on page 32](#) for more details. Note that the friendly name is not saved in the MIB configuration.
3. Set the following SNMP System Information:

Table 13: SNMP System Information

Information	Description
sysName	An administratively-assigned name, also known as SNMP MIB-2 sysname. By convention, this is the unit's fully-qualified domain name.
sysContact	The textual identification of the contact person, together with information on how to contact this person.
sysLocation	The physical location of the unit (e.g., “telephone closet, 3rd floor”).

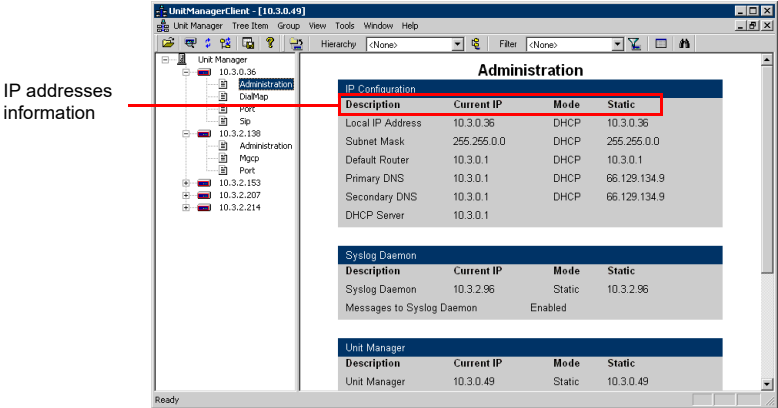
If you have selected a Mediatrix digital unit, this information will be set in the running configuration upon clicking on *OK*.

4. If applicable, save the information set in the running configuration into the startup configuration of the unit by checking the *Save running configuration after setting values* option.
See [“Synchronizing vs Refreshing the List” on page 66](#) for more details.
5. Click *OK* to set the changes.

Using IP Addresses

Mediatrix units can automatically receive an IP address via the DHCP server or use a static IP address you have defined. The overview of each category lists the IP addresses.

Figure 29: IP Addresses



The IP addresses information is displayed in columns.

Table 14: IP Addresses Information

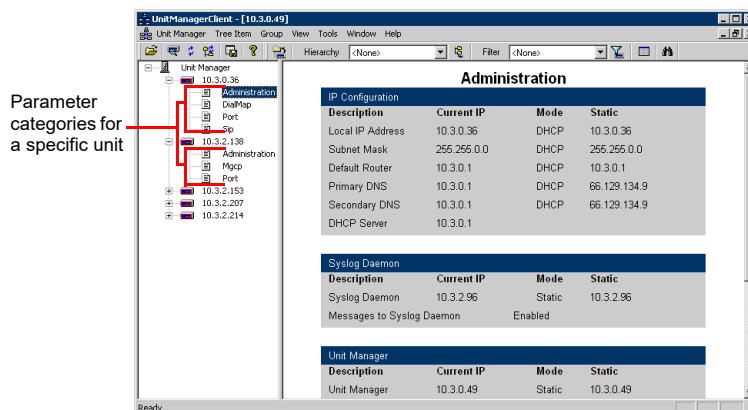
Column	Description
Description	Brief description of the IP address.
Current IP	Actual value of the IP address.
Mode	Source of the IP address. • <i>DHCP</i>: a DHCP server provided the IP address when the Mediatrix unit was powered on. • <i>Static</i>: you manually specified a static IP address.
Static	Indicates which IP address to use in case the DHCP server cannot be reached or if you are using static IP addresses.

Parameters Categories

The UMN allows you to access and modify the properties and settings of the units.

**Note:** The digital Mediatrix units do not have parameter categories.

- To manage a Mediatrix unit:
1. Select the Mediatrix unit to manage in the list of connected units and expand its parameter categories by clicking the [+] icon on the left.
The various parameters categories available for the selected unit are displayed. These categories vary depending on the protocol currently running in the unit.
 2. Select the parameter category to access.
Figure 30 illustrates the parameter categories available.

Figure 30: Mediatrix Units Parameter Categories

The UMN uses seven (7) distinct parameter categories.

Table 15: Parameter Categories

Link	Description
Administration	Sets the parameters and IP addresses used by a Mediatrix unit. See “Chapter 7 - Administration Parameters” on page 69.
Dial Map	Sets parameters pertaining to the Dial Map, which allows you to configure the ports of a Mediatrix unit when making calls. See “Chapter 8 - Dial Map Parameters” on page 79. Note: Only available for units that run the SIP or H.323 signalling protocol.
Gateway	Sets the various permission settings for gateway communication. See “Chapter 9 - Gateway Parameters” on page 85. Note: Only available for units that run the SIP signalling protocol.
Ports	Sets the FXS or FXO ports parameters. See “Chapter 10 - Ports Parameters” on page 91.
Subscriber Services	Sets the various subscriber services available on the user's telephone. See “Chapter 15 - Subscriber Services Parameters” on page 143. Note: Only available for FXS units that run the SIP v4.4, SIP v4.5, or H.323 v4.0 signalling protocol.
Telephony Attributes	Sets the various telephony attributes used to configure the characteristics of the telephony system being implemented. See “Chapter 16 - Telephony Attributes Parameters” on page 155. Note: Only available for units that run the SIP v4.4, SIP v4.5, or H.323 v4.0 signalling protocol.
MGCP	Sets MGCP-specific configuration parameters. See “MGCP Parameters” on page 101.
NCS	Sets NCS-specific configuration parameters. See “NCS Parameters” on page 103.
SIP	Sets SIP-specific configuration parameters. See “SIP Parameters” on page 106.
H.323	Sets H.323-specific configuration parameters. See “H.323 Parameters” on page 97.

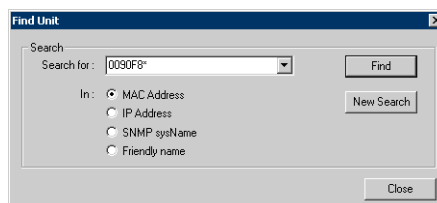
Searching for a Unit

The Find option allows you to look for a specific unit or multiple units in the list maintained by the UMN.

► To find units:

1. Click the  icon of the UMN tool bar.
You can also select the *Find Unit* task of the *Unit Manager* menu.
The following window opens:

Figure 31: Find Unit Window



2. Select the type of search to perform.
You have the following choices:
 - by MAC address
 - by IP address
 - by SNMP sysName (see [“Setting Unit Properties” on page 34](#))
 - by Friendly name (see [“Setting Unit Properties” on page 34](#))
3. Enter the string to search in the *Search for* field.
You can type all or part of the string to find. You can use the following special characters in the search process:

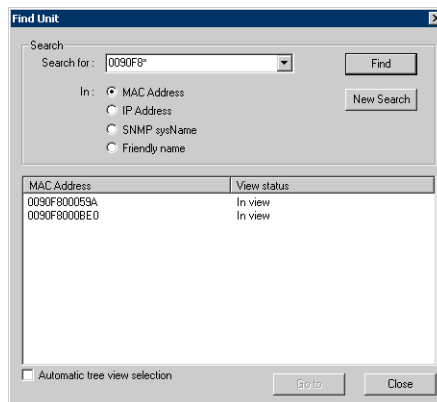
Table 16: Special Characters in Find

Special Character	Description
Asterisk (*)	You can use the asterisk as a substitute for zero or more characters. For instance, If you are looking for units with a MAC address that starts with 0090F8 , type the following: 0090F8* The <i>Find Unit</i> window will locate all units with a MAC address that begins with 0090F8 .
Pipe ()	You can use the “ ” operator (or) to define a range of search. For instance, to find units that either start with 0090 or 0080, type the following: 0090* 0080*

Notes:

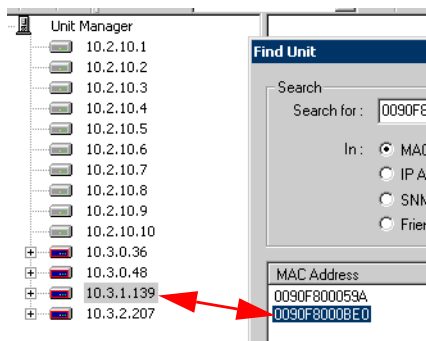
- If you get too many results, try entering additional search criteria to make your search more specific.
 - Click *New Search* to clear the search criteria field and begin a new search.
4. Click *Find* to start the search process.
The search results are listed in a new section below the find settings.

Figure 32: Find Results



5. To display the information on a specific unit, either:
 - Double-click the unit in the search results list.
 - Select the unit and click the *Go to* button.
 - Check the *Automatic tree view selection* option at the bottom of the window. Clicking a unit selects it in the tree list of the Administrator window.

Figure 33: Automatic Tree View Selection



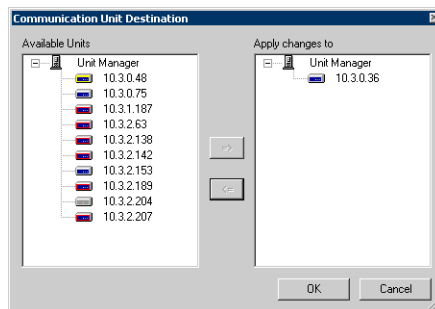
Setting Multiple Units

Most of the UMN windows allow you to apply settings to several units at the same time. This allows you to configure a large number of Mediatrix units.

► To apply changes to several Mediatrix units:

1. Click the *Set target units* button.
The *Communication Unit Destination* window opens.

Figure 34: Communication Unit Destination Window



The *Available Units* section (on the left) lists the available units currently connected to the UMN that are compatible with the settings defined.

The *Apply changes to* section (on the right) lists the Mediatrix units for which to apply the changes. The units are listed according to the hierarchy you have applied to the list of units (see [“Hierarchies” on page 47](#) for more details).

2. Transfer the Mediatrix units for which to apply the changes to the list on the right.

You can transfer units, groups, or instances. You can select several units at the same time:

- To select consecutive units, click the first unit, press and hold down <SHIFT>, and then click the last unit.
- To select units that are not consecutive, press and hold down <CTRL>, and then click each unit.

3. Click *OK* when changes are done.

Reports

The UMN offers two reports you can view and print: a summary report and a detailed report. These reports give you an exact status of the units connected to the UMN at a specific time.

Please note that:

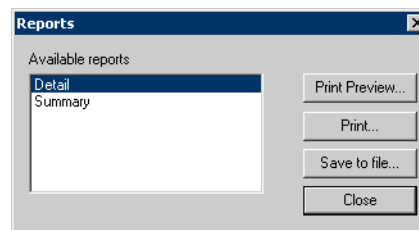
- ▶ If no Hierarchy nor Filter is applied, the report lists all units currently connected to the UMN.
- ▶ If a Hierarchy is applied, the report lists the units according to their Groups.
- ▶ If a Filter is applied, the report lists only the units affected by the filter.

See [“Chapter 5 - Using Groups, Hierarchies, and Filters” on page 43](#) for more details.

▶ To use the reports:

1. Click the  icon in the UMN tool bar.
You can also access the *Unit Manager* menu and select the *Reports* task.
The following window opens.

Figure 35: Reports Window



2. Select the report to produce (detail or summary), and then either press the *Print Preview* or *Print* buttons.
The report is printed.

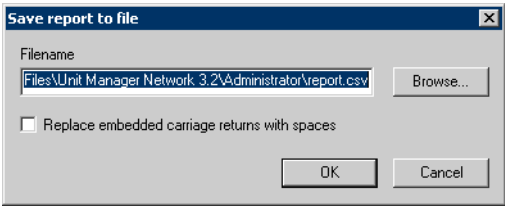
Saving a Report to File

The UMN allows you to save the report you have selected in a file.

▶ To save a report in a file:

1. In the *Reports* window, select the report to save, and then click the *Save to file* button.
The following window opens.

Figure 36: Save report to file Window



- 2. Define where to save the report file in the *Filename* field.
Use the *Browse* button to save in a different directory than the default one.
- 3. Check the *Replace embedded carriage returns with spaces* option if you want to remove from the exported data any carriage returns that may be embedded in text fields.
- 4. Click *OK* when done.
The file is saved in csv (comma-separated values or comma delimited) format. This format may be read by virtually any spreadsheet program.

Detailed Report

The detailed report gives information about such items as MAC address, Friendly name, SNMP information, etc.

Figure 37 on page 41 illustrates a detailed report example.

Figure 37: Detailed Report Example

Unit Manager Network - Detail report	
Group: \Accounting\Online	
MAC Address	0090F800059A
Friendly name	
SNMP sysName	
SNMP sysContact	
SNMP sysLocation	
SNMP sysDescr	APA_IV-4FXS V4.3.1.8 SIP MIB 1.1.6.18 Profile v1.2.1.1
SNMP sysObjectId	.1.3.6.1.4.1.4935.1.4
IP Address	10.3.2.138
Status	Online
Configuration state	Ready
Product type	Mediatrix 1104
Software version	4.3.1.8
Hardware version	DB_Rev_A AB_Rev_A
MAC Address	0090F8000998
Friendly name	
SNMP sysName	
SNMP sysContact	
SNMP sysLocation	
SNMP sysDescr	
SNMP sysObjectId	.0.1.3.6.1.4.1.4935.1.1.1.4
IP Address	10.3.0.148
Status	Online
Configuration state	Ready
Product type	III-4 FXS
Software version	2.4.8.32
Hardware version	DB_Rev_C AB_Rev_D

Summary Report

The summary report gives the following information:

- ▶ MAC address
- ▶ SNMP sysName

- ▶ IP address
- ▶ Status
- ▶ Type Description

Figure 38 on page 42 illustrates a summary report example.

Figure 38: Summary Report Example

Unit Manager Network - Summary report

<i>Group: \Accounting\Online</i>					
<i>MAC Address</i>	<i>SNMP sysName</i>	<i>IP Address</i>	<i>Status</i>	<i>Type</i>	<i>sysDescription</i>
0090F800059A		10.3.2.138	Online	Mediatrix 1104	APA_IV-4FXS v4.3.1.
0090F8000998		10.3.0.148	Online	III-4 FXS	Profile v1.2.1.1

Page: 1 of 4 Friday, August 02, 2002

Using Groups, Hierarchies, and Filters

The UMN uses a tree list located in the left pane of the Administrator window to list the units collection. You can customize this list by defining which units you want displayed at one time and in which fashion. This is possible by using groups, hierarchies, and filters.

- ▶ *Groups* are categories to which you can associate one or more units.
- ▶ *Hierarchies* are view definitions, created with groups, that you can apply to the list of units.
- ▶ *Filters* are display criteria that you can apply to the tree list of units to further customize how to display units.

Groups

Groups are categories to which you can associate one or more units. You can use two types of groups:

- ▶ Virtual Groups
- ▶ Static Groups

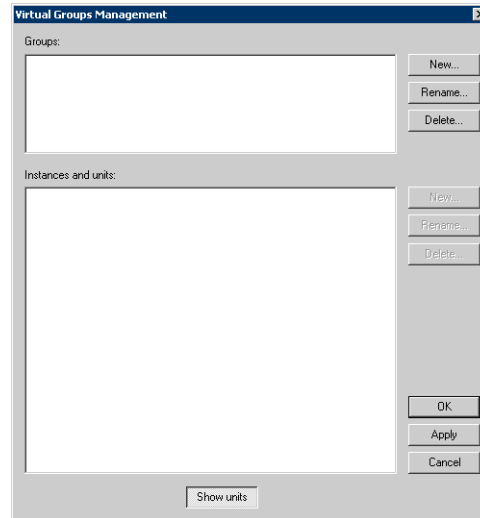
These groups are used to manage hierarchies, as described in [“Hierarchies” on page 47](#).

Virtual Groups

A virtual group is a group you can create to suit your own needs. For instance, virtual groups may be departments in your company.

Creating a Virtual Group

- ▶ **To create a virtual group:**
 1. Click the  icon in the UMN tool bar.
You can also select the *Groups* task in the *Group* menu.
The following window opens:

Figure 39: Virtual Groups Management Window

2. In the *Groups* section, click the *New* button.
3. In the *New Virtual Group* window that opens, enter the name of the new group, and then click *OK*. For instance, it could be something like “Departments”.
4. In the *Instances and units* section, click the *New* button.
An instance is a category of the group. It is displayed in the tree list as a sub-level of the UMN. A group may contain as many instances as you want.
For example, instances of the *Departments* group could be *Accounting*, *Marketing*, *R&D*, etc.
5. In the *New Instance* window that opens, enter the name of the new instance, and then click *OK*. It could be something like “Accounting”. You can:
 - Rename an existing instance by selecting it and clicking the *Rename* button in the *Instances and units* section.
 - Delete an existing instance by selecting it and clicking the *Delete* button in the *Instances and units* section. When deleting an instance, all units assigned to this instance are moved to the *Unknown* instance.

You are now ready to assign units to an instance as described in [“Associating Units to an Instance” on page 44](#).

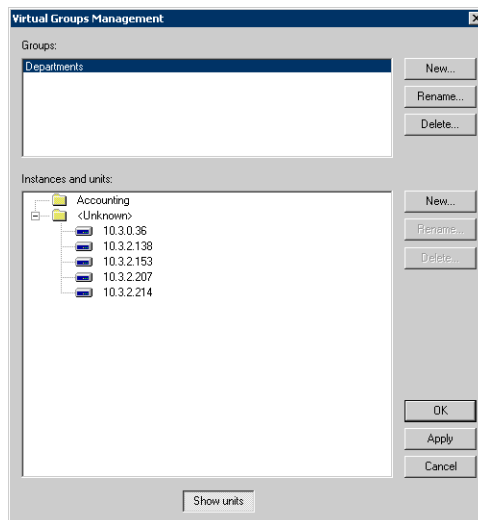


Note: The tree representation of available instances is always two levels deep: the instance itself and the units assigned to it.

Associating Units to an Instance

► To associate units to an instance of a group:

1. In the *Virtual Groups Management* window, click the *Show units* button at the bottom of the window. This displays all units currently listed in the UMN according to their view options.

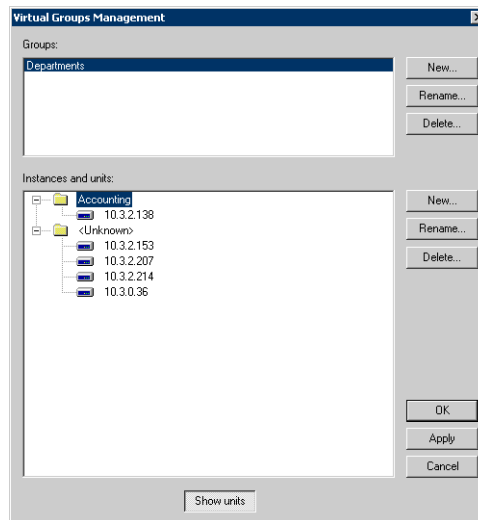
Figure 40: Virtual Groups Management Window

All units that are not currently assigned to a specific instance are listed in the *Unknown* instance.

2. Assign a specific unit to the *Accounting* instance by dragging and dropping this unit in the instance. You can also right-click the unit, select the *Assign to instance* option of the context sensitive menu that opens, and then the specific instance to which assign the unit.

You can select several units at the same time:

- To select consecutive units, click the first unit, press and hold down <SHIFT>, and then click the last unit.
- To select units that are not consecutive, press and hold down <CTRL>, and then click each unit.

Figure 41: Unit Assigned

3. Repeat the process with as many instances you want, and then click **OK**. You can also click the **Apply** button. In this case, the window stays open. Clicking on **Cancel** undoes all actions up to the last **Apply** you have made. You can now create a hierarchy with the groups and instances you just created as described in [“Hierarchies” on page 47](#).



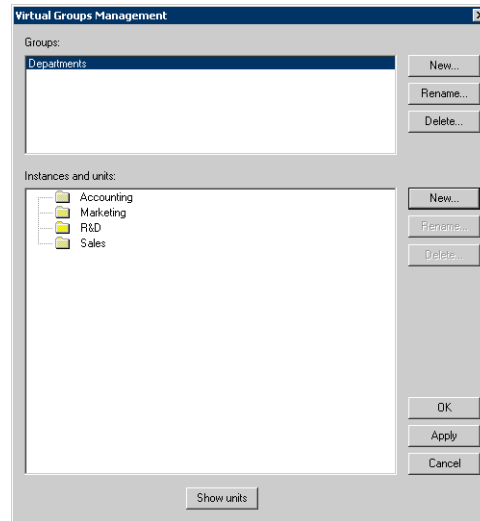
Note: A unit may be assigned to only one instance of one group at the same time.

Editing a Virtual Group

► To edit a virtual group:

1. Click the  icon in the UMN tool bar.
You can also select the *Groups* task in the *Group* menu.
The following window opens:

Figure 42: Virtual Groups Management Window



2. Select the group to edit.
3. If you want to rename the group, click the *Rename* button in the *Groups* section.
4. If you want to modify instances, follow the instructions in [“Associating Units to an Instance” on page 44](#).
5. When you are done, click *OK*.

Deleting a Virtual Group

► To delete a virtual group:

1. Click the  icon in the UMN tool bar.
You can also select the *Groups* task in the *Group* menu.
2. In the *Virtual Groups Management* window, select the group to delete and click the *Delete* button in the *Groups* section.
All instances created under this group are deleted.
3. When you are done, click *OK*.

Static Groups

A static group is a pre-defined group in the UMN. You cannot add, modify or delete a static group. Those groups are:

- Unit type (e.g. 1124, 1102, 1204)
- Software version
- Online/offline status
- Subnet

Hierarchies

A hierarchy is a view you can define and apply to the list of units in order to customize the way in which they are displayed. It does not affect the units themselves, only the way they are displayed. It may use one or more of the virtual groups you have created, one or more of the static groups available, or a combination of both types.

Creating a New Hierarchy

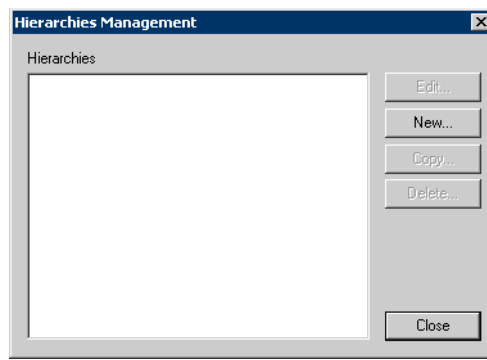
You can create a new view definition to sort and display the units collection of the UMN.

► **To create a new hierarchy:**

1. Click the  icon of the UMN tool bar.

You can also access the *Group* menu and select the *Hierarchies* task. The following window opens:

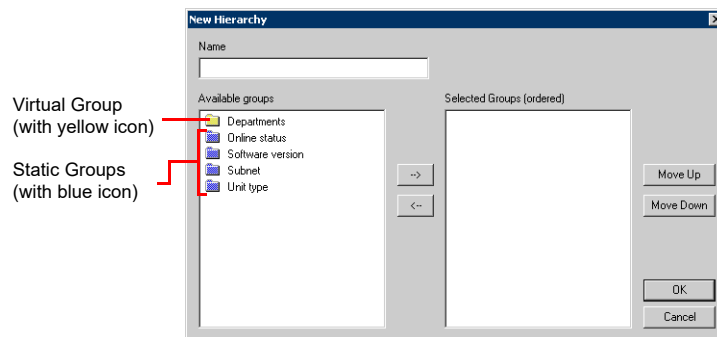
Figure 43: Hierarchies Management Window



2. Click the *New* button.

The following window opens:

Figure 44: New Hierarchy Window



The *Available groups* list on the left displays all the static and virtual groups currently defined. Virtual groups are displayed with a yellow folder icon, while static groups are displayed with a blue folder icon.

3. Enter a name to the new hierarchy in the *Name* field.
It could be something like "Departments_Online".
4. Select which groups you want to use in the hierarchy by transferring the proper groups from the left list to the right list.

Select the group to transfer and click the right arrow between the lists. To remove a group from the hierarchy, select it and click the left arrow.

In the *Department_Online* example, you could transfer the *Department* virtual group and the *Online status* static group.

5. Once you have selected the groups to use, sort them in the order you want them displayed.
In the *Selected Groups* list on the right, select the group to move and either click the *Move Up* or *Move Down* button. This step is important because the groups are displayed in levels in the Administrator window, the first one in the *Selected Groups* list being the first level, the second one the second level, etc.
6. When the new hierarchy is properly defined, click *OK*.
The new hierarchy is added to the list of available hierarchies.

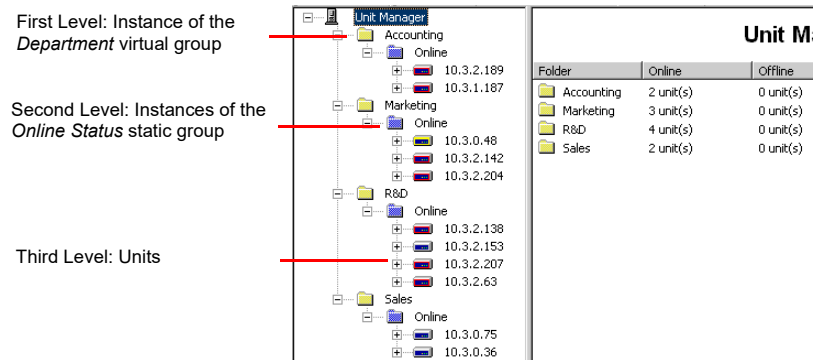
Applying a Hierarchy

Select an existing hierarchy to apply to the list of units to show/hide units as you need.

► To apply a hierarchy:

1. In the *Hierarchy* drop-down menu of the UMN tool bar, select the specific one to apply.
For instance, you could select the *Department_Online* hierarchy created **above**. The tree list is modified according to the hierarchy you have selected.

Figure 45: Levels Example



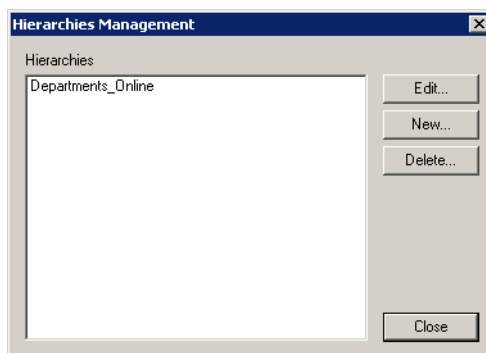
Note: Right-clicking an instance in the tree list and selecting the *Delete* option in the context-sensitive menu that opens deletes all units under this instance. Since the instance no longer has units associated to it, it disappears from the tree list, but it is still available in the *Virtual Groups Management* window if you want to assign other units to it.

Modifying a Hierarchy

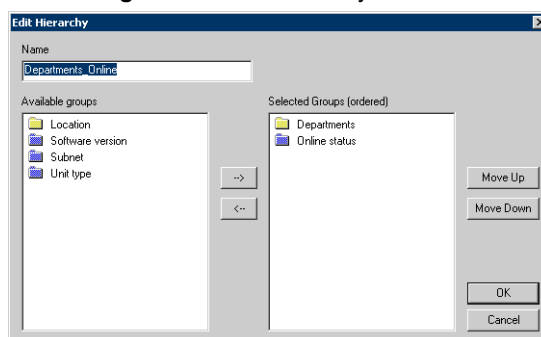
You can modify a hierarchy.

► To modify an existing hierarchy:

1. Click the  icon of the UMN tool bar.
You can also access the *Group* menu and select the *Hierarchies* task. The following window opens:

Figure 46: Hierarchies Management Window

2. Select the hierarchy to modify.
3. Click the *Edit* button or double-click the selected hierarchy.
The following window opens:

Figure 47: Edit Hierarchy Window

4. If applicable, rename the hierarchy.
5. Add/remove groups to the hierarchy as needed.
6. When the hierarchy is properly modified, click *OK*.

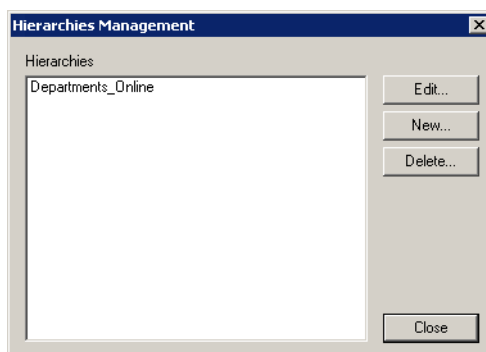
Copying a Hierarchy

You can copy a hierarchy.

► To copy a hierarchy:

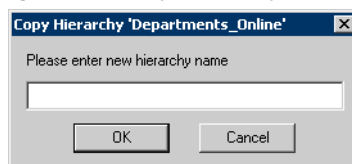
1. Click the  icon of the UMN tool bar.

You can also access the *Group* menu and select the *Hierarchies* task. The following window opens:

Figure 48: Hierarchies Management Window

2. Select the hierarchy to copy.
3. Click the *Copy* button.
The following window opens:

Figure 49: Copy Hierarchy Window



4. Enter the name of the new hierarchy, and then click *OK*.

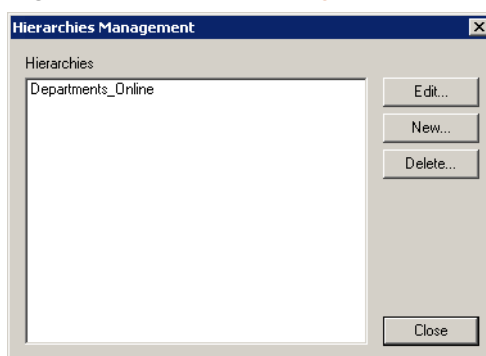
Deleting a Hierarchy

You can delete a hierarchy.

► To delete a hierarchy:

1. Click the  icon of the UMN tool bar.
You can also access the *Group* menu and select the *Hierarchies* task. The following window opens:

Figure 50: Hierarchies Management Window



2. Select the hierarchy to delete.
3. Click the *Delete* button.
The hierarchy is deleted.

Filters

Filters are display criteria you can apply to the list of units to further customize how to display units. A filter may be simple (only uses one group condition) or complex (uses a combination of as many logical and group conditions as you want).

Filter Logical Expressions

Before working with filters, you need to be familiar with writing filters and with using the tree in the *New Filter* and *Edit Filter* windows.

A Filter is a logical expression that consists of:

- One or more group conditions
A condition consists of a group (all the virtual and static groups currently available), a relational operator (*is* or *is not*), and an instance to be compared to the value of the group.

For example, a condition might be:

```
Unit type is not 4104
```

Unit type is a group selected from the list of groups, *is not* is the relational operator, and *4104* is the value to be located in the *Unit type* group.

- The logical operators that bind the conditions together: AND and OR

For example, you can use all unit types that are not 4104 and are also part of the Accounting department. You need the following two conditions bound together with the logical operator AND:

```
Unit type is not 4104
```

```
Departments is Accounting
```

Notice the tree format the UMN uses for filters. Once you get used to this format, you can easily determine what the filter does. Also notice that the *Text representation* field at the bottom of the *New/Edit Filter* window allows you to review the query in a text format.

Creating a New Filter

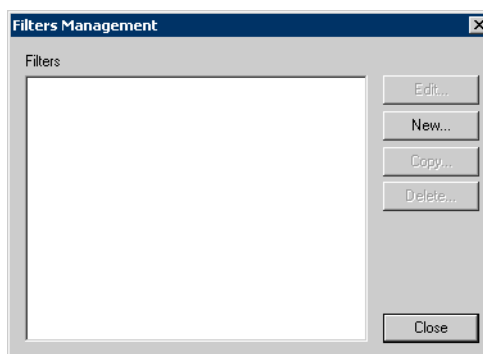
A simple filter only uses one group condition, while a complex filter may use as many group conditions and logical conditions as you want.

- To create a new filter:

1. Click the  icon of the UMN tool bar.

You can also access the *Group* menu and select the *Filters* task. The following window opens:

Figure 51: Filters Management Window



2. Click the *New* button.

The following window opens:

Figure 52: New Filter Window

3. Enter a name for the new filter in the *Name* field.
To follow the example used in previous sections, it could be something like “Accounting”.
4. Write queries that will make up the new filter.
5. If you want to create a complex filter with more than one group conditions, click the *New AND* or *New OR* button in the *Logical conditions* section.
This becomes the root of your filter definition.
 - AND: Means that the AND logical condition is applied to all the conditions created under it.
 - OR: Means that the OR logical condition is applied to all the conditions created under it.
6. In the *Group conditions* section, select a group from the *Group* drop-down list box.
This box lists all the virtual and static groups currently available. Select one of these groups to access the other two parameters.
7. In the *Group conditions* section, select an operator from the *Operator* drop-down list.
You have the choice between:
 - is
 - is not
8. In the *Group conditions* section, type in a value or select one from the *Instance* drop-down list.

Table 17: Instances for Each Group

Group	Choice in the <i>Instance</i> field
Any virtual group	Lists all the instances created under this group.
<i>Online status</i> static group	Available values are <i>Online</i> and <i>Offline</i> .
<i>Unit type</i> static group	Lists all the unit types currently connected to the UMN.

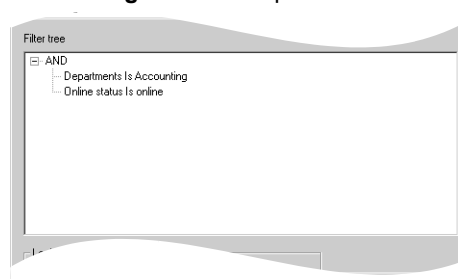
Table 17: Instances for Each Group (Continued)

Group	Choice in the <i>Instance</i> field
<i>Software version</i> or <i>Subnet</i> static groups	Type a proper value in this field. For instance, a proper value for the <i>Subnet</i> group can be <i>192.170.0</i>. You can use the following special characters when defining the <i>Instance</i> field: Asterisk (*): You can use the asterisk as a substitute for zero or more characters. For instance, to filter all subnets under 192.168, type the following: 192.168.0* Pipe (): You can use the “ ” operator (or) to define a range. For instance, to filter subnets 192.168 or 192.169, type the following: 192.168.0 192.169.0

This value is compared with the value of the selected group for each available item.

9. Click the *Add* button to place this condition in the *Filter Tree* box.
10. To add more conditions for this operator, repeat steps 4 to 9 for each additional condition. Then go on to step 11.
You can only add new conditions by selecting a logical condition. If you select a group condition, the *Add* button in the *Groups condition* section becomes a *Modify* button and you can edit the group condition.
11. (Optional) To add another logical operator:
 - Select an existing logical operator (the one that should precede the new operator in the query and, therefore, be its parent in the tree).
 - Click the *New AND* or *New OR* button.
 - Repeat steps 6–9.

You can change a AND logical condition to a OR by selecting the condition and clicking the *Toggle AND/OR* button.
12. (Optional) Repeat step 7 for additional logical operators.
You can add as many levels and/or logical conditions as you want.
13. If you want to remove a condition (logical or group), select it and click the *Remove condition* button.
A text representation of the filter is displayed in the *Text representation* field at the bottom of the window.

Figure 53: Complex Filter

14. When the new filter is properly defined, click *OK*.
The new filter is added to the list of available filters.

Applying a Filter

You can select an existing filter and apply it to the list of units to show/hide units as you need.

► **To apply a filter:**

1. In the *Filter* drop-down menu of the UMN, select the specific one to apply.
For instance, you could select the *Accounting* filter created **above**. The tree list is modified according to the filter you have selected. In the example, only the units assigned to the Accounting instance and currently online are displayed.

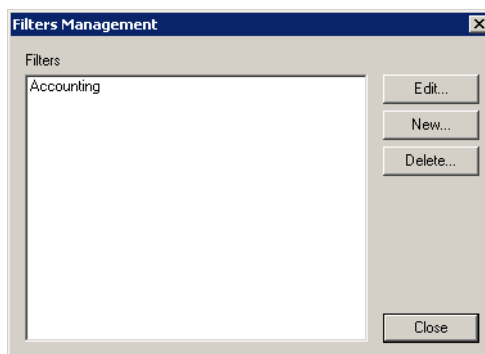
Modifying a Filter

You can modify a filter.

► **To modify a filter:**

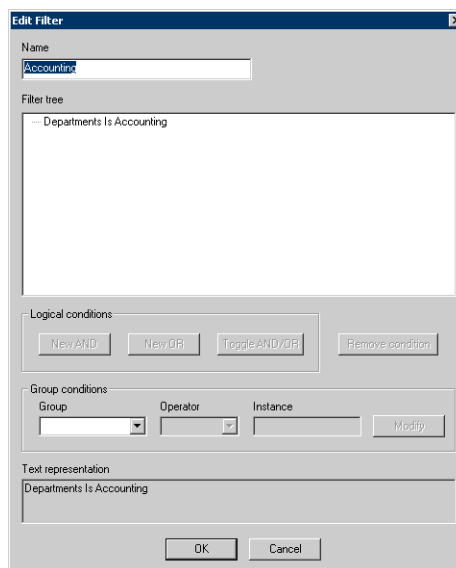
1. Click the  icon of the UMN tool bar.
You can also access the *Group* menu and select the *Filters* task. The following window opens:

Figure 54: Filter Management Window



2. Select the filter to modify.
3. Click the *Edit* button.
The following window opens:

Figure 55: Edit Filter Window



4. If applicable, rename the filter.
5. Modify the filter **according to the explanations given in "Creating a New Filter" on page 51.**
6. When the filter is properly modified, click *OK*.

Copying a Filter

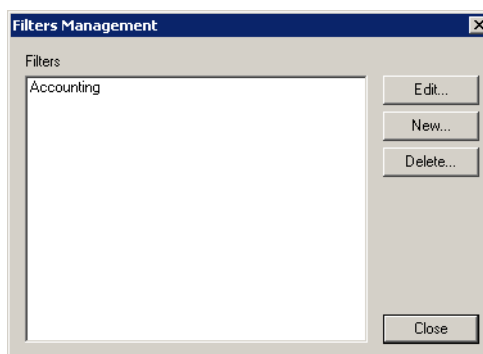
You can copy a filter.

► **To copy a filter :**

1. Click the  icon of the UMN tool bar.

You can also access the *Group* menu and select the *Filters* task. The following window opens:

Figure 56: Filter Management Window

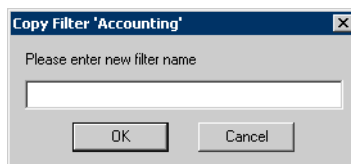


2. Select the filter to copy.

3. Click the *Copy* button.

The following window opens:

Figure 57: Copy Filter Window



4. Enter the name of the new filter, and then click *OK*.

Deleting a Filter

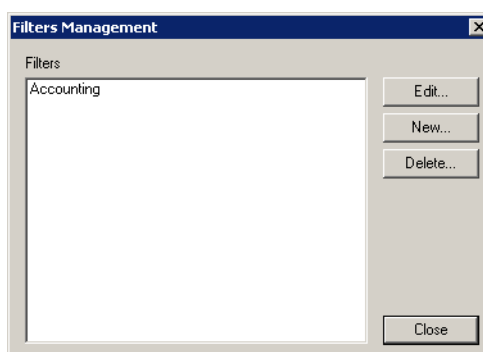
You can delete a filter.

► **To delete a filter:**

1. Click the  icon of the UMN's tool bar.

You can also access the *Group* menu and select the *Filters* task. The following window opens:

Figure 58: Filters Management Window



2. Select the filter to delete.
3. Click the *Delete* button.
The filter is deleted.

Performing Actions on Mediatrix Units

The UMN lets you perform a number of actions on Mediatrix units.

Downloading a Software Version

The following describes how to perform a software download. The procedure differs for analog and digital Mediatrix units. It is also different if you are performing a software download on a Mediatrix 3000 Series or a Mediatrix 4400 Series unit.

Downloading a software version into the Mediatrix unit requires a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.



Note: Refer to [“Chapter 13 - Software Download Parameters” on page 127](#) if you want to configure automatic update parameters.

Software Download – Analog Units

The following describes how to perform a software download on Mediatrix analog units. The procedure slightly differs depending on the version of the unit (SIP v2.x, SIP/MGCP v4.x/v5.x, or Dgw v1.1/2.0).

Version SIP 2.x Units Software Download

The following describes how to download a software version into a SIP v2.x Mediatrix unit.

► **To download a software into the selected Mediatrix unit (SIP v2.x):**

1. In the UMN, set the software download information. See [“Software and Emergency Download” on page 71](#).
2. Right-click the Mediatrix unit into which download a new software.
3. In the context sensitive menu that opens, select the *Action > Download Software* option.
If the Mediatrix unit is not in use, it downloads the software available on the software server. The unit cannot be used during the download time, which varies depending on the performance of the network to which the Mediatrix unit is connected.
A message indicates that the software download has started. Approximately 10 to 20 seconds after receiving this message, you can refresh the Mediatrix unit information to see the result of the software download.
If the unit is in use, the software download is not processed.

Version SIP/MGCP 4.x/5.x Units Software Download

The following describes how to download a new software version into a SIP/MGCP v4.x/v5.x Mediatrix unit.

► **To download a new software into the selected Mediatrix unit (SIP/MGCP v4.x/v5.x units):**

1. In the UMN, set the software download information. See [“Software and Emergency Download” on page 71](#).
2. Extract the contents of the zip file that contains the software information. Be sure to use the defined folder name. It will create a directory that includes the files required for the Mediatrix unit to properly update its software.



Caution: Do not change the name or content of the directory extracted. Media5 suggests that a folder, named identically to the software build, be available and used for the files related to that build only. Each folder should include only one delivery to ensure accuracy.

3. In the UMN, right-click the Mediatrix unit into which download a new software.
4. In the context sensitive menu that opens, select either one of the following options: *Action > Download Software (Abrupt)* or *Action > Download Software (Graceful)*.
 - Abrupt download: starts the download immediately.
 - Graceful download: waits for the state of all ports to be locked, and then starts the download.

If the Mediatrix unit is not in use, it downloads the software available on the software server. The unit cannot be used during the download time, which varies depending on the performance of the network to which the Mediatrix unit is connected.

A message indicates that the software download has started. Approximately 10 to 20 seconds after receiving this message, you can refresh the Mediatrix unit information to see the result of the software download.

If the Mediatrix unit is in use, the software download is not processed.

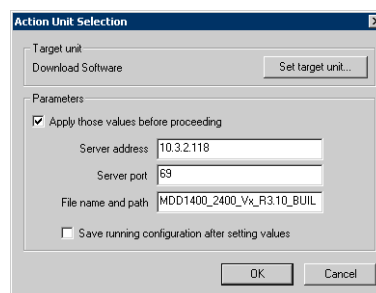
Software Download – Digital Units

The following describes how to perform a software download on Mediatrix digital units.

► **To download a new software into the selected Mediatrix digital unit:**

1. In the UMN, right-click the Mediatrix digital unit into which download a new software.
2. In the context sensitive menu that opens, select the following option: *Action > Download Software*. The following window opens:

Figure 59: Download Software Window



3. If applicable, access the *Parameters* section and set software download parameters by checking the *Apply those values before proceeding* option.

If you do not set these parameters, the UMN uses the parameters that are already set in the MIB of the Mediatrix unit.

You can define the following parameters:

Table 18: Software Download Parameters

Parameter	Description
Server address	IP address of the TFTP server on which is located the software to download.
Server port	IP port number of the TFTP server on which is located the software to download.
File name and path	Server path and file name of the firmware batch file.

This information will be set in the running configuration upon clicking on *OK*.

4. If applicable, save the information set in the running configuration into the startup configuration of the unit by checking the *Save running configuration after setting values* option.
See [“Synchronizing vs Refreshing the List” on page 66](#) for more details.
5. To download the software to several Mediatrix units, click the *Set target unit* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).



Caution: Be careful with the Mediatrix digital units version you select. Downloading the software into different versions of digital units may cause some problems.

6. Click *OK* to start the process.
Please refer to the digital unit's *Software Configuration Guide* for more details on the software download process.

Software Download – Dgw 1.1/2.0 Units

The following describes how to perform a software download on Dgw v1.1/2.0 units.

► To download a software into the selected Dgw 1.1/2.0 unit:

1. In the UMN, set the software download information. See [“Software Download Window \(Dgw v1.1/2.0 Units\)” on page 135](#).
2. Extract the contents of the zip file that contains the software information. Be sure to use the defined folder name. It will create a directory that includes the files required for the Mediatrix unit to properly update its software.



Caution: Do not change the name or content of the directory extracted. Media5 suggests that a folder, named identically to the software build, be available and used for the files related to that build only. Each folder should include only one delivery to ensure accuracy.

3. In the UMN, right-click the Mediatrix unit into which download a new software.
4. In the context sensitive menu that opens, select the *Action > Download Software (Abrupt)* option.
5. To download the software to several Mediatrix units, click the *Set target unit* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).



Caution: Be careful with the Mediatrix digital units version you select. Downloading the software into different versions of digital units may cause some problems.

6. Click *OK* to start the process.
Please refer to the *Dgw 1.1/2.0 Software Configuration Guide* for more details on the software download process.

Downloading a Configuration File

The following describes how to perform a configuration file download. The procedure differs for analog and digital Mediatrix units.



Note: Refer to [“Chapter 12 - Configuration File Fetching Parameters” on page 119](#) if you want to configure automatic update parameters.

Configuration Download – Analog Units

You can download a configuration file into the Mediatrix unit to provide it with new parameters. This file, saved in the `\CfgFile` directory, is named `XXX.cfg`, where `XXX` represents the MAC address of the unit. You can update the configuration file corresponding to a Mediatrix unit at any time. See [“Uploading a Configuration File” on page 62](#) for more details.



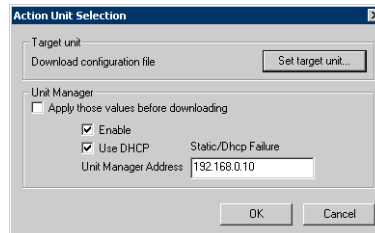
Note: The UMN accepts configuration files modified by users with a size between 0 and 512 KB. If the file size is null or over 512 KB, the UMN displays an error message in the *Status* section of the unit's *Overview* page.

When sending this file, the UMN converts it to XML format, which increases the file size. The unit that receives the configuration file may thus reject it, even if it is not over 512 KB when you edit it.

► To download a configuration file into a unit:

1. Right-click the Mediatrix unit into which download a configuration file.
2. In the context sensitive menu that opens, select the *Configuration File > Transfer to unit* option. The following window opens.

Figure 60: Action Unit Selection Window



This window defines the parameters to retrieve the configuration file.

3. If you do not want to send the location information to the unit, uncheck the *Apply those values before downloading* option and go to step 6. This assumes that the unit currently has the most recent information.
4. If you want the Mediatrix unit to connect to the UMN, check the *Enable* option. In that case, the unit uses the automated connection method. See [“Appendix B - Unit Collection Methods” on page 189](#) for more details.
5. Set the IP address information.
 - If you want the Mediatrix unit to receive the UMN IP address via a DHCP server, check the *Use DHCP* option.
 - If you want to enter a static IP address where to locate the configuration server, uncheck the *Use DHCP* option and enter the IP address in the *Unit Manager Address* field.
6. To download the configuration file to several Mediatrix units, click the *Set target unit* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).
7. Click *OK* to start the process.

Startup Configuration Download – Digital Units

You can download a startup configuration file into the Mediatrix digital unit to provide it with new parameters. This requires a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the configuration file server.

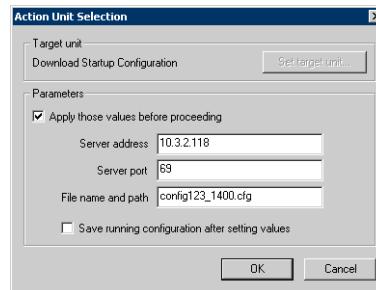
It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

► **To download a startup configuration into the selected Mediatrix digital unit:**

1. In the UMN, right-click the Mediatrix digital unit into which download the startup configuration.
2. In the context sensitive menu that opens, select the following option: *Action > Download Startup Configuration*.

The following window opens:

Figure 61: Download Startup Configuration Window



3. If applicable, access the *Parameters* section and set startup configuration download parameters by checking the *Apply those values before proceeding* option.

If you do not set these parameters, the UMN uses the parameters that are already set in the MIB of the Mediatrix unit.

You can define the following parameters:

Table 19: Startup Configuration Download Parameters

Parameter	Description
Server address	IP address of the TFTP server on which is located the startup configuration to download.
Server port	IP port number of the TFTP server on which is located the startup configuration to download.
File name and path	Server path and file name of the file to download into the Mediatrix unit.

This information will be set in the running configuration upon clicking on *OK*.

4. If applicable, save the information set in the running configuration into the startup configuration of the unit by checking the *Save running configuration after setting values* option.

See [“Synchronizing vs Refreshing the List” on page 66](#) for more details.

5. Click *OK* to start the process.

Please refer to the digital unit's *Software Configuration Guide* for more details on the startup configuration download process.

Uploading a Configuration File

The following describes how to perform a configuration file upload. The procedure differs for analog and digital Mediatrix units.

Configuration Upload – Analog Units

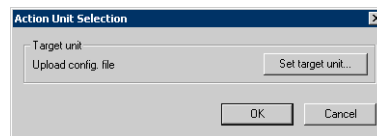
The UMN creates a configuration file for each Mediatrix unit that requests a default configuration. This file, saved in the `\CfgFile` sub-directory, is named `XXX.cfg`, where `XXX` represents the MAC address of the unit. You can update this file at any time with the configuration parameters of the selected unit. If the configuration file already exists, the UMN overwrites it.



Note: The UMN accepts configuration files with a size between 0 and 512 KB. If the file size is null or over 512 KB, the UMN displays an error message in the *Status* section of the unit's *Overview* page.

- **To upload the current configuration of the selected Mediatrix unit into a configuration file:**
 1. Right-click the Mediatrix unit from which upload the current configuration.
 2. In the context sensitive menu that opens, select the *Configuration File > Transfer from unit* option. The following window opens.

Figure 62: Action Unit Selection Window



This window updates the configuration file of the selected unit with the current configuration.

3. To update the configuration file of several Mediatrix units, click the *Set target unit* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).
4. Click *OK* to start the process.

Startup Configuration Upload – Digital Units

You can take the current configuration of the Mediatrix digital unit and upload it to a startup configuration file on the designated TFTP server.

Uploading a startup configuration file into the unit requires a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the configuration file server.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

- **To upload a startup configuration from the selected Mediatrix digital unit:**
 1. In the UMN, right-click the Mediatrix digital unit from which to upload the startup configuration.
 2. In the context sensitive menu that opens, select the following option: *Action > Upload Startup Configuration*. The following window opens:

Figure 63: Upload Startup Configuration Window

3. If applicable, access the *Parameters* section and set startup configuration upload parameters by checking the *Apply those values before proceeding* option.
If you do not set these parameters, the UMN uses the parameters that are already set in the MIB of the Mediatrix unit.
You can define the following parameters:

Table 20: Startup Configuration Upload Parameters

Parameter	Description
Server address	IP address of the TFTP server where to upload the startup configuration.
Server port	IP port number of the TFTP server where to upload the startup configuration.
File name and path	Server path and file name of the file where to upload the startup configuration.

This information will be set in the running configuration upon clicking on OK.

4. If applicable, save the information set in the running configuration into the startup configuration of the unit by checking the *Save running configuration after setting values* option.
See [“Synchronizing vs Refreshing the List” on page 66](#) for more details.
5. To upload the startup configuration of several Mediatrix units, click the *Set target unit* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).



Caution: Be careful with the Mediatrix digital units version you select. Uploading the startup configuration from different versions of digital units to the same file may cause some problems.



Note: The *Set target units* procedure does not apply the value set in the *File name and path* field if you have selected several units. Units will rather receive a file name built from each unit's MAC address, for instance “0090F800059A.cfg”. No path are allowed in that case, which means that all *mac.cfg* type files will be uploaded to the root path of the TFTP server.

6. Click OK to start the process.
Please refer to the digital unit's *Software Configuration Guide* for more details on the startup configuration download process.

Saving a Configuration File to XML Format

You can convert an existing configuration file to the XML format for units that support XML.



Note: This option is available for SIP v5.0 and MGCP v5.0 units only.

When saving the configuration file to XML, the server takes the unit's configuration file (from the server folder *UnitManager\CfgFile*) and converts it to XML format. The new XML file is saved as "XXXXXXXXXXXXX.xml" in the server folder "UnitManager\CfgFile".



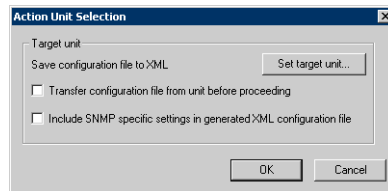
Note: The server only converts the configuration file it already has on disk to XML. It does not get the configuration file from the unit. In order to get the current unit parameter values in the XML file, you should select the *Transfer configuration file from unit before proceeding* option in the *Action Unit Selection* window, as described in Step 3 below.

If you perform a "Save to XML" action when the server does not have the unit's configuration file, the UMN generates both .cfg AND .xml configuration files from the default configuration file for this unit type (taken from the server folder "UnitManager\DefaultCfgFile").

► To save the configuration of the selected Mediatrix unit in XML:

1. Right-click the Mediatrix unit for which to save the configuration file in XML format.
2. In the context sensitive menu that opens, select the *Configuration File > Save to XML* option. The following window opens.

Figure 64: Action Unit Selection Window



This window saves the configuration file of the selected unit in XML format.

3. If you want to update the configuration file with the current unit's configuration before converting the file to XML, select the *Transfer configuration file from unit before proceeding* option.
4. If you want to include generic SNMP settings into the XML file, check the *Include SNMP specific settings in generated XML configuration file* option.

This appends the contents of the *SnmpGenericTemplate.xml* file at the end of the generated XML file. The *SnmpGenericTemplate.xml* contains the default Media5 parameters related to SNMP. Default values enable SNMPv1, SNMPv2, and SNMPv3 and provide default Media5 credentials for SNMPv3.

When this XML configuration file is sent back to the unit, the unit compares it to the last configuration file it received. If the two configuration files are different, the unit changes its configuration accordingly.

5. To save the configuration file of several Mediatrix units, click the *Set target unit* button. Follow the procedure described in ["Setting Multiple Units" on page 39](#).
6. Click *OK* to start the process.

Saving a Configuration File to Dgw Config Script Format

In the event you want to upgrade a unit from the SIP v5.0 to Dgw v2.0 applicaion version, you can convert an existing configuration file to the Dgw configuration script format. This option is available for the following units:

- ▶ Mediatrix 4102/4102S
- ▶ Mediatrix 4104
- ▶ Mediatrix 4108
- ▶ Mediatrix 4116
- ▶ Mediatrix 4124

When saving the configuration file to Dgw config script, the server takes the unit's configuration file (from the server folder *UnitManager\CfgFile*) and converts it to the Dgw format. The new file is saved as "XXXXXXXXXXXX_DGW_Script.cfg" in the server folder "*UnitManager\CfgFile*", where the Xs correspond to the unit's MAC address.



Note: The server only converts the configuration file it already has on disk. It does not get the configuration file from the unit. In order to get the current unit parameter values in the Dgw config script, you should select the *Transfer configuration file from unit before proceeding* option in the *Action Unit Selection* window, as described in Step 3 below.

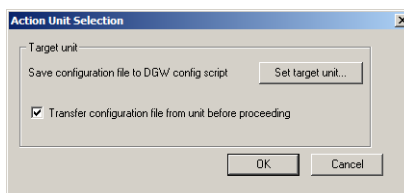
If you perform a "Save to Dgw config script" action when the server does not have the unit's configuration file, an error message is displayed alerting that no configuration file can be found.

▶ **To save the configuration of the selected Mediatrix unit in Dgw config script:**

1. Right-click the Mediatrix unit for which to save the configuration file in Dgw config script.
2. In the context sensitive menu that opens, select the *Configuration File > Save to Dgw config script* option.

The following window opens.

Figure 65: Action Unit Selection Window



This window saves the configuration file of the selected unit in Dgw config script format.

3. If you want to update the configuration file with the current unit's configuration before converting the file to Dgw config script, select the *Transfer configuration file from unit before proceeding* option.
4. To save the configuration file of several Mediatrix units, click the *Set target unit* button. Follow the procedure described in ["Setting Multiple Units" on page 39](#).
5. Click *OK* to start the process.

Restarting a Unit

You can restart a selected unit when this is required.

► **To restart the selected Mediatrix unit:**

1. Right-click the Mediatrix unit to restart.
2. In the context sensitive menu that opens, select either one of the following options: *Action > Restart (Abrupt)* or *Action > Restart (Graceful)*.
 - Abrupt restart: restarts immediately.
 - Graceful restart: waits for the state of all ports to be locked, and then restarts.



Note: The *Graceful* option is not available on Mediatrix digital units.

If the unit is not in use, a message informs you that it is about to restart. Approximately 10 to 20 seconds after receiving this message, you can refresh the unit information.

If it is in use, the restart is not processed.

Synchronizing vs Refreshing the List

The UMN can synchronize or refresh its list of units.

Synchronizing the List

When synchronizing its list, the UMN contacts its server and checks the online status of all Mediatrix units currently in the list.

To synchronize the list, right-click the *Unit Manager* level and select *Synchronize* in the context sensitive menu that opens. You can also select the *Synchronize* task of the *Tree Item* menu.

Refreshing the List

There are two refresh options: *Refresh* and *Refresh tree*. When refreshing its list, the UMN updates the information it has and rebuilds the tree display, which could be annoying if you have expanded and collapsed branches. On the other hand, the *Refresh tree* option does not alter the expanded/collapsed display, unless there are changes in the units locations.

To refresh the list, right-click the *Unit Manager* level and select either *Refresh* or *Refresh tree* in the context sensitive menu that opens. You can also select either the *Refresh* or *Refresh tree* task of the *Tree Item* menu.

Removing all DHCP Options

Using static IP addresses allows you to bypass the DHCP server or still be able to use the Mediatrix unit if you are not running a DHCP server.



Note: This option is not available on Mediatrix digital units.

In this case, having one or more configuration source variable set to DHCP will slow down the restart process. If any information is set to come from the DHCP server (for example, SNTP address), the restarting unit will wait for a maximum period of two minutes if the DHCP server cannot be reached, even if most other settings are set to “static”.

The reason for this delay is that the Mediatrix unit cannot function as configured if part of its configuration (the DHCP information) is unavailable.

You can set all configuration sources the Mediatrix unit supports to “static”.



Note: This feature applies to SIP v4.4, SIP v4.5, and H.323 v4.0 units. It can be used either in normal mode of operation or when the unit is in Recovery mode.

► **To remove all DHCP options of the selected Mediatrix unit:**

1. Right-click the Mediatrix unit for which remove all DHCP options.
2. In the context sensitive menu that opens, select the *Action > Remove all DHCP options* option.

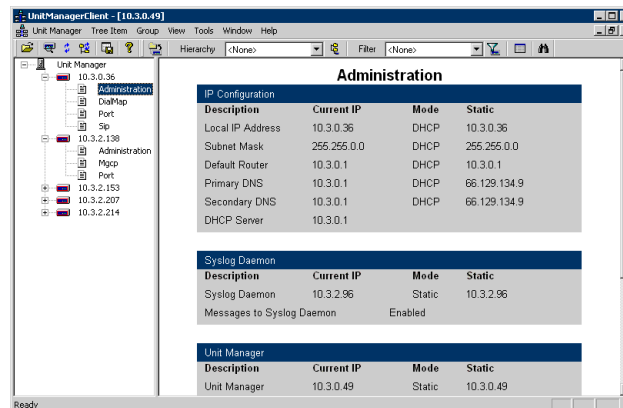
Administration Parameters

This **chapter** describes the Administration parameters you can set. These are the parameters and IP addresses used by a Mediatrix unit.

Administration Overview

Upon selecting the *Administration* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 66: Administration Parameters Overview



You can change the value of these parameters by accessing the *Administration* window. For Dgw v1.1/2.0 units, an alternate *Administration* window is available.

Administration Window

The *Administration* window allows you to define the IP addresses and other related information of Mediatrix units.

► **To access the *Administration* window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Administration* category.

The *Administration* window opens, which contains several sections.

Figure 67: Administration Window

The screenshot shows the 'Administration' window with the following sections:

- IP Configuration:**
 - ☒ Use DHCP: Static
 - Local IP Address: 192.168.0.1
 - Subnet Mask: 255.255.255.0
 - Default Router: 192.168.0.10
 - Primary DNS: 192.168.0.10
 - Secondary DNS: 192.168.0.10
- Unit Manager Server:**
 - ☒ Enable
 - ☐ Use DHCP: Static
 - Unit Manager: 10.3.123.248
- SNTP Server:**
 - ☐ Enable
 - ☐ Use DHCP: Static
 - SNTP Server: 192.168.0.10
- Syslog Daemon:**
 - ☒ Use DHCP: Static
 - Syslog Daemon: 192.168.0.96
 - Messages: Disabled (dropdown)
- Software Download Servers:**
 - ☒ Use DHCP: Static
 - Primary server: 192.168.0.10
 - Secondary Server: 192.168.0.10
 - Pathname: swdownload

Buttons at the bottom: Set target units..., ☐ Exclude IP Configuration on multiple targets, OK, Cancel.



Note: The *Software and Emergency Download* section slightly differs if you are editing a SIP v2.x, SIP/MGCP v4.x/v5.x, or Dgw v1.1/2.0 unit.



Caution: The Administration window differs if the unit is a Dgw v1.1/2.0 unit. See [“Administration Window \(Dgw v1.1/2.0 Units\)”](#) on page 73.

IP Configuration

The *IP Configuration* section sets the general IP addresses used by the Mediatrix unit.

► To set IP configuration parameters:

- Set the IP addresses information.
 - If you want the Mediatrix unit to receive its IP addresses via a DHCP server, check the *Use DHCP* option.
 - If you want to enter static IP addresses, uncheck the *Use DHCP* option and enter the IP addresses in the corresponding fields.

Table 21 describes the IP addresses you can define.

Table 21: Static IP Addresses Parameters

Parameter	Definition
Local IP address	Local IP address of the Mediatrix unit.
Subnet Mask	Subnet mask used by the Mediatrix unit. The subnet mask enables the network administrator to further divide the host part of the address into two or more subnets.
Default Router	Default router IP address used by the Mediatrix unit. A router is a device that connects any number of LANs.
Primary DNS	Primary Domain Name Server IP address used by the Mediatrix unit. A DNS is an Internet service that translates domain names into IP addresses.

Table 21: Static IP Addresses Parameters (Continued)

Parameter	Definition
Secondary DNS	Secondary Domain Name Server IP address used by the Mediatrix unit.

2. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#). You can exclude the IP addresses you have defined by checking the *Exclude IP Configuration on multiple targets* option. You must then set the IP configuration on the other units.
3. Click *OK* when the changes are done.
The changes are applied to the selected Mediatrix unit(s).

Software and Emergency Download

The *Software and Emergency Download* section defines the parameters for software updates.

► To set Software and Emergency download parameters:

1. Set the IP addresses information.
 - If you want the Mediatrix unit to receive the software servers IP addresses via a DHCP server, check the *Use DHCP* option.
 - If you want to enter static IP addresses, uncheck the *Use DHCP* option and enter the IP addresses in the corresponding fields.

[Table 22 describes the IP parameters you can define.](#)

Table 22: Software Download Configuration Parameters

Parameter	Definition
Primary Server	Primary server running the TFTP protocol to allow the software updates of the Mediatrix unit software.
Secondary Server	Secondary server to contact in case the Mediatrix unit software is interrupted while it is internally updating its software version.
Filename/Pathname	SIP Version 2.x Units: Name of the file that contains the new software. It can have up to 50 alphanumeric characters (a-z, A-Z, 0-9). Spaces and dots are allowed. SIP/MGCP Version 4.x/5.x Units: Name of the directory where the files required for the Mediatrix unit are located. This directory shall be located under the TFTP root path as defined in your TFTP server. Note: If you leave an empty path, the unit looks for the software download information in the root directory of the software download server. Note: You should use the “/” character when defining the path to indicate sub-directories. For instance, <i>c:/temp/download</i>. However, some TFTP servers on Windows do not recognize the “/” character and produce an error. In this case, you should rather use the “\” character. Media5 suggests that a folder, named identically to the software build, be available and used for the files related to that build only. Each folder should include only one delivery to ensure accuracy.

2. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
3. Click *OK* when the changes are done.
The changes are applied to the selected Mediatrix unit(s).

Syslog Daemon

The *Syslog Daemon* section is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from your unit. If no Syslog daemon address is provided by a DHCP server or specified by the administrator, no messages are sent.

For instance, when downloading a new software into a Mediatrix unit, you can monitor each step of the software download phase. Furthermore, if the unit encounters an abnormal behaviour, you may see accurate messages that will help you troubleshoot the problem.

► To set Syslog daemon parameters:

1. Set the IP address information.
 - If you want the Mediatrix unit to receive the IP address of the server running the Syslog daemon via a DHCP server, check the *Use DHCP* option.
 - If you want to enter a static IP address, uncheck the *Use DHCP* option and enter the IP address in the *Syslog Daemon* field.



Note: If no Syslog daemon address is provided by a DHCP server or specified by the administrator, no messages are sent.

2. In the *Messages* drop down menu, set the message state.
The states available are different for SIP v2.x or SIP/MGCP v4.x/v5.x units.

Table 23: Syslog Message States

SIP v2.x States	SIP/MGCP v4.x/v5.x States
• Enabled • Disabled	• Disabled • Critical • Error • Warning • Informational • Debug

3. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
4. Click *OK* when the changes are done.
The changes are applied to the selected Mediatrix unit(s).

Unit Manager Server

The *Unit Manager Server* section defines the parameters to connect to the UMN.

► To set UMN parameters:

1. If you want the Mediatrix unit to connect to the UMN, check the *Enabled* option.
In that case, the unit uses the automated connection method. See [“Unit Collection Methods” on page 189](#) for more details.
2. Set the IP address information.

- If you want the Mediatrix unit to receive the UMN IP address via a DHCP server, check the *Use DHCP* option.
 - If you want to enter a static IP address, uncheck the *Use DHCP* option and enter the IP address in the *Unit Manager* field.
3. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
 4. Click *OK* when the changes are done.
The changes are applied to the selected unit(s).

SNTP

The *SNTP* section defines the parameters to connect to a SNTP server.

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Mediatrix unit. It updates the internal clock of the unit, which is the client of a SNTP server. It is required when dealing with features such as the caller ID.

SNTP is used to synchronize a SNTP client with a SNTP or NTP server by using UDP as transport (see RFC 1769 for more details).



Note: SNTP parameters are available for units that run the following software versions: SIP v2.4, SIP v4.3, SIP v4.4, SIP v4.5, and H.323 v4.0.

► **To set SNTP parameters:**

1. If you want the Mediatrix unit to connect to a SNTP server, check the *Enabled* option.
2. Set the IP address information.
 - If you want the Mediatrix unit to receive the SNTP server IP address via a DHCP server, check the *Use DHCP* option.
 - If you want to enter a static IP address, uncheck the *Use DHCP* option and enter the IP address in the *SNTP Server* field.
3. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
4. Click *OK* when the changes are done.
The changes are applied to the selected unit(s).

Administration Window (Dgw v1.1/2.0 Units)

The *Administration* window allows you to define the IP addresses and other related information of Dgw v1.1/2.0 units. This window differs depending on the unit model.

► **To access the *Administration* window for Dgw 1.1/2.0 units:**

1. Select the unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Administration* category.
The *Administration* window opens, which contains several sections.

Figure 68: Administration Window

The screenshot shows the 'Administration' window with the following sections:

- Uplink (Wan) Configuration:** Source (Dhcp), Local IP (Static) (192.168.10.1/24), Service Name, Protocol (Chap), User Name, Password.
- Host Configuration:** Host Name (allo), Obtain automatically (checked), Domain Name.
- Default Gateway Configuration:** Obtain automatically (checked), Static, Default Gateway (192.168.0.10).
- DNS Configuration:** Obtain automatically (checked), Static, Primary DNS, Secondary DNS, Third DNS, Fourth DNS.
- SNTP Configuration:** Obtain automatically (checked), Static, Host Name (192.168.0.10.123), Time Zone (EST5DST4,M4.1.0/02:00:00,M10), Synchronization Period (1440 min), Synchronization period On Error (60 min).

Buttons at the bottom: Set target units..., Exclude Host Name and Uplink Configuration on multiple targets, OK, Cancel.

Uplink (Wan) Configuration

The *Uplink (Wan) Configuration* section allows you to configure the general uplink information required by the unit to properly connect to the WAN. By default, this interface uses the DHCP connection type.

► To configure uplink parameters:

1. Select the configuration source of the uplink information in the *Source* drop-down menu.

Table 24: Uplink Configuration Sources

Source	Description
DHCP	The value is provided at start-time by querying a DHCP server and using standard DHCP fields or options. Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. This is the default value.
Static	You manually enter the value and it remains the same every time the unit restarts. Use the static configuration if you are not using a DHCP server/PPP peer or if you want to bypass it.
PPPoE	IPv4 over PPP connection, address and network mask are provided by the PPP peer using IPCP. DHCP servers and PPP peers may provide a list of DNS to use.

2. If the uplink configuration source is **Static**, enter the IPv4 address and network mask of the *Uplink* network interface in the *Local IP (Static)* field.
This address is used for incoming signalling, media and management traffic. The default value is **192.168.10.1/24**.
3. If the uplink configuration source is **PPPoE**, set the name of the service requested to the access concentrator (AC) when establishing the next PPPoE connection in the *Service Name* field.
This string is used as the *Service-Name* field of the packet broadcasted to the access concentrators. See RFC 2516 section 5.1 for details.
The field may be set with any string of characters, with a maximum of 255 characters.
If you leave this field empty, the unit looks for any access concentrator.
4. If the uplink configuration source is **PPPoE**, select the authentication protocol to use for authenticating the system to the PPP peer in the *Protocol* drop-down menu.

- PAP: Use the Password Authentication Protocol.
 - CHAP: Use the Challenge Handshake Authentication Protocol.
5. If the uplink configuration source is **PPPoE**, set the PPP user name and password that identify the system to the PPP peer during the authentication process in the *User Name* and *Password* fields. When connecting to an access concentrator, it may request that the unit identifies itself with a specific user name and password.
There are no restrictions, you can use any combination of characters.
 6. To apply changes to several units, click the *Set target units* button. You can exclude the uplink parameters you have defined by checking the *Exclude Host Name and Uplink Configuration on multiple targets* option. You must then set the uplink parameters on the other units.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
 7. Click *OK* when the changes are done.
The changes are applied to the selected unit(s).

Host Configuration

The *Host Configuration* section allows you to configure the host name and domain name of the unit.

► To set the host configuration:

1. Set the system's host name in the *Host Name* field.
The host name is the unique name by which the device is known on a network.
2. Set the domain name information.
 - If you want the unit to automatically receive the domain name, check the *Obtain automatically* option.
The domain name is automatically provided by querying the network server (for instance, through a DHCP server or PPP access concentrator). The value obtained depends on the connection type of the Uplink network interface (see [“Uplink \(Wan\) Configuration” on page 74](#)). Using the automatic configuration assumes that you have properly set your network server with the relevant information.



Note: Some Uplink connection types (for example *Static* and *PPPoE*) cannot obtain domain name information from the network, and therefore lead to no domain name being applied to the system.

- If you want to enter a static domain name, uncheck the *Obtain automatically* option and enter the domain name in the *Domain Name* field.
A domain name is a name of a device on the Internet that distinguishes it from the other systems on the network. For instance: example.com.
When switching from the Static to Automatic configuration source, the last value correctly obtained from the network (if any) is applied to the system.
3. To apply changes to several units, click the *Set target units* button. You can exclude the host name you have defined by checking the *Exclude Host Name and Uplink Configuration on multiple targets* option. You must then set the host name on the other units.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
 4. Click *OK* when the changes are done.
The changes are applied to the selected unit(s).

SNTP Configuration

The *SNTP Configuration* section allows you to configure the SNTP client of the unit. The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Mediatrix unit. SNTP is used to synchronize a SNTP client with a SNTP or NTP server by using UDP as transport. It updates the internal clock of the unit to maintain the system time accurate. It is required when dealing with features such as the caller ID.

The Dgw v1.1/2.0 unit implements a SNTP version 3 client.

► **To set the SNTP client of the unit:**

1. Set the SNTP information.

- If you want the unit to automatically receive the SNTP information, check the *Obtain automatically* option.

The SNTP parameters are automatically provided by querying the network server (for instance, through a DHCP server or PPP access concentrator). The values obtained depend on the connection type of the Uplink network interface (see ["Uplink \(Wan\) Configuration" on page 74](#)). Using the automatic configuration assumes that you have properly set your network server with the relevant information.



Note: Some Uplink connection types (for example *Static* and *PPPoE*) cannot obtain SNTP information from the network, and therefore lead to no SNTP parameters being applied to the system.

- If you want to enter a static SNTP server IP address or domain name and port number, uncheck the *Obtain automatically* option and enter the address in the *Host Name* field.

When switching from the Static to Automatic configuration source, the last values correctly obtained from the network (if any) are applied to the system.

2. If the SNTP configuration source is **Static**, enter a valid string in the *Time Zone* field.

The format of the string is validated upon entry. Invalid entries are refused. The default value is:

EST5DST4,M4.1.0/02:00:00,M10.5.0/02:00:00

See the *Dgw v1.1/2.0 Software Configuration Guide* for more details on the time zone parameters.

3. Set the synchronization information:

Table 25: SNTP Synchronization Information

Field	Description
Synchronisation Period	Time interval (in minutes) between system time synchronization cycles. Each time this interval expires, a SNTP request is sent to the SNTP server and the result is used to set the system time. The maximum value is set to 1 440 minutes, which corresponds to 24 hours.
Synchronisation Period on Error	Time interval (in minutes) between retries after an unsuccessful attempt to reach the SNTP server. The maximum value is set to 1 440 minutes, which corresponds to 24 hours.

4. To apply changes to several units, click the *Set target units* button.

Follow the procedure described in ["Setting Multiple Units" on page 39](#).

5. Click *OK* when the changes are done.

The changes are applied to the selected unit(s).

Default Gateway Configuration

The *Default Gateway Configuration* section allows you to set the default gateway information. The default gateway (also known as default router) is the router to which the unit sends packets when all other internally known routes have failed.

► **To set the default gateway configuration:**

1. Set the default gateway information.

- If you want the unit to automatically receive the default gateway information, check the *Obtain automatically* option.

The default gateway is automatically provided by querying the network server (for instance, through a DHCP server or PPP access concentrator). The values obtained depend on the connection type of the Uplink network interface (see ["Uplink \(Wan\)](#)

[Configuration" on page 74](#)). Using the automatic configuration assumes that you have properly set your network server with the relevant information.



Note: Some Uplink connection types (for example *Static*) cannot obtain default gateway information from the network, and therefore lead to no default gateway being applied to the system.

- If you want to enter a static default gateway IP address or domain name, uncheck the *Obtain automatically* option and enter the address in the *Default Gateway* field.

When switching from the Static to Automatic configuration source, the last value correctly obtained from the network (if any) is applied to the system.

2. To apply changes to several units, click the *Set target units* button.
Follow the procedure described in ["Setting Multiple Units" on page 39](#).
3. Click *OK* when the changes are done.
The changes are applied to the selected unit(s).

DNS Configuration

The *DNS Configuration* section allows you to set up to four Domain Name Servers (DNS) to which the unit can connect. The DNS servers list is the ordered list of DNS servers that the unit uses to resolve network names. DNS query results are cached on the system to optimize name resolution time.

► To set the DNS configuration:

1. Set the DNS information.
 - If you want the unit to automatically receive the DNS information, check the *Obtain automatically* option.

The DNS servers are automatically provided by querying the network server (for instance, through a DHCP server or PPP access concentrator). The values obtained depend on the connection type of the Uplink network interface (see ["Uplink \(Wan\) Configuration" on page 74](#)). Using the automatic configuration assumes that you have properly set your network server with the relevant information.



Note: Some Uplink connection types (for example *Static*) cannot obtain DNS information from the network, and therefore lead to no DNS servers being applied to the system.

- If you want to enter up to four static DNS addresses, uncheck the *Obtain automatically* option and enter the addresses in the *Primary DNS*, *Secondary DNS*, *Third DNS*, and *Fourth DNS* fields.

When switching from the Static to Automatic configuration source, the last values correctly obtained from the network (if any) are applied to the system.

2. To apply changes to several units, click the *Set target units* button.
Follow the procedure described in ["Setting Multiple Units" on page 39](#).
3. Click *OK* when the changes are done.
The changes are applied to the selected unit(s).

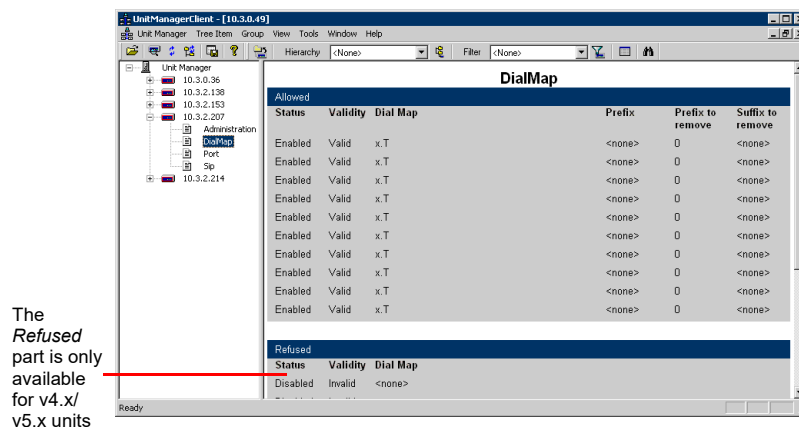
Dial Map Parameters

A Dial Map¹ (also known as Digit Map) allows you to configure the ports of a Mediatrix unit by comparing the number users just dialed to a string of arguments. If they match, users can make the call. If not, users will get a busy signal. It is thus essential to define very precisely a Dial Map before actually implementing it, or your users may encounter calling problems. See “How to Use a Dial Map” on page 83 for more information.

Dial Map Overview

Upon selecting the *Dial Map* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 69: Dial Map Parameters Overview



Dial Maps are checked sequentially. If a phone number potentially matches two of the rules, the first rule encountered is applied.



Note: SIP v2.x only – Dial maps assume that you have properly set the *Area Code* and *Country Code* parameters in the *SIP* section. See “[SIP Parameters](#)” on page 106 for more details.

You can change the value of the Dial Map parameters by accessing the *Dial Map* window.

Dial Map Window

The Dial Map window allows you to define the dial map strings that are used when making calls.

► **To access the *Dial Map* window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Dial Map* category.
The *Dial Map* window opens.

1. Valid only for units that run the SIP or H.323 signalling protocol.

Figure 70: Dial Map Window – SIP v2.x Units

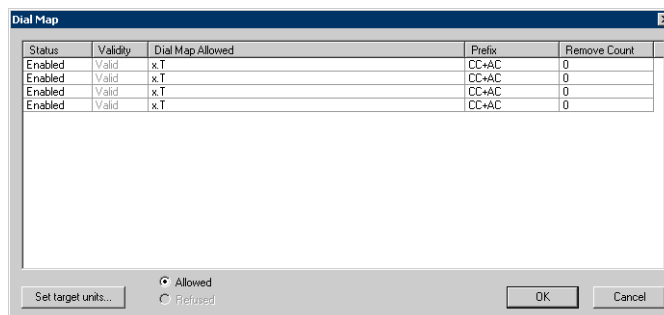
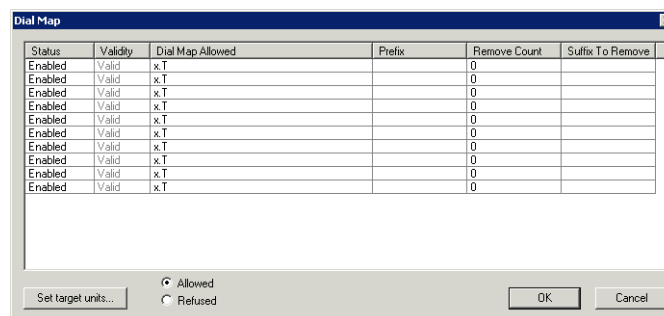


Figure 71: Dial Map Window – SIP/MGCP v4.x/v5.x units



You can define:

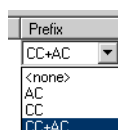
- up to four (4) dial map rules in SIP v2.x units
- up to ten (10) dial map rules in SIP/MGCP v4.x/v5.x units.
- up to ten (10) refused dial map rules in SIP/MGCP v4.x/v5.x units. A refused dial map may be defined to restrict your users to call specific numbers; for instance to accept all 1-8xx numbers except 1-801.

3. **SIP/MGCP v4.x/v5.x units only:** Click the *Allowed* or *Refused* option according to the type of dial maps you want to work with.
4. Modify the values you want.

To modify a value:

- Select it in the row you want to change.
This value becomes highlighted.
- Modify the value for the variable, and then press the <Enter> key of your keyboard
If the value offers choices, you can click twice on the variable at a one second interval and a drop-down menu with all the available values displays. Select the proper value.

Figure 72: Drop Down Menu



You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 26: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

5. Select the Dial Map rule to set in the list.

The following settings can be configured:

Table 27: Dial Map Rules Parameters

Column	Description
Status	When enabled, the Mediatrix unit compares the number users dial to the valid Dial Maps for a match. Each of them is compared and, if there is a match with any rule, the call proceeds.
Validity	The Dial Map is validated when you change cells. The result (valid, invalid) is displayed.
Dial Map	Actual Dial Map string to which the number is compared. A valid Dial Map could be: (011x.T 011x.# 1xxxxxxxxx [2-8]xxxxxx) Note: Enclose the dial map in parenthesis when using the " " feature. See "Creating a Dial Map" on page 82 for more details.
Prefix	Adds the selected digits to the number dialed by users. Values: CC, AC, CC+AC Note: Does not apply to refused dial maps.
Remove Count	When making a call, specifies the number of digits to remove from the number dialed by users. A complete and valid telephone number shall contain a Country Code, an Area Code, and a number. Note: Does not apply to refused dial maps.
Suffix to remove	Post-Dial number modification. This setting specifies a string to look for and remove from the end of the dialed number. This can be especially helpful if one of your dial maps contains a terminating character that shall not be dialed. Note: This column is available only for v4.x/v5.x units and does not apply to refused dial maps.



Note: When doing PSTN emulation with the UMN, the Mediatrix unit's ports identify themselves to the server as the combination of their current CC+AC+Assigned network telephone number. When making a call, the server is expecting such a number. The various Dial Map rules thus allow an administrator to configure what the unit shall do to obtain such a number from the dialed number.

6. To apply changes to more than one Mediatrix unit, click the *Set target units* button.
Follow the procedure described in ["Setting Multiple Units" on page 39](#).

Creating a Dial Map

Because it is hard for the Mediatrix unit to predict how many digits it needs to accumulate before transmission, the Dial Map could be used, for instance, to determine exactly when there are sufficient digits entered from the user to place a call.

For instance, using the phone on your desk, you can dial the following numbers:

Table 28: Number Examples

Number	Description
0	Local operator
00	Long distance operator
xxxx	Local extension number
8xxxxxxx	Local number
#xxxxxxx	Shortcut to local number at other corporate sites
91xxxxxxxxxx	Long distance numbers
9011 + up to 15 digits	International number

The solution to this problem is to load the unit with a Dial Map that corresponds to the dial plan. This Dial Map is expressed by using a specific syntax.

A unit that detects digits or timers applies the current dial string to the Dial Map, attempting a match to each regular expression in the Dial Map in lexical order.

- ▶ If the result is under-qualified (partially matches at least one entry in the Dial Map), waits for more digits.
- ▶ If the result matches, dials the number.
- ▶ If the result is over-qualified (i.e. no further digits could possibly produce a match), sends a fast busy signal.

Using the Dial Map Special Characters

Dial Maps use specific characters and digits in a particular syntax. A Dial Map may have up to 255 individual characters, including any special characters such as the “|” operator. Those characters are:

Table 29: Dial Map Characters

Character	Use
Digits (0, 1, 2... 9)	Indicates specific digits in a telephone number expression.
T	The Timer can be used to indicate that if users have not dialed a digit for 4 seconds, it is likely that they have finished dialing and the UMN can make the call.
x	Matches any digit, excluding “#” and “*”.
	Indicates a choice of matching expressions (OR).
.	Matches an arbitrary number of occurrences of the preceding digit, including 0.
[	Indicates the start of a range of characters.
]	Indicates the end of a range of characters.

How to Use a Dial Map

Let's say you are in an office and you want to call a co-worker's 3-digit extension. You could create a Dial Map that said "after the user has entered any 3 digits, make the call". The Dial Map could look as follows:

```
xxx
```

You could refine this Dial Map by including a range of digits. For instance, you know that all extensions in your company either begin with 2, 3, or 4. The corresponding Dial Map could look as follows:

```
[2-4]xx
```

You have just entered a range of digits. Therefore, if the number you dial begins by anything other than 2, 3, or 4, the call is not placed and you get a busy signal. Another way to achieve the same result would be:

```
[234]xx
```

Combining Several Expressions

It is possible to combine two or more expressions in the same Dial Map by using the "|" operator, which is equivalent to OR. Each expression (the characters between "|" operators) may have up to 25 characters. Keep in mind that the whole Dial Map shall not exceed 255 characters.



Note: Enclose the dial map in parenthesis when using the "|" feature.

Let's say you want to specify a choice: the Dial Map is to check if the number is internal (extension), or external (a local call). Assuming that you shall first dial "9" to make an external call, you could define a Dial Map as follows:

```
([2-4]xx|9[2-9]xxxxxx)
```

The Dial Map checks if:

- ▶ the number begins by 2, 3, or 4 **and**
- ▶ the number has 3 digits

If not, it checks if:

- ▶ the number begins with 9 **and**
- ▶ the second digit is any digit between 2 and 9 **and**
- ▶ the number has 7 digits

Using the "#" and "*" Characters

It may sometimes be required that users dial the "#" or "*" to make calls. This can be easily incorporated into a Dial Map:

```
xxxxxxx#  
xxxxxxx*
```

The "#" or "*" character could indicate users shall dial the "#" or "*" character at the end of their number to indicate it is complete.



Note: When making the actual call and dialing the number, the Mediatrix unit automatically removes the "#" or "*" found at the end of a dialed number, if there is one (after a match). Those characters are for indication purposes only.

Using the Timer

The Timer is set to 4 seconds. It can be used to indicate that if users have not dialed a digit for 4 seconds, it is likely that they have finished dialing and the gateway can make the call. A Dial Map for this could be:

[2-9]xxxxxxT



Note: When making the actual call and dialing the number, the Mediatrix unit automatically removes the "T" found at the end of a dialed number, if there is one (after a match). This character is for indication purposes only.

Using a Dial Map for Calls Outside the Country

If your users are making calls outside your country, it may sometimes be hard to determine exactly the number of digits they shall enter. You could devise a Dial Map that takes this problem into account:

001x.T

The Dial Map looks for a number that begins with 001, and then any number of digits after that (x.).

Example

[Table 28 on page 82](#) outlined various call types one could make. All these possibilities could be covered in one Dial Map:

(0T|00T|[[1-7]xxx|8xxxxxxx|#xxxxxxx|91xxxxxxxxxx|9011x.T)

Validating a Dial Map

When entering a Dial Map expression in one of the Dial Map rules, and then clicking *OK*, the Mediatrix unit validates the Dial Map and indicates if it is correct or not.

Gateway Parameters

This chapter describes how to set Gateway parameters, which are used by the Mediatrix unit when making a call. Note that the Gateway¹ category is only available for analog gateways such as the Mediatrix 1204. Analog gateways link the SCN world and the IP world.

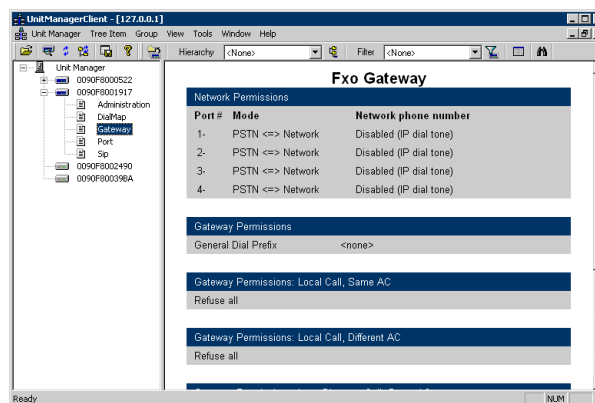


Note: Gateway parameters are only available for units that run the SIP v2.x signalling protocol.

Gateway Overview

Upon selecting the *Gateway* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 73: Gateway Category Overview



You can change the value of these parameters by accessing the *Gateway Permissions* window.

Gateway Permissions Window

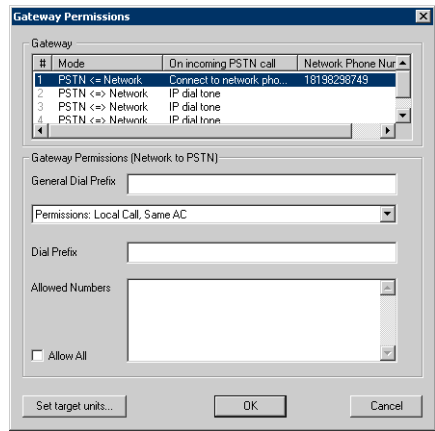
The *Gateway Permissions* window allows you to set the Gateway parameters to use.

► **To access the *Gateway Permissions* window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left. This unit must be an analog gateway such as the Mediatrix 1204.
2. Double-click the *Gateway* category.
The *Gateway Permissions* window opens.

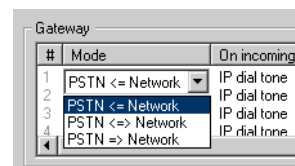
¹. Valid only for units that run the SIP signalling protocol.

Figure 74: Gateway Permissions Window



- 3. Set the *Mode* column by clicking twice at a one second interval on the setting corresponding to the value to change and a drop-down menu with all the available values displays.

Figure 75: Drop Down Menu



You have the following choices:

Table 30: Gateway Modes

Mode	Description
PSTN <= Network	The FXO port can be used for Network to PSTN Gateway. An Internet user can use the FXO port to make calls from the Internet to the PSTN.
PSTN <=> Network	The FXO port can be used both for Network to PSTN and PSTN to Network Gateway. - An Internet user can use the FXO port to make calls from the Internet to the PSTN. - A PSTN user can call on the FXO port and get a dial tone to place a call on the Internet.
PSTN => Network	The FXO port can be used for PSTN to Network Gateway. A PSTN user can call on the FXO port and get a dial tone to place a call on the Internet.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 31: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.

Table 31: Apply Value Methods (Continued)

Method	Description
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

4. Define the port behaviour when receiving an incoming PSTN call in the *On incoming PSTN call* column.
- Click twice at a one second interval on the setting corresponding to the value to change. A drop-down menu with all the available values displays. You have the following choices:

Table 32: Incoming PSTN Calls options

Mode	Description
Connect to network phone number	Forces all incoming calls on the FXO port to be redirected to a specific telephone number. This telephone number must be specified in the <i>Network Phone Number</i> column and have its country code and area code prefixed. There is no need to specify the special dialing extensions required to indicate that the call is long distance (if this is the case). For instance, a valid telephone number in this field would be 18198298749.
IP Dial Tone	The PSTN user can call on the FXO port and get a dial tone to place a call on the Internet.

5. Set the *General Dial Prefix*.
- Prefix to dial on the FXO port before any other number. Such a prefix is required if you are in an office and must dial a number to make calls outside your office. This can also include a special character such as “;”, which is used to pause for one second before processing the next character. If no prefix is required, leave the field empty.
6. Select the permission to set.
- The gateway permissions allow you to set the various telephone numbers that can be called on the FXO port from the network. See [“Using Permissions” on page 88](#) for more details.
- Setting permissions is a very important step of the Mediatix unit configuration. If the permissions are not set properly, your users could have difficulties placing calls, or have access to phone numbers they should not be able to reach.

Table 33: Gateway Permissions

Permission	Description
Dial Prefix	Prefix to dial before the destination number. It can be numbers and/or a special character such as “;”, which is used to pause for one second before processing the next character. If no prefix is required, leave the field empty. Note: the <i>General Dial Prefix</i> is dialed before this dial prefix, but both can be dialed.
Allowed Numbers	Semi-colon-separated list of numbers that can be reached on the FXO port when placing a gateway call from the network to the PSTN. You can specify a range of numbers by entering only the first digits.
Allow All	Checking this box makes all numbers in the category accessible by the Mediatix unit when placing a gateway call from the network to the PSTN. The specified numbers in the <i>Allowed Numbers</i> box are then ignored.

7. To apply changes to several Mediatix units, click the *Set target units* button.
- Follow the procedure described in [“Setting Multiple Units” on page 39](#).

8. Click *OK* when all changes are done.

Using Permissions

Permissions describe the type of calls that one can make with a Mediatrix unit. Special processing and rights can be associated to each category.

The following acronyms are used:

- ▶ **CC:** country code
- ▶ **AC:** Area Code (the North American equivalent to National Destination Code)

The permissions are as follows:

Table 34: Permissions

Category	Description
Local Call, Same AC	The call destination is in the same area code as the Mediatrix unit location and it is a local call. Numbers required in <i>Allowed Numbers</i>: call numbers
Local Call, Different AC	The call destination is in a different area code than the one where the Mediatrix unit is located, but it is still a local call. Numbers required in <i>Allowed Numbers</i>: area code, call numbers
Long Distance Call, Same AC	The call destination is in the same area code as the Mediatrix unit location, but it is considered a long distance call. It thus may need a different prefix. Numbers required in <i>Allowed Numbers</i>: call numbers
Long Distance Call, Different AC	The call destination is in a different area code than the one where the Mediatrix unit is located and the call is long distance. Numbers required in <i>Allowed Numbers</i>: area code, call numbers
Long Distance Call, Different CC	The call destination is in a different country than where the Mediatrix unit is located and the call is long distance. Numbers required in <i>Allowed Numbers</i>: country code, area code, call numbers

See “Examples” on page 89.

How to Set Proper Permissions

International phone numbers are made up of three parts:

- ▶ Country Code (1-3 digits)
- ▶ Area Code (AC)
- ▶ Actual telephone number

When entering numbers in the various fields to grant permissions, remember that location prefixes are typically assigned to a geographic area and are primarily used for ease of administration. Thus, the first digit is the most significant.

For instance, let's consider the number 567-1234. If you want to set permissions for this number, you can do so in various ways:

- ▶ 5: using the 5 prefix allows to call all numbers that begin by 5.
- ▶ 56: using the 56 prefix rules out the use of 55, 57, etc.
- ▶ 567: using the 567 prefix is even more restrictive, as it allows to call numbers that only begin with 567.
- ▶ etc.

The more digits you specify, the more restrictive is the permission.

When setting permissions for the various destination categories, determine the level of restriction to apply. Be cautious when setting permissions, since the less digits you enter, the more numbers your users are able to reach.

Examples

The following are examples you can use and modify to create dial maps.

Local Call, Same AC

Numbers required in *Allowed Numbers*: call numbers only.

You are in Seattle, Washington, and you want to set permissions so that your users can make calls in the 206 area code. The Gateway settings would be as follows:

- ▶ **Dial prefix:** Enter any special dial prefix to dial.
- ▶ **Allowed Numbers:** You can list specific numbers that are allowed, or more general numbers. All numbers are separated by a semi-colon. For instance, entering:

234;456;32;5

Means that your users can call all numbers that begin with these digits. To restrain permission to specific numbers, enter more digits such as the following:

2344567;4563764;3236745

Local Call, Different AC

Numbers required in *Allowed Numbers*: area code, call numbers.

Sometimes you can make a call in a different area code, but this call is still a local call. The Gateway settings would be as follows:

- ▶ **Dial prefix:** Enter any special dial prefix to dial.
 - ▶ **Allowed Numbers:** 425
- You can list specific numbers that are allowed, or more general numbers with the same area code. All numbers are separated by a semi-colon. For instance, entering:

425

Means that your users can call all numbers that begin with the 425 area code. To restrain permission to more specific numbers, enter something such as the following:

425234;42578;4251

Long Distance Call, Same AC

Numbers required in *Allowed Numbers*: call numbers only.

To make long distance calls in the same area code, define which numbers you want active. The Gateway settings would be as follows:

- ▶ **Dial prefix:** Enter any special dial prefix to dial.
- ▶ **Allowed Numbers:** You can list specific numbers that are allowed, or more general numbers with the same area code. All numbers are separated by a semi-colon. For instance, entering:

378;86;6

Means that your users can call all numbers that begin with these digits. To restrain permission to more specific numbers, enter something such as the following:

3786534;8654132;1698360



Note: You don't need to specify the area code, since you are calling in the same area code and it is already defined.

Long Distance Call, Different AC

Numbers required in *Allowed Numbers*: area code, call numbers.

To make long distance calls in other area codes but still in the same country, define which numbers you want active. The Gateway settings would be as follows:

- ▶ **Dial prefix:** Enter any special dial prefix to dial.
- ▶ **Allowed Numbers:** You can list specific numbers that are allowed, or more general area code numbers. All numbers are separated by a semi-colon. For instance, entering:

```
418;819;613
```

Means that your users can call all numbers in these area codes. To restrain permission to specific numbers, enter something such as the following:

```
418567;81986;6138306543
```

Long Distance Call, Different CC

Numbers required in *Allowed Numbers*: country code, area code, call numbers.

To make long distance calls in other countries, define which numbers you want active. The Gateway settings would be as follows:

- ▶ **Dial prefix:** 011
Dialing 011 specifies that you want to make a long distance call outside the country.
- ▶ **Allowed Numbers:** You can list specific numbers that are allowed, or more general country code numbers. All numbers are separated by a semi-colon. For instance, entering:

```
44;33
```

Means that your users can call all numbers in the United Kingdom and France. To restrain permission to specific numbers, enter something such as the following:

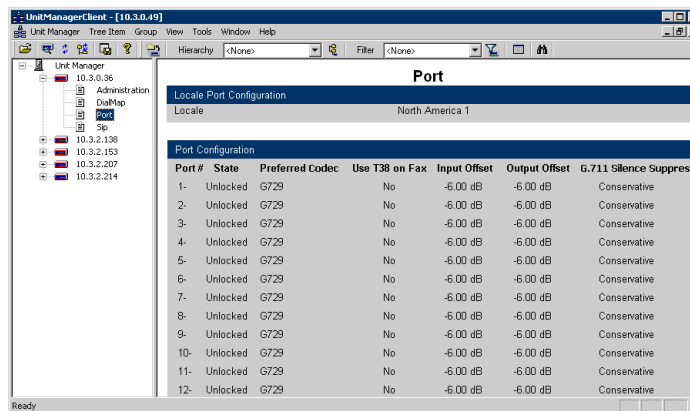
```
441;334
```

This chapter describes how to set the FXS (Foreign Exchange Service/Station) or FXO (Foreign Exchange Office) ports parameters.

Port Overview

Upon selecting the *Ports* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 76: Ports Parameters Overview



Port Configuration						
Port #	State	Preferred Codec	Use T38 on Fax	Input Offset	Output Offset	G.711 Silence Suppress
1-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
2-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
3-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
4-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
5-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
6-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
7-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
8-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
9-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
10-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
11-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative
12-	Unlocked	G729	No	-6.00 dB	-6.00 dB	Conservative

You can change the value of these parameters by accessing the *Port* window.

Port Configuration Window

The *Port* window allows you to change the value of the ports parameters.

► **To access the Port window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Port* category.
The *Port* window opens.

Figure 77: Port Configuration Window – SIP v2.x Units

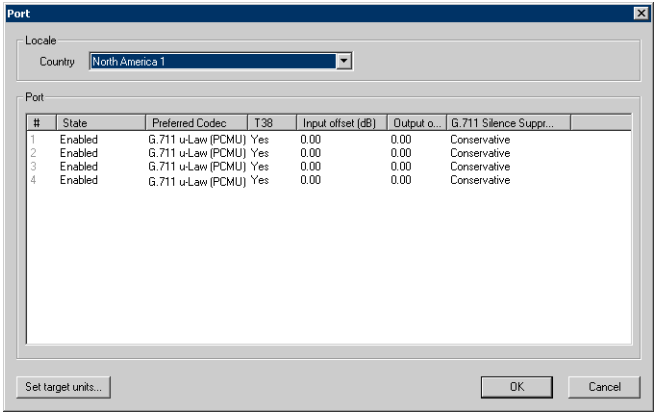
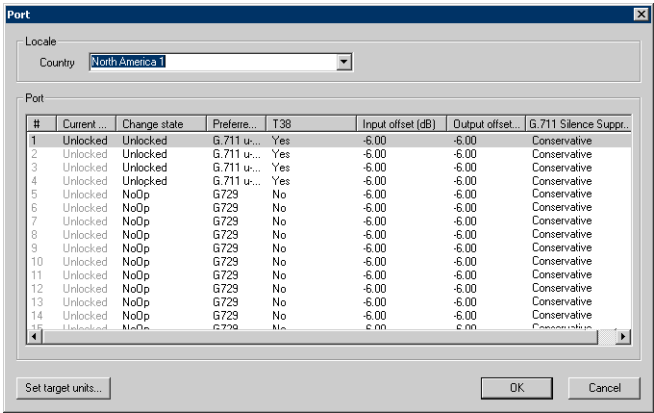


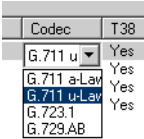
Figure 78: Port Configuration Window – SIP/MGCP v4.x/v5.x Units



The port values are presented in a table in which all ports of the unit are listed.

3. Select the country in which the Mediatrix unit is located.
- When selecting a country, the parameters specific to this country are automatically set. See the Mediatrix unit *Administration Manual* for parameters specific to each supported country.
4. Modify the values you want.
- To modify a value:
- Select it in the row (port) you want to change.
This value becomes highlighted.
 - Modify the value for the variable, and then press the <Enter> key of your keyboard.
If the value offers choices, you can click twice on the variable at a one second interval and a drop-down menu with all the available values displays. Select the proper value.

Figure 79: Drop Down Menu



You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 35: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

The following parameters can be set:

Table 36: Ports Parameters

Parameter	Definition
State	SIP v2.x units only: enables or disables the port.
Change State	SIP/MGCP v4.x/5.x units only: Sets the port state. Available values are: <i>NoOp</i>: No operation <i>Lock</i>: Cancels the port collection to the server. However, active calls in progress remain established until normal call termination. No new calls may be initiated. <i>Unlock</i>: Identifies the port to the server. <i>ForceLock</i>: Cancels the port collection to the server. All active calls in progress are terminated immediately. No new calls may be initiated.
Preferred Codec	The preferred voice-coding algorithm used by the Mediatrix unit when placing calls. Note that if you want to use a fax, select G.711 A-law or G.711 μ -law. Values: G.711 A-law (PCMA), G.711 μ -law (PCMU), G.723.1, G.729.AB Default: G.711 A-law (PCMA)
T38	Specifies that you want to send/receive faxes in T.38 mode. Default: Yes
Input offset (dB)	Sound level received by the Mediatrix unit in dB. Warning: Media5 recommends not to change the value of this setting. If you do so, default calibrations are modified and some fax or modem tones may not be recognized anymore.
Output offset (dB)	Sound level sent by the Mediatrix unit in dB. Warning: Media5 recommends not to change the value of this setting. If you do so, default calibrations are modified and some fax or modem tones may not be recognized anymore.

Table 36: Ports Parameters (Continued)

Parameter	Definition
G.711 Silence suppression	Level of silence detection/suppression. A high level can chop some part of the voice transfers. Values: Conservative, Off, Transparent Default: Conservative Note: The difference between transparent and conservative is how “aggressive” the algorithm considers something as an inactive voice and how “fast” it stops the voice stream. A setting of conservative is a little bit more aggressive to react to silence compared to a setting of transparent.

- To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Codec Activation

The *Codec Activation* sub-category allows you to enable or disable the codecs supported by the unit.



Note: Codec activation parameters are available for units that run the SIP v4.4/v4.5/v5.x, MGCP/NCS v4.4/v4.6/v5.x, and H.323 v4.o/5.x signalling protocols.

Codec Activation Overview

Upon selecting the *Codec Activation* category (under the *Ports* category) of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 80: Codec Activation Parameters Overview

Port #	G.711 u-law (PCMU)	G.711 a-law (PCMA)	G.723.1	G.729 AB	G.726-16kbps	G.726-24kbps	G.726-32kbps	G.726-40kbps
1-	Disabled	Enabled	Disabled	Enabled	Disabled	Enabled	Disabled	Disabled
2-	Disabled	Enabled	Disabled	Enabled	Disabled	Enabled	Disabled	Disabled
3-	Disabled	Enabled	Disabled	Enabled	Disabled	Enabled	Disabled	Disabled
4-	Disabled	Enabled	Disabled	Enabled	Disabled	Enabled	Disabled	Disabled

You can change the value of these parameters by accessing the *Codec Activation* window.

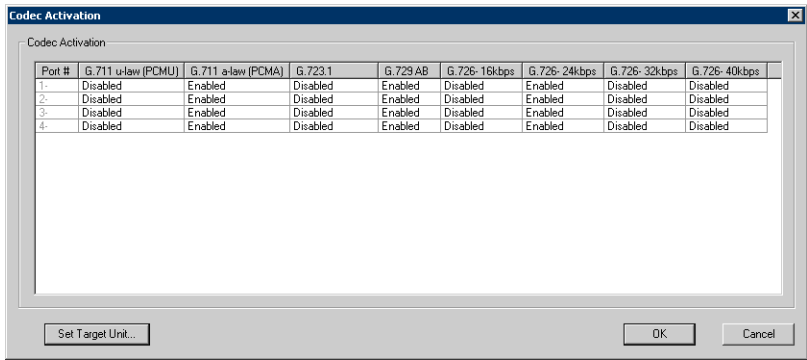
Codec Activation Configuration Window

The *Codec Activation* window allows you to enable or disable the codecs supported by the unit.

► **To access the Codec Activation window:**

- Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
- Double-click the *Codec Activation* category (under the *Ports* category).
The *Codec Activation* window opens.

Figure 81: Codec Activation Configuration Window



Each column represents the codecs that the Mediatrix unit supports.

3. Enable or disable one or more codecs for each line of the Mediatrix unit.

To modify a value:

- Select it in the row (port) you want to change.
This value becomes highlighted.
- Click twice on the variable at a one second interval and a drop-down menu with all the available values displays. Select the proper value.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 37: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

4. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

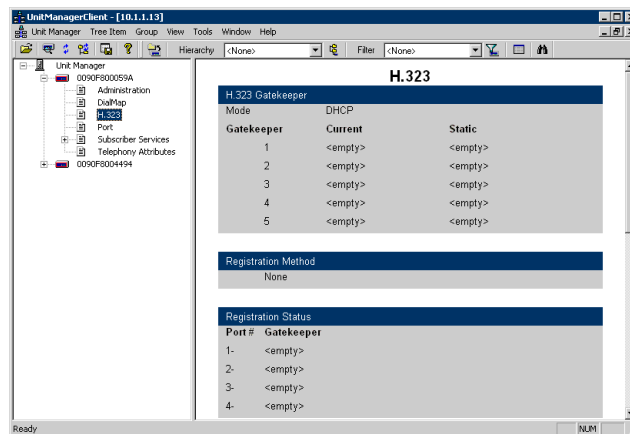
Signalling Protocols Parameters

This [chapter](#) describes how to set parameters pertaining to the H.323, SIP, MGCP, and NCS protocols.

H.323 Parameters

The *H.323* section allows you to set the parameters specific to the H.323 signalling protocol.

Figure 82: H.323 Parameters Overview



You can change the value of these parameters by accessing the *H.323* window.

H.323 Configuration Window

The *H.323* window allows you to set parameters pertaining to the H.323 signalling protocol.

► **To access the H.323 Configuration window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *H.323* category.
The *H.323* window opens.

Figure 83: H.323 Configuration Window

#	IP address
1	10.0.0.217
2	10.0.0.217
3	10.0.0.217
4	10.0.0.217
5	10.0.0.217

Registration Method: Single

#	Type 1	Alias 1	Type 2	Alias 2
1	H323ID	666	E164	999
2	E164	777	E164	999

3. Set the H.323 Gatekeeper information.

The Mediatrix unit can register with one gatekeeper at a time from a list of up to five (5) gatekeepers. A gatekeeper sends the proper information to the Mediatrix unit and manages calls from and to the unit.

- If you want the Mediatrix unit to receive the H.323 Gatekeepers IP addresses via a DHCP server, check the *Use DHCP* option.
- If you want to enter static IP addresses, uncheck the *Use DHCP* option and enter the IP addresses in the corresponding fields. The addresses can be a dotted IP string.

4. Set the *Registration Method* to use.

The Mediatrix unit may use one of three registration methods. Each method has its own distinctive features.

Table 38: H.323 Registration Methods

Method	Definition
None	The Mediatrix unit does not register with a gatekeeper. The unit can be reached by dialing its IP address.
Single	The Mediatrix unit registers as a single entity (and routes the call to the appropriate line). This registration method uses one RAS exchange to register all the lines / groups of lines of the Mediatrix unit once. The unit registers the aliases of its lines / groups of lines together.
Multiple	The Mediatrix unit registers as a terminal with multiple lines/groups of lines (phone numbers). This method registers each line/group of lines of the Mediatrix unit in a separate RAS exchange. The registration request message contains the aliases of each line/group. When using this method, the gatekeeper must resolve the phone number into both an IP address and a port number.

5. Set the *Alias* information.

In H.323, an “address” is called an “alias address” or simply an “alias”. You can define the following aliases:

- FXS unit: two (2) aliases of the same type and/or of different types per port.
- FXO unit: two (2) aliases of the same type and/or of different types per unit. The *H.323* window has only one row in the *Alias* section.

For example, an H.323 ID and an E.164 alias can be specified.

For each port or unit, you can set the following information:

Table 39: H.323 Aliases Information

Parameter	Definition
Type	A port/unit may be configured with E.164 aliases, H.323 ID aliases and party number aliases such as PUU, which is “Public Unknown”. Clicking twice at a one second interval displays a menu of available types.
Alias	Actual value of the alias. Ensure to enter an alias that is relevant to the type you have selected. For instance, “221” is a proper E.164 type alias, while “user1” is not.

To modify a value:

- Select it in the row (port) you want to change.
This value becomes highlighted.
- Modify the value for the variable, and then press the <Enter> key of your keyboard.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 40: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.
Increment Remaining	Allows to change all aliases in the rows located below so that the numbering is sequential. For instance, if an alias is 201, the next would rows be 202, 203, etc.

6. If applicable, set Direct Gateway Call settings. See [“Direct Gateway Call” on page 99](#) for more details.
7. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).



Note: The *Set target units* procedure applies the gatekeeper addresses and the registration method selected. The aliases and Direct Gateway Call settings are not applied to other units.

Direct Gateway Call

The Direct Gateway Call feature allows you to use a gateway without the presence of a gatekeeper. The user simply dials a telephone number. The new outgoing call goes directly to the gateway.

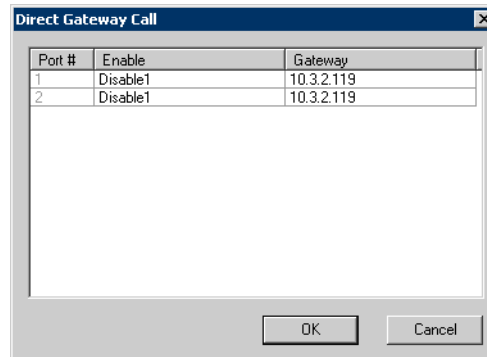
This procedure applies only to lines that are not configured to register:

- ▶ The unit is configured with the multiple registration method and the registration for the line is disabled (see [“H.323 Configuration Window” on page 97](#)).
- OR
- ▶ The unit is configured with the none registration method (see [“H.323 Configuration Window” on page 97](#)).

► **To set the Direct Gateway Call feature:**

1. In the *H.323* window, click the *Direct Gateway Call* button at the bottom.
The *Direct Gateway Call* window opens.

Figure 84: Direct Gateway Call Window

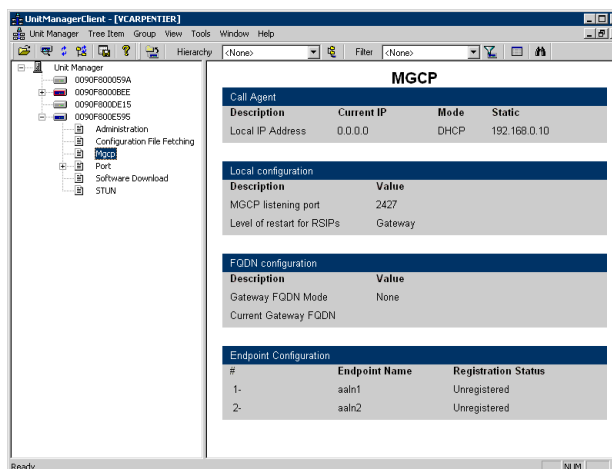


2. Select the port for which to enable the service in the list on the left.
 3. Set the corresponding *Enable* column to **enable**.
 4. Set the IP address of the gateway in the *Gateway* column.
 5. Repeat for the other ports if applicable.
 6. Click *OK* when all changes are done.
- When the user dials the telephone number of a line for which you have enabled the Direct Gateway Call feature, the call is made without the use of a gatekeeper.

MGCP Parameters

The *MGCP* section allows you to set the parameters specific to the MGCP signalling protocol.

Figure 85: MGCP Parameters Overview



You can change the value of these parameters by accessing the *MGCP Configuration* window.

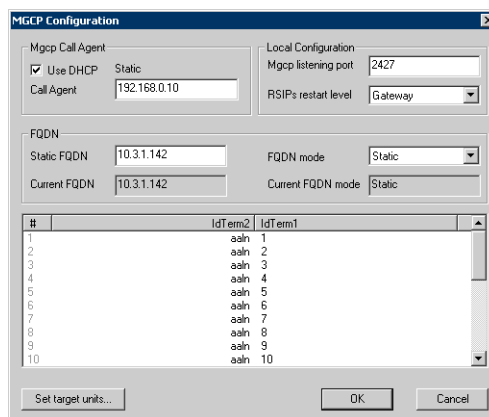
MGCP Configuration Window

The *MGCP Configuration* window allows you to set parameters pertaining to the MGCP signalling protocol.

► **To access the MGCP Configuration window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *MGCP* category.
The *MGCP Configuration* window opens.

Figure 86: MGCP Configuration Window



3. Set the MGCP Call Agent information.
This is the call agent to which the Mediatrix unit registers. A Call Agent is the server that sends the proper information to the Mediatrix unit and manages calls from and to the unit.
 - If you want the Mediatrix unit to receive the MGCP Call Agent IP address via a DHCP server, check the *Use DHCP* option.

- If you want to enter a static IP address, uncheck the *Use DHCP* option and enter the IP address in the corresponding field. The address can be a dotted IP string or a Fully Qualified Domain Name (FQDN).

4. Set the *Local Configuration* options.

Table 41: MGCP Local Configuration Parameters

Parameter	Definition
MGCP listening port	UDP port number on which the Mediatix unit is listening for any MGCP request.
RSIPs restart level	Level of restart for initial RSIP (Restart in Progress). • Gateway • Group • Endpoint The RSIP notifies the Call Agent that the gateway, or a group of endpoints managed by the gateway, is being taken out of service or is being placed back in service.

5. Set the *FQDN* options.

The Mediatix unit uses the FQDN (Fully Qualified Domain Name) to register to the MGCP call agent.

Table 42: MGCP FQDN Configuration Source

Parameter	Definition
Static FQDN	IP address to use as FQDN when the <i>FQDN mode</i> is set to <i>static</i> .
Current FQDN	FQDN value assigned to the Mediatix unit.
FQDN Mode	Source to use for the provisioning of the Mediatix unit FQDN information. • Dhcp: The DHCP-provided “host name” (option number 12) is used. No site specific code is provided. The Mediatix unit takes the FQDN in the DHCP offer. • Dns: The FQDN is set with the name associated to the host IP address. This DNS is taken from the Primary and Secondary DNS information set in the <i>Administration</i> category. See “IP Configuration” on page 70 for more details. • None: The Mediatix unit uses the host IP address inserted within angle brackets (i.e. [192.168.0.1]). • Static: Set a static IP address in the <i>Static FQDN</i> field.
Current FQDN Mode	Mode used during the last restart sequence of the Mediatix unit.



Note: Some of the above fields may be unavailable depending on the software version of the selected Mediatix unit.

6. Set the name of the endpoint.

The endpoint name is created as follows: *term2/term1@localHostFqdn*. Endpoints are originating or terminating devices such as phones or faxes.

Table 43: MGCP Endpoint Parameters

Parameter	Definition
IdTerm2	Second term from the right of the local endpoint name.
IdTerm1	The right most term of the local endpoint name.

To modify a value:

- Select it in the row (port) you want to change.
This value becomes highlighted.
- Modify the value for the variable, and then press the <Enter> key of your keyboard.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 44: Apply Value Methods

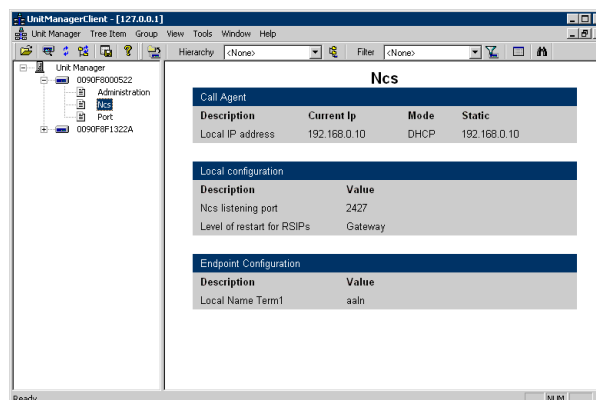
Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

7. To apply these settings to all ports of the Mediatrix unit, click *Apply to all* in the lower right corner of the window.
8. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

NCS Parameters

The NCS section allows you to set the parameters specific to the NCS signalling protocol.

Figure 87: NCS Parameters Overview



You can change the value of these parameters by accessing the *NCS Configuration* window.

NCS Configuration Window

The *NCS Configuration* window allows you to set parameters pertaining to the NCS signalling protocol.

► **To access the NCS Configuration window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *NCS* category.
The *NCS Configuration* window opens.

Figure 88: NCS Configuration Window

3. Set the NCS Call Agent information.
This is the call agent to which the Mediatrix unit registers. A Call Agent is the server that sends the proper information to the Mediatrix unit and manages calls from and to the unit.
 - If you want the Mediatrix unit to receive the NCS Call Agent IP address via a DHCP server, check the *Use DHCP* option.
 - If you want to enter a static IP address, uncheck the *Use DHCP* option and enter the IP address in the corresponding field. The address can be a dotted IP string or a Fully Qualified Domain Name (FQDN).
4. Set the *Local Configuration* options.

Table 45: NCS Local Configuration Parameters

Parameter	Definition
NCS listening port	UDP port number on which the Mediatrix unit is listening for any NCS request.
RSIPs restart level	Level of restart for initial RSIP (Restart in Progress). • Gateway • Group • Endpoint The RSIP notifies the Call Agent that the gateway, or a group of endpoints managed by the gateway, is being taken out of service or is being placed back in service.

5. Set the *FQDN* options.

The Mediatrix unit uses the FQDN (Fully Qualified Domain Name) to register to the NCS call agent.

Table 46: NCS FQDN Configuration Source

Parameter	Definition
Static FQDN	IP address to use as FQDN when the <i>FQDN mode</i> is set to <i>static</i> .
Current FQDN	FQDN value assigned to the Mediatrix unit.
FQDN Mode	Source to use for the provisioning of the Mediatrix unit FQDN information. • Dhcp: The DHCP-provided “host name” (option number 12) is used. No site specific code is provided. The Mediatrix unit takes the FQDN in the DHCP offer. • Dns: The FQDN is set with the name associated to the host IP address. This DNS is taken from the Primary and Secondary DNS information set in the <i>Administration</i> category. See “IP Configuration” on page 70 for more details. • None: The Mediatrix unit uses the host IP address inserted within angle brackets (i.e. [192.168.0.1]). • Static: Set a static IP address in the <i>Static FQDN</i> field.
Current FQDN Mode	Mode used during the last restart sequence of the Mediatrix unit.



Note: Some of the above fields may be unavailable depending on the software version of the selected Mediatrix unit.

6. Set the name of the endpoint.

The endpoint name is created as follows: *Local Name/term1@localHostFqdn*. Endpoints are originating or terminating devices such as phones or faxes.

Table 47: NCS Endpoint Parameters

Parameter	Definition
Local Name	Second term from the right of the local endpoint name.
IdTerm1	The right most term of the local endpoint name.

To modify a value:

- Select it in the row (port) you want to change.
This value becomes highlighted.
- Modify the value for the variable, and then press the <Enter> key of your keyboard.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 48: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.

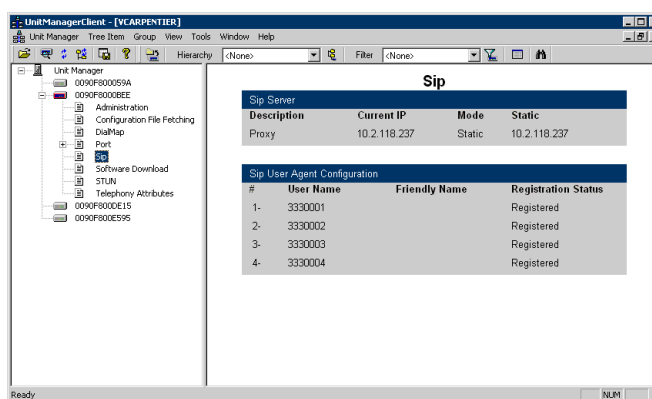
Table 48: Apply Value Methods (Continued)

Method	Description
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

- To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

SIP Parameters

The *SIP* section allows you to set the parameters specific to the SIP signalling protocol.

Figure 89: SIP Parameters Overview

You can change the value of these parameters by accessing the *SIP Configuration* window.

SIP Configuration Window

The *SIP Configuration* window allows you to set parameters pertaining to the SIP signalling protocol.

► **To access the SIP Configuration window:**

- Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
- Double-click the *SIP* category.

The *SIP Configuration* window opens.

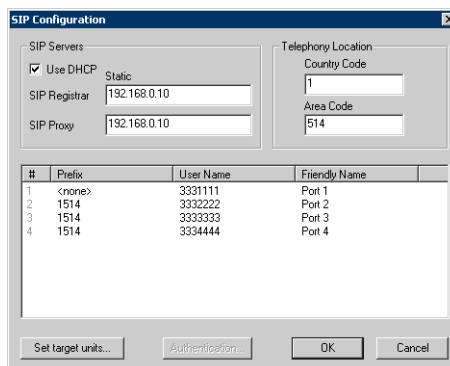
Figure 90: SIP Configuration Window – SIP v2.x Units

Figure 91: SIP Configuration Window – SIP/MGCP v4.x/v5.x Units

The SIP Configuration window is divided into two main sections. The 'SIP Servers' section on the left has a 'Use DHCP' checkbox checked, with 'Static' selected. Below are text boxes for 'SIP Registrar' (192.168.0.10) and 'SIP Proxy' (192.168.0.10). The 'Telephony Location' section on the right has text boxes for 'Country Code' and 'Area Code'. At the bottom is a table with 4 columns: '#', 'User Name', 'Friendly Name', and an empty column. The table contains 4 rows of data. At the very bottom are buttons for 'Set target units...', 'Authentication...', 'OK', and 'Cancel'.

#	User Name	Friendly Name	
1	3330001	Port 1	
2	3330002	Port 2	
3	3330003	Port 3	
4	3330004	Port 4	

► **To set SIP parameters:**

- Set the IP addresses information.
 - If you want the Mediatrix unit to receive the SIP Servers IP addresses via a DHCP server, check the *Use DHCP* option.
 - If you want to enter static IP addresses, uncheck the *Use DHCP* option and enter the IP addresses in the corresponding fields.

Table 49 describes the IP addresses you can define.

Table 49: SIP Servers Parameters

Parameter	Definition
SIP Registrar	IP address of the server where the Mediatrix unit sends the register request for its ports (if they are enabled).
SIP Proxy	IP address of the server where the Mediatrix unit sends its INVITE messages to initiate phone calls.



Warning: If you are modifying v2.4 units and change both the SIP Registrar and SIP Proxy addresses, the unit will unregister from the current Registrar, then send a registration request to two servers: the new one and the previous one. If the previous Registrar is still responding, the unit may then be registered with the two servers at the same time.

- Set the *Telephony Location* information.



Note: These settings are only available for SIP v2.x units

Table 50: SIP Telephony Information

Parameter	Definition
Country Code	The country code associated to the current location of the Mediatrix unit. Example: North American code is 1
Area Code	The area code associated to the current location of the Mediatrix unit.

- In the list box, set the *Prefix* by clicking twice on the setting corresponding to the value to change at a one second interval and a drop-down menu with all the available values displays.
 - None
 - CC+AC (as defined in the *Telephony Location* section)

The Prefix (Country Code and Area Code) is prefixed to the user name.



Note: These settings are only available for SIP v2.x units

4. In the list box, set the *User Name*.

The User Name identifies the Mediatrix unit application. It usually is a telephone number. To modify a value:

- Select the cell to change.
This value becomes highlighted.
- Modify the value, and then press the <Enter> key of your keyboard.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 51: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.
Increment Remaining	Allows to change all aliases in the rows located below so that the numbering is sequential. For instance, if an alias is 201, the next would rows be 202, 203, etc.

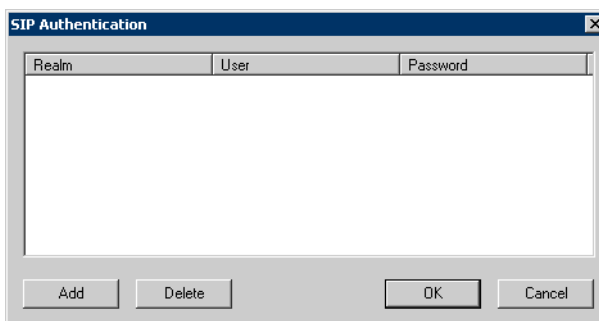
5. In the list box, set the friendly name.
The friendly name is an alias of the user name easier to understand. Note that the friendly name is not saved in the MIB configuration.
6. Set the Authentication parameters. See [“SIP Authentication” on page 108](#) for more details.
7. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

SIP Authentication

The *SIP Authentication* window allows you to manage authentication information for a selected user agent.

► To add SIP authentication:

1. In the *SIP Configuration* window, select a user agent in the list box at the bottom.
2. Click the *Authentication* button.
The following window opens.

Figure 92: SIP Authentication Window

Note: The *Add* and *Delete* buttons are only available for SIP v2.x units.

3. Add new authentication information.
 - In SIP v2.x units, click the *Add* button.
 - In SIP/MGCP v4.x/v5.x units, click inside the table.

Default values are displayed.

4. Set the SIP authentication parameters.

Table 52: SIP Authentication Parameters

Parameter	Definition
Realm	When authentication information is required from users, the string in the <i>Realm</i> column is displayed to users to identify who requests this information. The string thus represents this particular SIP Server and should contain at least the name of the host performing the authentication.
User	The user name and password provide enhanced security when registering users.
Password	The user name and password provide enhanced security when registering users.

5. Click *OK* to apply the changes.

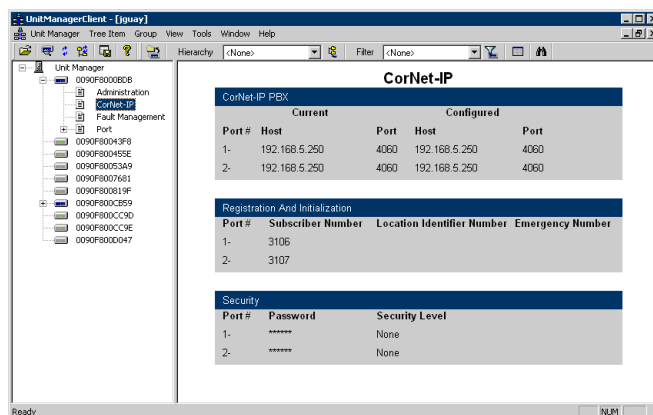
► **To delete existing SIP authentication:**

1. In the *SIP Authentication* window, select the authentication information to delete.
2. Delete the authentication information.
 - In SIP v2.x units, click the *Delete* button.
 - In SIP/MGCP v4.x/v5.x units, delete the information in each cell.
3. Click *OK* to apply the changes.

CorNet-IP Parameters

The *CorNet-IP* section allows you to set the parameters specific to the CorNet-IP signalling protocol.

Figure 93: CorNet-IP Parameters Overview



You can change the value of these parameters by accessing the *CorNet-IP* window.

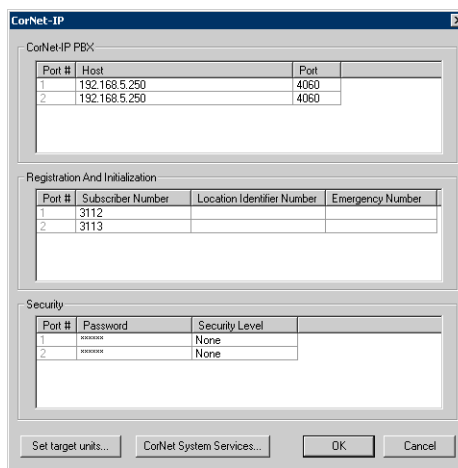
CorNet-IP Configuration Window

The *CorNet-IP* window allows you to set parameters pertaining to the CorNet IP proprietary signalling protocol.

► **To access the CorNet-IP Configuration window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *CorNet-IP* category.
The *CorNet-IP* window opens.

Figure 94: CorNet-IP Configuration Window



3. In the *CorNet-IP PBX* section, set the IP address or domain name and port number of the PBX to which the line registers.
A CorNet-IP PBX is also called a HFA server. No DHCP value is available.
4. In the *Registration And Initialization* section, set the *Subscriber Number* (E.164 alias) of the line. Each line must have a unique Subscriber Number. The Subscriber Number can't be left empty. The line provides its Subscriber Number to the PBX during the registration process.

5. Set the *Location Identifier Number*.

The Location Identifier Number describes the physical location of the line. The PBX uses this information to route emergency calls. The Location Identification Number may be left empty.

The line provides its Location Identifier Number to the PBX during the registration process.

- If the line provides a Location Identifier Number to the PBX, the PBX uses this information to route emergency calls.
- If the line does not provide a Location Identifier Number to the PBX, the PBX does not guarantee the proper routing of emergency calls.

6. Set the *Emergency Number* of the line.

The PBX uses the Emergency Number to route emergency calls.

The line provides its Emergency Number to the PBX during the initialization process.

- If the line provides an Emergency Number to the PBX, the PBX uses this information to route emergency calls.
- If the line does not provide an Emergency Number to the PBX, the PBX does not guarantee the proper routing of emergency calls.

7. In the *Security* section, set the authentication password used to authenticate the endpoint during the CorNet registration in the *Password* column.



Caution: The Security support is for Line 1 only, which means only this line tries to register when the password is configured. Line 2 becomes unusable when the security is activated on Line 1.

This provides security when registering to a HFA server:

- Authentication of CorNet registration.
- Message integrity of CorNet signalling.
- H.235 security in H.323 signalling.

If you let this variable empty, the endpoint does not use authentication.

8. Set the security level used by an endpoint in the *Security Level* column.

Table 53: System Security Levels

Security Level	Description
None	The endpoint does not use security. This is the default value. The endpoint uses this security level when the <i>Password</i> column is empty (see Step 7).
Reduced	The endpoint uses the reduced security profile: • authentication in the CorNet registration. • message integrity in outgoing CorNet signalling. • H.235 security in H.323 signalling.
Full	The endpoint uses the full security profile: • authentication in the CorNet registration. • message integrity in outgoing/incoming CorNet signalling. • H.235 security in H.323 signalling.

9. Set the System Services parameters. See [“System Services” on page 112](#) for more details.

10. To apply changes to several Mediatrix units, click the *Set target units* button.

Follow the procedure described in [“Setting Multiple Units” on page 39](#).



Note: The *Set target units* procedure does not apply the parameters in the *Registration And Initialization* section if several units are selected.

System Services

The *CorNet System Services* window allows you to define key sequences that will emulate the function keys of IP phones and activate different services offered by the CorNet gatekeeper (transfer, conference, call forward, etc.).

There are two types of services:

- ▶ Services that only require an activation sequence.
- ▶ Services that require additional data input once the service is called (two-stage services).

▶ **To define the system services access parameters:**

1. In the *CorNet-IP* window, click the *CorNet System Services* button.
The following window opens.

Figure 95: CorNet System Services Window

#	Name	Enable	Key Code	Activation Sequence	2 Stage Flag	First Digit Timer
1		Enable	18	*18	0	20000
2		Disable	0		0	20000
3		Disable	0		0	20000
4		Disable	0		0	20000
5		Disable	0		0	20000
6		Disable	0		0	20000
7		Disable	0		0	20000
8		Disable	0		0	20000
9		Disable	0		0	20000
10		Disable	0		0	20000

2. Select the entity to which apply the authentication information in the *Apply To* column.

Table 54: Authentication Entity

Parameter	Description
Unit	The authentication entry applies to the unit.
Endpoint	The authentication entry applies to a specific endpoint.

▶ **To define the system services access parameters:**

1. Define whether to enable all service requests by selecting the *Call Features Enable* option.
This is the master switch to enable all service requests. When enabled, the dialed DTMFs are compared against the activation sequences contained in the *Features* section. If a match is found, the corresponding feature code is sent to the gatekeeper via a KB_KEY request. When disabled, or if no match can be found, each DTMF dialed is blindly relayed to the gatekeeper.
This applies to all services.
2. Select the method used to determine that second stage dialing is complete in the *Ending method* drop-down menu.

After this point, any DTMF entered is sent in-band.

Table 55: Ending Method Parameters

Parameter	Description
Timer	Second stage dialing will end when a period of time equal to that specified in the <i>Timeout</i> field elapses without any keys being pressed.
EndCharacter	Second stage dialing will end as soon as the character set in the <i>End Key</i> field is entered by the user.

This applies to all two-stage services.

3. If the ending method is *EndCharacter*, define the DTMF key that will end all second stage dialing sequences in the *End Key* field.
The default value is #.
This applies to all two-stage services.
4. If the ending method is *Timer*, set the amount of time to wait (in milliseconds) after a DTMF entry before deciding that second stage dialing is over in the *Timeout* field.
This applies to all two-stage services.
5. Define the timeout associated with the 'T' character in the digit maps contained in the *Activation Sequence* column of the *Features* section in the *Timeout Inter Digit* field.
The 'T' digit is used to express a time lapse between the detection of two DTMFs.
This value is expressed in milliseconds (ms).
This applies to all services.
6. In the *Features* section, define the name of each service in the *Name* column.
7. Activate/deactivate the corresponding service by setting the *Enable* column to **Enable** or **Disable**.
8. Define the feature code identifying the corresponding service in the CorNet server in the *Key Code* column.
9. Define the digit map that the user needs to dial when requesting the corresponding service in the *Activation Sequence* column.
For instance, you could decide to put “*70” as the sequence to activate the service. This sequence must be unique and follow the syntax for digit maps. Dialing this digit map does not have any effect unless the service’s status is “enabled”.
10. For each service, set the boolean flag used to distinguish between the services that only require the user to enter the activation sequence and two-stage services in the *2 Stage Flag* field.

Table 56: Two-Stage Flag Parameters

Parameter	Description
0	Dialing the activation sequence is all that is needed to request the service.
1	Following the service request, the server signals the user and awaits the entry of further data. These services use the <i>Ending Method</i> , <i>Timeout</i> , and <i>End Key</i> fields to establish how the end of second stage dialing is detected.

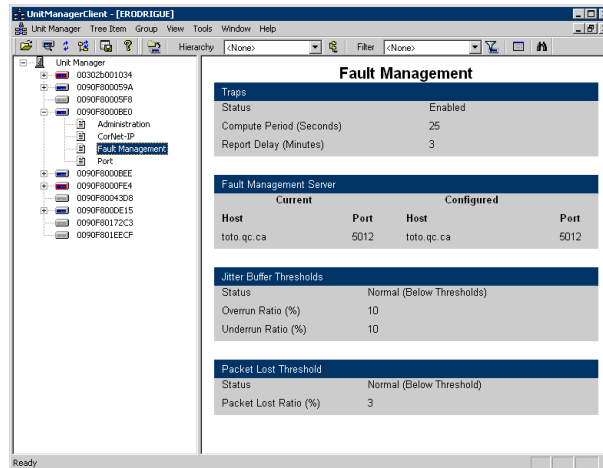
11. Set the amount of time to wait (in milliseconds) for user input while in the second stage of a service request in the *First Digit Timer* field.
This applies to the second stage of two-stage services. If the delay expires, the service request is cancelled altogether. This avoids waiting forever after the user has dialed an activation sequence for a two-stage service. The default value is 20000 ms.

CorNet-IP Fault Management Parameters

The *Fault Management* section allows you to set the parameters specific to the CorNet-IP fault management feature.

Fault management includes maintaining and examining error logs, accepting and acting on error detection notifications, tracing and identifying faults, carrying out sequences of diagnostics tests, correcting faults, reporting error conditions, and localizing and tracing faults.

Figure 96: CorNet-IP – Fault Management Overview



You can change the value of these parameters by accessing the *Fault Management* window.

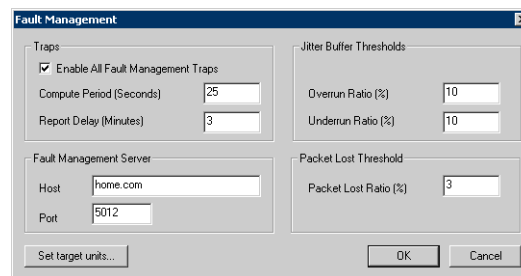
Fault Management Window

The *Fault Management* window allows you to set parameters pertaining to the CorNet IP proprietary fault management feature.

► **To access the Fault Management window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Fault Management* category.
The *Fault Management* window opens.

Figure 97: Fault Management Window



3. In the *Traps* section, check the *Enable All Fault Management Traps* option.
The fault management traps are sent to the fault management host whenever a defined trigger is hit.
4. Define the interval, in seconds, at which to compute the different ratios in the *Compute Period* field.
For instance, the Mediatrix unit computes the packets lost ratio after each period. If the packets lost ratio is greater than the value of the field *Packets Lost Ratio*, then a SNMP trap is sent to the fault management host.
The same applies for the Jitter Buffer Overrun and Underrun Ratios. This value is also used when detecting LAN errors.

The same trap will not be sent again to the fault management host until the value set in the *Report Delay* field elapses.

5. Set the time, in minutes, to wait before sending a given trap again in the *Report Delay* field.

The trap is sent to indicate one of the two following conditions:

- The faulty condition is still present – Traps: authentication, packet lost, jitter buffer overrun, jitter buffer underrun.
- The faulty condition is not present anymore – Traps: packet lost, jitter buffer overrun, jitter buffer underrun, lan error.

See [“Fault Management Events” on page 115](#) for traps description and number.

6. In the *Fault Management Server* section, set the following:
 - the IP address or domain name of the CorNet fault management host to which SNMP traps related to fault management are sent in the *Host* field.
 - the CorNet fault management host IP port on which the SNMP traps related to the fault management are sent in the *Port* field.
7. In the *Jitter Buffer Thresholds* section, set the maximum acceptable jitter buffer overrun ratio (percentage) before a jitter buffer trap is sent to the fault management host in the *Overrun Ratio* field.

The ratio is as follows:

$$\frac{\text{time duration the jitter buffer is overrunning}}{\text{Compute Period field value}}$$

8. Set the maximum acceptable jitter buffer underrun ratio (percentage) before a jitter buffer trap is sent to the fault management host in the *Underrun Ratio* field.

The ratio is as follows:

$$\frac{\text{time duration the jitter buffer is underrunning}}{\text{Compute Period field value}}$$

9. In the *Packet Lost Threshold* section, set the maximum acceptable packets lost ratio (percentage) before a packet lost trap is sent to the fault management host in the *Packets Lost Ratio* field.

The ratio is as follows:

$$\frac{\text{number of RTP packets lost}}{\text{number of RTP packets received + number of RTP packets lost during a Compute Period field value}}$$

10. To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Fault Management Events

The following are the fault management traps the Mediatrix unit sends to the fault management host.

Table 57: Fault Management Events

Trap	Trap #	Description
corNetFault ManagementReboot Trap	1050	The unit has rebooted. This trap also includes the following information: • sysObjectID • sysMacAddress

Table 57: Fault Management Events (Continued)

Trap	Trap #	Description
corNetFault Management AuthenticationFailure Trap	1150	An SNMP authentication failure occurred. This trap also includes the following information: • sysObjectID • sysMacAddress
corNetFault ManagementLanTrap	1250	A LAN error was detected. The unit sends a trap when it detects the LAN has been down for more than the consecutive number of seconds set in the variable <i>CorNetFaultManagerTrapsCompute Period</i> . The trap will be sent once the LAN is operational again. This trap also includes the following information: • sysObjectID • sysMacAddress
corNetFault ManagementPackets LostTrap	1350	One of the following occurred: 1. the <i>corNetSystemFault ManagementTrapsMaximum PacketsLostRatio</i> has been exceeded. OR 2. the RTP packets lost ratio returns within the normal limit (i.e., under the value of <i>corNetSystemFault anagementTrapsMaximum PacketsLostRatio</i>). A packet lost trap indicating condition #2 is sent only if a packet lost trap indicating condition #1 has been previously sent. condition #1 is indicated by: <i>corNetFaultManagementPacketsLost Status</i> = error (1) condition #2 is indicated by: <i>corNetFaultManagementPacketsLost Status</i> = normal (0) This trap also includes the following information: • sysObjectID • sysMacAddress • corNetFaultManagementPacketsLostStatus

Table 57: Fault Management Events (Continued)

Trap	Trap #	Description
corNetFaultManagementJitter BufferTrap	1450	One of the following occurred: 1. the <i>corNetSystemFault ManagementTrapsMaximumJitter BufferOverrunRatio</i> has been exceeded. OR 2. the <i>corNetSystemFault ManagementTrapsMaximumJitter BufferUnderrunRatio</i> has been exceeded. OR 3. the overrun/underrun ratios return within the normal limit (i.e., under the value of the variable <i>corNetSystemFaultManagementTrapsMaximumJitterBuffer OverrunRatio</i> and the variable <i>corNetSystemFaultManagementTrapsMaximumJitterBuffer UnderrunRatio</i>). A jitter buffer trap indicating condition #3 is sent only if a jitter buffer trap indicating condition #1 or #2 has been previously sent. condition #1 is indicated by: <i>corNetFaultManagementJitterBuffer Status</i> = overrun (1) condition #2 is indicated by: <i>corNetFaultManagementJitterBuffer Status</i> = underrun (2) condition #3 is indicated by: <i>corNetFaultManagementJitterBuffer Status</i> = normal (0) This trap also includes the following information: • sysObjectID • sysMacAddress • corNetFaultManagementJitter BufferStatus.

Configuration File Fetching Parameters

The configuration file download (also called file fetching) feature allows to update the Mediatix unit configuration by transferring a configuration file via TFTP or HTTP.



Note: Refer to [“Downloading a Configuration File” on page 60](#) if you want to manually download a configuration file.



Note: Configuration file fetching parameters are available for units that run the SIP v4.5, SIP v5.x, H.323 v5.x, and MGCP/NCS v5.x signalling protocols.

Before Downloading

To download a configuration file, you may need to setup the following applications on your computer:

- ▶ TFTP server with proper root path
- ▶ SNTP server properly configured
- ▶ HTTP server with proper root path

Configuring the TFTP Server

If you are to perform a configuration file download by using the TFTP protocol, you must install a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the TFTP server host. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

If you are to use the automatic configuration file update feature (see [“Auto-Update Settings” on page 124](#) for more details), you need to have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation.

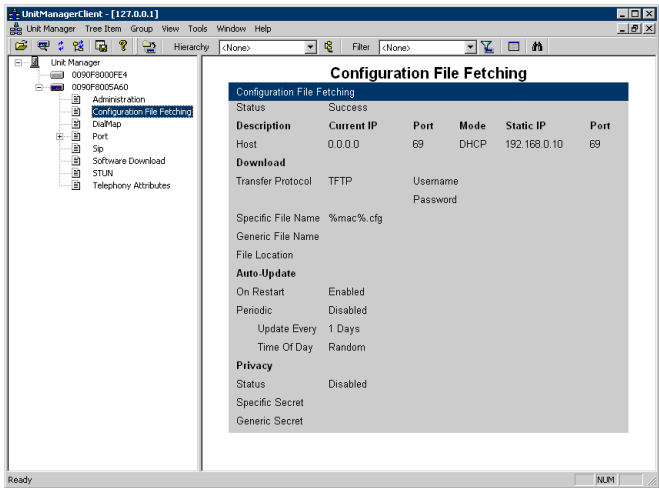
Configuring the HTTP Server

If you are to perform a configuration file download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

Configuration File Fetching Overview

Upon selecting the *Configuration File Fetching* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 98: Configuration File Fetching Parameters Overview



You can change the value of the Configuration File Fetching parameters by accessing the *Configuration File Fetching* window.

Configuration File Fetching Window

When performing a configuration file download, you can download two different files:

- ▶ A generic configuration file that should be used to update a large number of units with the same configuration.
- ▶ A specific configuration file that contains the configuration for a single unit, for instance the telephone numbers of its lines.

When both the generic and specific configuration files are downloaded, settings from the specific configuration file always override the settings from the generic configuration file. These files must be located in the same directory.

▶ **To access the *Configuration File Fetching* window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Configuration File Fetching* category.
The *Configuration File Fetching* window opens.

Figure 99: Configuration File Fetching Window

3. Enable the Configuration File Fetching feature by checking the **Enable** option.
4. Set the following parameters:
 - [“Server Settings” on page 122](#)
 - [“Auto-Update Settings” on page 124](#)
 - [“Privacy Settings” on page 126](#)
5. To apply changes to more than one Mediatrix unit, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Server Settings

The *Server* section of the *Configuration File Fetching* window allows you to define how to transfer the files.

► To set server parameters:

1. In the *Server* section, set the transfer protocol to use in the *Transfer Protocol* field.
You have the choice between **TFTP** and **HTTP**.
Your HTTP server may activate some caching mechanism for the file download. This mechanism caches the initial file download for later processing, thus preventing changes or update of the original file by the user. This can cause strange problems if a user wants to edit a configuration file to modify values and upload it immediately. The result will still return the original file and not the new one.
2. If your HTTP server requires authentication to download the configuration file, set the following:
 - The user name in the *Username* field.
 - The password in the *Password* field.

The Mediatrix unit supports basic and digest HTTP authentication, as described in RFC 2617.

3. Set the IP information.
 - If you want the Mediatrix unit to receive its IP information via a DHCP server, check the *Use DHCP* option.
 - If you want to enter static IP information, uncheck the *Use DHCP* option and enter the IP information in the corresponding fields.

[Table 58](#) describes the static IP information you can define.

Table 58: Static IP Information Parameters

Parameter	Definition
Host	Configuration file server static IP address or domain name. This is the current address of the PC that hosts the configuration files.
Port	Configuration file server static IP port number. The default port value (69) complies to RFC 1340 on the well-known ports (assigned numbers). This value applies to a TFTP server. It may be different for other servers. If you are using an HTTP server to perform the configuration file download, you must change the port value to 80.

4. Set the name of the specific configuration file to download in the *Specific File Name* field.

The file name is case sensitive hence it must be entered properly.

This file should be used to update the configuration of a single unit.

This field may contain macros that are substituted by actual values when downloading the configuration file. Supported macros are:

- %mac%: the MAC address of the unit
- %product%: the product name of the unit
- %%: the character “%”

For instance:

- The “%mac%.xml” value for a Mediatrix unit with MAC address “0090F12345AB” will be “0090F12345AB.xml”.
- The value “Hello%%Hi” will result in “Hello%Hi”.
- The value “%%mac%%mac%.xml” will result in “%0090F12345AB%mac%.xml”.
From left to right: the first macro encountered is first substituted, the second macro encountered is then substituted, etc.

When the character “%” is not part of a macro, it is not replaced. The following are examples:

- The value “%mac.xml” stays “%mac.xml”

- The value "Hello%Hi" stays "Hello%Hi"
- The value "%moc%.xml" stays "%moc%.xml"

If the field is empty (after macro substitution), the Mediatrix unit does not download the specific configuration file.

5. Set the name of the generic configuration file to download in the *Generic File Name* field.

The file name is case sensitive hence it must be entered properly.

This file should be used to update a large number of units with the same configuration.

If you leave the field empty, the Mediatrix unit does not download the generic configuration file.

6. Set the path, on the remote server, of the directory where the configuration files are located in the *File Location* field.

The path is case sensitive hence it must be entered properly. The path is relative to the root path of the transfer server. Use the "/" character when defining the path to indicate sub-directories.

Let's consider the following example:

- The directory that contains the configuration file is called: **Config_File**.
- This directory is under **C:/Root/Download**.

Table 59: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	Config_File
c:/	root/download/Config_File
c:/root	download/Config_File

The following are some tips to help your download process:

- If available, use the *Browse* button (or equivalent) of the TFTP/HTTP server to select the directory, eliminating typographical errors.
- Use the "/" character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the "/" character and produce an error. In this case, use the "\" character.
- Use basic directory names, without spaces or special characters such as "~", "@", etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted files into the configuration file path of the Mediatrix unit (you may have to convert "\" into "/") to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file names may also differ from the example shown above.

Auto-Update Settings

You can configure the Mediatrix unit to automatically update its configuration. This update can be done:

- ▶ Every time the Mediatrix unit restarts.
- ▶ At a specific time interval you can define.

▶ **To set the automatic update parameters:**

1. In the *Auto-Update* section of the *Configuration File Fetching* window, select the auto-update feature to use:

Table 60: Auto-Update Options

Parameter	Description
Enable on Restart	Updates the Mediatrix unit every time it restarts. The unit configuration is only updated if at least one parameter value defined in the downloaded configuration files is different from the actual unit configuration.
Enable Periodic	Updates the Mediatrix unit at a specific time interval you can define. In that case, go to Step 2.

2. For a Periodic update, set the waiting period between each configuration update in the *Update Every* fields.

The time base available for automatic configuration updates is as follows:

Table 61: Time Unit Parameters

Parameter	Description
Seconds	Updates the unit's configuration every x seconds. You can specify the x value in the first field.
Minutes	Updates the unit's configuration every x minutes. You can specify the x value in the first field.
Hours	Updates the unit's configuration every x hours. You can specify the x value in the first field.
Days	Updates the unit's configuration every x days. You can specify the x value in the first field. You can also define the time of day when to perform the update in the <i>Time Range</i> field (see Step 3) or <i>Time of Day</i> field (see Step 4).

The time unit values available are from 1 to 48.

It may be possible that the Mediatrix unit skips a scheduled periodic update if the previous periodic update has not finished yet. This may happen with periods of a few seconds.

Let's say for instance that you set the period to two seconds and the automatic update mechanism takes five seconds to complete. The following describes the behaviour:

Table 62: Scheduled Periodic Update

Time (s)	Description
0	Beginning of the automatic update mechanism.
2	Automatic update. The file transfer starts.
4	Automatic update. The Mediatrix unit skips this scheduled update because the previous update has not finished yet.
6	Automatic update. The Mediatrix unit skips this scheduled update because the previous update has not finished yet.

Table 62: Scheduled Periodic Update (Continued)

Time (s)	Description
7	The file transfer is finished and the configuration file is applied.
8	Automatic update. The file transfer starts.

- If you have selected **days** in Step 6, set the time of the day when to initiate a configuration update in the *Time Range* field.



Note: The *Time Range* field is not supported by all units. If it is greyed out, go to Step 4 to set the *Time of Day* field.

The time of the day is based on the SNTP time zone settings of the Mediatrix unit.

You must have a time server SNTP that is accessible and properly configured, or the automatic configuration update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. See ["SNTP" on page 73](#) for information on how to connect to a SNTP server.

If a time range is specified, the unit will download the configuration files at a random time within the interval specified.

The format should be one of the following:

```
hh[:mm[:ss]]
hh[:mm[:ss]] - hh[:mm[:ss]]
```

Where:

```
hh: Hours.
mm: Minutes.
ss: Seconds.
```

The configuration files are downloaded at the first occurrence of this value and thereafter with a period defined by the *Update Every* drop-down menus. Let's say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the time range is set to '14:00 - 15:00' and the automatic unit configuration update is enabled within those hours, the first update will take place the following day. This means that a range of '00:00:00 - 23:59:59' will always take place the next day.

- If you have selected **Days** in Step 2, set the time of the day when to initiate a configuration update in the *Time of Day* field.



Note: This parameter has been deprecated in certain Mediatrix units and replaced with the *Time Range* parameter (see Step 3). It is still available for these units, but Media5 suggests to use the *Time Range* parameter.

The time of the day is based on the SNTP time zone settings of the Mediatrix unit.

You must have a time server SNTP that is accessible and properly configured, or the automatic configuration update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. See ["SNTP" on page 73](#) for information on how to connect to a SNTP server.

The configuration files are downloaded at the first occurrence of this value and thereafter at the period defined by the *Update Every* drop-down menus. Let's say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the automatic update is enabled after 14h00, the first update will take place the day after at 14h00, then the second download two days later at the same hour, and so on.

Selecting **Random** means that the time of the day at which the Mediatrix unit first downloads the configuration files is randomly selected.

Privacy Settings

You can secure the exchange of configuration files between the server and the Mediatrix unit. A privacy key allows the unit to decrypt a previously encrypted configuration file.

To encrypt a configuration file (generic or specific), you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts files before sending them to the Mediatrix unit. Contact your sales representative for more details.

The following describes how to decrypt a previously encrypted generic or specific configuration file. You must have one key for the generic configuration file and another key for the specific configuration file.

► To set privacy settings:

1. In the *Privacy* section of the *Configuration File Fetching* window, select the **Enable Decryption of Configuration File** option.

The Mediatrix unit will be able to decrypt the next encrypted generic or specific configuration file. If you do not select the option, the configuration file is not decrypted by the unit and the configuration update fails.

2. Set the proper decryption password field with the password used to decrypt the configuration file.

Table 63: Decryption Passwords

Configuration File	Field
Generic	Generic Secret
Specific	Specific Secret

The password is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F. All other characters are not supported.

Each character encodes 4 bits of the key. For instance, a 32-bit key requires 8 characters.

- If you enter too many bits, the key is truncated to the first 448 bits.
- If you do not enter enough bits, the key is padded with zeros.

For instance, a 32-bit key could look like the following: A36CB299.

This key must match the key used for the encryption of the relevant configuration file.

If the field is empty, the configuration file is not decrypted.

Software Download Parameters

This [chapter](#) describes how to automatically download a software version available on the designated software server into the Mediatrix unit.



Note: Refer to [“Downloading a Software Version” on page 57](#) if you want to manually download a software load.



Note: Software Download parameters are available for units that run the SIP v4.5, SIP v5.x, H.323 v5.x, and MGCP/NCS v5.x signalling protocols. They are also available on the Dgw v1.1/2.0 units.

Before Downloading

To download a software, you may need to setup the following applications on your computer:

- ▶ TFTP server with proper root path
- ▶ Software upgrade zip file
- ▶ SNTP server properly configured
- ▶ HTTP server with proper root path
- ▶ Syslog daemon (optional)

Configuring the TFTP Server

If you are to perform a software download by using the TFTP protocol, you must install a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server. This PC must not have a firewall running. Media5 also recommends to place the PC and the UMN in the same subnet.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

If you are to use the automatic software update feature (see [“Auto-Update Settings” on page 132](#) for more details), you must have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation.

Configuring the HTTP Server

If you are to perform a software download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. This PC must not have a firewall running. Media5 also recommends to place the PC and the Mediatrix unit in the same subnet.

It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

Extracting the Zip File

The zip file contains the software information required for the download.

Extract the contents of the zip file on the PC designated as the software download server. Be sure to use the defined folder name. This creates a directory that contains the files required for the Mediatrix unit to properly update its software.

The directory name must be the same as the name defined in the *Remote File Location* field or *Static Image Location* field. See [“Download Settings” on page 130](#) for more details.

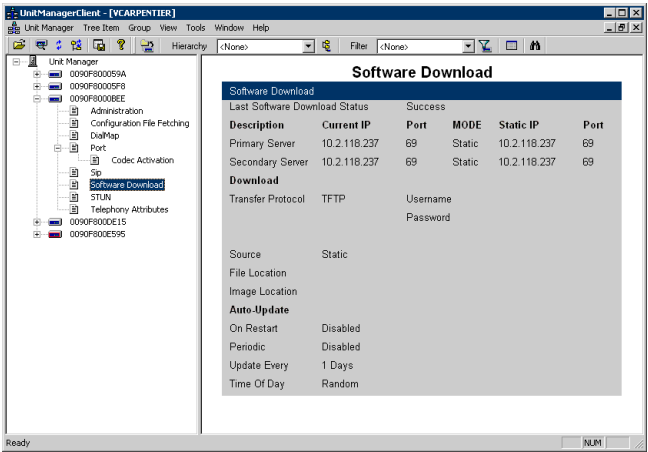
Media5 suggests that a folder, named identically to the software build, be available and used for the files related to that build only. Each folder should include only one delivery to ensure accuracy.

This directory must be located under the root path as defined in the TFTP/HTTP server or the software download will not proceed.

Software Download Overview

Upon selecting the *Software Download* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 100: Software Download Parameters Overview



You can change the value of the Software Download parameters by accessing the *Software Download* window. For Dgw v1.1/2.0 units, an alternate *Software Download* window is available.

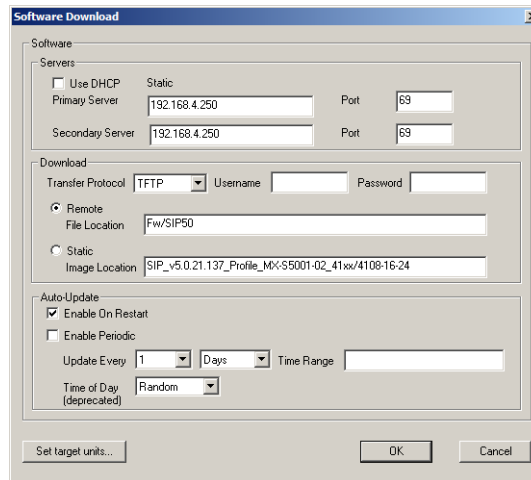
Software Download Window

The *Software Download* window allows you to define the various parameters to download a software version.

► **To access the *Software Download* window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Software Download* category.
The *Software Download* window opens.

Figure 101: Software Download Window



3. Set the following parameters:
 - [“Server Settings” on page 129](#)
 - [“Download Settings” on page 130](#)
 - [“Auto-Update Settings” on page 132](#)
4. To apply changes to more than one Mediatrix unit, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Server Settings

The *Server* section of the *Software Download* window allows you to define how to transfer the software.

► **To set server parameters:**

1. In the *Server* section, set the IP information.
 - If you want the Mediatrix unit to receive its IP information via a DHCP server, check the *Use DHCP* option.
 - If you want to enter static IP information, uncheck the *Use DHCP* option and enter the IP information in the corresponding fields.

Table 64 describes the static IP information you can define.

Table 64: Static IP Information Parameters

Parameter	Definition
Primary Server	Software download primary server static IP address/domain name and port. The default port value (69) complies to RFC 1340 on the well-known ports (assigned numbers). This value applies to a TFTP server. It may be different for other servers. If you are using an HTTP server to perform the software download, you must change the port value to 80.
Secondary Server	Software download secondary server static IP address or domain name and port. The default port value (69) complies to RFC 1340 on the well-known ports (assigned numbers). This value applies to a TFTP server. It may be different for other servers. If you are using an HTTP server to perform the software download, you must change the port value to 80.

Download Settings

The *Download* section allows you to define how to transfer the software version into the Mediatrix unit.

► To set download parameters:

1. In the *Download* section of the *Software Download* window, set the transfer protocol to use in the *Transfer Protocol* field.
You have the choice between **TFTP** and **HTTP**.
Your HTTP server may activate some caching mechanism for the software download. This mechanism caches the initial software download for later processing, thus preventing changes or update of the original download by the user. This can cause problems if a user wants to modify the software download and perform it again immediately. The result will still return the original download and not the new one.
2. If your HTTP server requires authentication to download the software file, set the following:
 - The user name in the *Username* field.
 - The password in the *Password* field.

The Mediatrix unit supports basic and digest HTTP authentication, as described in RFC 2617.
3. Set the software download path.
When performing a software download, you must configure the path, on the remote software download server, of the directory where you extracted the files required for the download.
The directory must be located under the root path, as defined in the TFTP or HTTP server, or the software download will not proceed. See [“Before Downloading” on page 127](#) for more details.
The Mediatrix unit first downloads a file called “setup.inf”. This file contains the list of all the other files to download, depending on the product. The “setup.inf” file and all the other files must be in the same directory. If any of the files is missing, the procedure will not work properly.

You have the following choices:

Table 65: Image Location Parameters

Parameter	Description
Remote File Location	The image location is defined in a file called "mediatrixNNNtargetimage.inf", where <i>NNN</i> corresponds to a specific product name. Set the location of this file in the field. See the Mediatrix unit <i>Reference Manual</i> for the proper product name. This is useful if you are using automatic updates with multiple units.
Static Image Location	Set the directory in the field.

4. If you selected the **Remote File Location** method (see Step 3):
 - a. Create a text file and write the path and/or name of the directory that contains the files required for download. Save this file as "mediatrixNNNtargetimage.inf" under the server root path, where *NNN* corresponds to a specific product name.



Note: If you leave the file empty, the Mediatrix unit will look for the software download information in the root directory of the software download server.

- b. Configure the path of the "mediatrixNNNtargetimage.inf" file in the *Remote File Location* field. Note that the selection file name is in lower case. Some web servers are case sensitive.
This is useful if you are using automatic updates with multiple units. If you want the units to download a new version, you only have to change the path once in the "mediatrixNNNtargetimage.inf" file. If you were to use the *Static Image Location* option, you would have to change the path in every unit.

Example

Let's consider the following example:

- ▶ The directory that contains the files required for download is called: **SIP_v5.0.1.1_MX-S5001-01**.
- ▶ This directory is under **C:/Root/Download**.

Table 66: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	SIP_v5.0.1.1_MX-S5001-01
c:/	root/download/SIP_v5.0.1.1_MX-S5001-01
c:/root	download/SIP_v5.0.1.1_MX-S5001-01

The following are some tips to help your download process:

- ▶ If available, use the *Browse* button (or equivalent) of the TFTP/HTTP server to select the directory, eliminating typographical errors.
- ▶ Use the "/" character when defining the path to indicate sub-directories. For instance, *root/download*.
If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the "/" character and produce an error. In this case, use the "\" character.
- ▶ Use basic directory names, without spaces or special characters such as "~", "@", etc., which may cause problems.
- ▶ Cut and paste the path and/or name of the directory that contains the extracted files into the image path of the Mediatrix unit (you may have to convert "\" into "/") to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file names may also differ from the example shown above.

Auto-Update Settings

You can configure the Mediatrix unit to automatically update its software version. This update can be done:

- ▶ Every time the Mediatrix unit restarts.
- ▶ At a specific time interval you can define.

▶ To set the automatic update parameters:

1. In the *Auto-Update* section of the *Software Download* window, select the auto-update feature to use:

Table 67: Auto-Update Options

Parameter	Description
Enable on Restart	Updates the Mediatrix unit every time it restarts.
Enable Periodic	Updates the Mediatrix unit at a specific time interval you can define. In that case, go to Step 2.

2. For a Periodic update, set the waiting period between each software update in the *Update Every* fields.

The time base available for automatic software updates is as follows:

Table 68: Time Unit Parameters

Parameter	Description
Seconds	Updates the unit's software every x seconds. You can specify the x value in the first field.
Minutes	Updates the unit's software every x minutes. You can specify the x value in the first field.
Hours	Updates the unit's software every x hours. You can specify the x value in the first field.
Days	Updates the unit's software every x days. You can specify the x value in the first field. You can also define the time of day when to perform the update in the <i>Time Range</i> field (see Step 3) or <i>Time of Day</i> field (see Step 4).

The time unit values available are from 1 to 48.

It may be possible that the Mediatrix unit skips a scheduled periodic update if the previous periodic update has not finished yet. This may happen with periods of a few seconds.

Let's say for instance that you set the period to two seconds and the automatic update mechanism takes five seconds to complete. The following describes the behaviour:

Table 69: Scheduled Periodic Update

Time (s)	Description
0	Beginning of the automatic update mechanism.
2	Automatic update. The file transfer starts.
4	Automatic update. The Mediatrix unit skips this scheduled update because the previous update has not finished yet.
6	Automatic update. The Mediatrix unit skips this scheduled update because the previous update has not finished yet.

Table 69: Scheduled Periodic Update (Continued)

Time (s)	Description
7	The file transfer is finished and the software is applied.
8	Automatic update. The file transfer starts.

3. If you have selected **Days** in Step 2, set the time of the day when to initiate a software update in the *Time Range* field.



Note: The *Time Range* field is not supported by all units. If it is greyed out, go to Step 4 to set the *Time of Day* field.

The time of the day is based on the SNTP time zone settings of the Mediatrix unit.

You must have a time server SNTP that is accessible and properly configured, or the automatic software update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. See [“SNTP” on page 73](#) for information on how to connect to a SNTP server.

If a time range is specified, the unit will initiate the image software download at a random time within the interval specified.

The format should be one of the following:

```
hh[:mm[:ss]]
hh[:mm[:ss]] - hh[:mm[:ss]]
```

Where:

```
hh: Hours.
mm: Minutes.
ss: Seconds.
```

The image software download is initiated at the first occurrence of this value and thereafter with a period defined by the *Update Every* drop-down menus. Let's say for instance the automatic update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the time range is set to '14:00 - 15:00' and the automatic update is enabled within those hours, the first update will take place the following day. This means that a range of '00:00:00 - 23:59:59' will always take place the next day.

4. If you have selected **Days** in Step 2, set the time of the day when to initiate a software update in the *Time of Day* field.



Note: This parameter has been deprecated in certain Mediatrix units and replaced with the *Time Range* parameter (see Step 3). It is still available for these units, but Media5 suggests to use the *Time Range* parameter.

The time of the day is based on the SNTP time zone settings of the Mediatrix unit.

You must have a time server SNTP that is accessible and properly configured, or the automatic software update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. See [“SNTP” on page 73](#) for information on how to connect to a SNTP server.

The software file is downloaded at the first occurrence of this value and thereafter at the period defined by the *Update Every* drop-down menus. Let's say for instance the automatic software update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on.
- If the automatic update is enabled after 14h00, the first update will take place the day after at 14h00, then the second download two days later at the same hour, and so on.

Selecting **Random** means that the time of the day at which the Mediatrix unit first downloads the software is randomly selected.

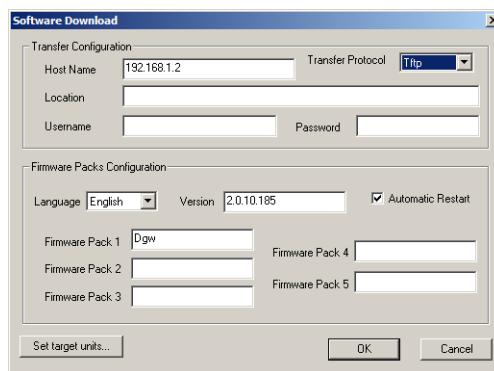
Software Download Window (Dgw v1.1/2.0 Units)

The *Software Download* window allows you to define the various parameters to download a software version.

► **To access the *Software Download* window:**

1. Select the unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *Software Download* category.
The *Software Download* window opens.

Figure 102: Software Download Window



3. Set the following parameters:
 - [“Transfer Configuration” on page 135](#)
 - [“Firmware Packs Configuration” on page 136](#)
4. To apply changes to more than one Mediatrix unit, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Transfer Configuration

The following describes how to configure the transfer parameters required to perform a firmware update.

► **To setup the firmware download path:**

1. In the *Transfer Configuration* section, set the static update files server IP address or domain name and port number to use when downloading a firmware pack in the *Host Name* field.
This is the current address and port number of the PC that hosts the firmware packs. Use the special port value 0 to indicate the protocol default. For instance, the TFTP default port is 69, the HTTP default port is 80, and the HTTPS default port is 443.
The default value is **0.0.0.0:0**.
This parameter is not required if you have selected the **File** transfer protocol.
2. Select a transfer protocol to transfer a firmware pack in the *Transfer Protocol* drop-down menu.
You have the following choices:
 - HTTP: Standard Hyper Text Transfer Protocol.
 - HTTPS: Hyper Text Transfer Protocol over Transport Layer Security.
 - TFTP: Trivial File Transfer Protocol.
 - FTP: File Transfer Protocol. Note that the UMN FTP client does not support the EPSV command.
 - File: The firmware pack is located on an external USB device.

HTTP and HTTPS support basic or digest authentication mode as described in RFC 2617. HTTPS requires a valid certificate.



Note: The File transfer protocol is not currently supported.

If you have selected HTTP or HTTPS, please note that your HTTP server may activate some caching mechanism for the firmware pack download.

If you have selected TFTP, be sure that UDP ports 60000 to 60512 inclusively are opened in your firewall.

3. Set the firmware download path in the *Location* field.

This is the location of the “Mediatix” folder that contains the modules to download into the UMN. In other words, this is where the zip file containing the firmware pack has been extracted. This path is relative to the root of the external media and excludes the “Mediatix” directory.

Let's consider the following example:

- The directory that contains the files required for download is called: **Mediatix**.
- This directory is under **C:/Root/Download**.

Table 70: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	N/A
c:/	root/download
c:/root	download

The following are some tips to help your download process:

- Use the “/” character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol, note that some TFTP servers on Windows do not recognize the “/” character and produce an error. In this case, use the “\” character.
- Use basic directory names, without spaces or special characters such as “~”, “@”, etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted files into the image path of the UMN (you may have to convert “\” into “/”) to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file names may also differ from the example shown above.

4. If your server requires authentication when downloading a firmware pack, set the following:
 - The user name in the *User Name* field.
 - The password in the *Password* field.
5. Proceed to [“Firmware Packs Configuration” on page 136](#).

Firmware Packs Configuration

► To set the firmware pack parameters:

1. In the *Firmware Packs Configuration* section, enter the version of the firmware pack to install in the *Version* field.

Currently, you cannot install two firmware packs with different versions.



Note: The *Language* drop-down menu currently supports only English.

2. Check the *Automatic Restart* option if you want the unit to restart once the download is complete.
3. Enter the name of up to five firmware packs to install in the *Firmware Pack* fields.
You can install several firmware packs at the same time. In that case, enter the firmware pack names in different rows of the table.
When extracting the content of the ZIP file, available firmware packs are listed as directories under the *Mediatrix/FirmwarePacks* directory.

STUN (Simple Traversal of UDP through NATs) is a simple client / server protocol that uses UDP packets to discover the configuration information of NATs and firewalls between a device and the public Internet:

- ▶ NAT type
- ▶ NAT binding public address
- ▶ NAT binding time to live

NAT (Network Address Translator) is a device that translates the IP address used within a “private” network to a different IP address known in another “public” network.



Note: STUN parameters are available for units that run the SIP v5.x and MGCP/NCS v5.x signalling protocols.

Introduction

STUN supports a variety of existing NAT devices and does not require any additional hardware or software upgrades on the NAT device.

The Mediatrix unit uses the STUN protocol to discover its NAT binding for the following three IP addresses/ports (sockets):

- ▶ Signalling protocol (SIP) IP address/port
- ▶ RTP IP address/port
- ▶ T.38 IP address/port

SIP Outbound Proxy



Note: This applies only to units that run the SIP protocol.

For a SIP unit to work properly behind a firewall, it must keep a pinhole opened by sending keepalive packets through the firewall.

The Mediatrix unit only sends keepalive packets to the last destination for a specific socket. When a unit is not configured with an outbound proxy, it can send, through its SIP socket, messages to various destinations, such as a SIP redirect server, another SIP unit, or a MWI server. If, for instance, the last SIP message was sent to the MWI server, the Mediatrix unit will keep the pinhole opened for the MWI server only (sending keepalive message to the MWI server) and won't be reachable by other units outside the firewall.

To avoid those issues, all SIP message should come and go from the same source/destination on the public side of the firewall, i.e., a SIP outbound proxy. Media5 thus recommends that you use a SIP outbound proxy.

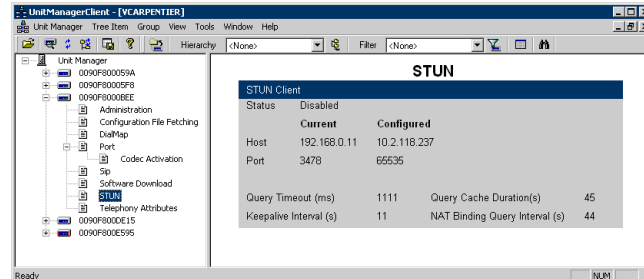
Restrictions on the Media5 STUN Implementation

- ▶ The Mediatrix unit does not currently support NAT type discovery.
- ▶ The Mediatrix unit does not currently support STUN NAT binding time to live discovery.
- ▶ The Mediatrix unit does not currently support the TLS security mechanism.
- ▶ Due to a limitation of most routers, an RTP portal might be required in order for two units behind the same NAT/firewall to be able to communicate with each other.

STUN Overview

Upon selecting the *STUN* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 103: STUN Parameters Overview



You can change the value of the STUN parameters by accessing the *STUN* window.

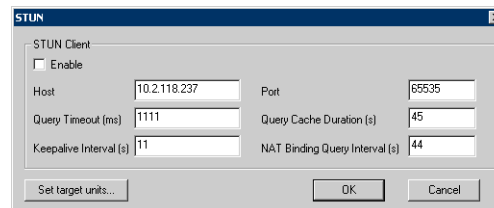
STUN Window

The *STUN* window allows you to define the Mediatrix unit STUN client.

► **To access the *STUN* window:**

1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
2. Double-click the *STUN* category.
The *STUN* window opens.

Figure 104: STUN Window



3. Enable the STUN client by selecting the **Enable** option.
This enables the STUN client for all sockets (VoIP signalling, RTP and T.38) altogether.
The following behaviour only applies to units that run the SIP protocol.:
 - If a unit is unable to re-register and there are no ongoing calls, it tries to rediscover its NAT binding for the signalling protocol socket.
 - If a STUN server is unresponsive, it is put in a “penalty box” for 60 seconds.
4. Set the static STUN server IP address or Fully Qualified Domain Name (FQDN) in the *Host* field.
5. Set the static STUN server IP port number in the *Port* field.
The default value is **3478**.
6. Set the maximum amount of time, in milliseconds, the Mediatrix unit should wait for an answer to a STUN query sent to a STUN server in the *Query Timeout* field.
Available values range from 500 ms to 10000 ms.

Caution is advised in setting long timeouts. In the advent of an unresponsive STUN server, the unit may end up waiting a long time before it determines that a call cannot be made due to the STUN server failure.

7. Set the amount of time, in seconds, the Mediatrix unit should keep a STUN query result in its internal cache in the *Query Cache Duration* field.

Keeping a query in a cache helps to reduce the amount of unnecessary STUN queries when an RTP or T.38 socket is re-used within a short period of time. Available values range from 0 s to 3600 s.

When set to **0**, the cache is disabled and the unit performs a STUN query each time a socket needs to be used.

8. Define the interval, in seconds, at which the Mediatrix unit sends blank keepalive messages to keep a firewall hole opened in the *Keepalive Interval* field.

Keepalive messages are used by both the signalling protocol socket (SIP) and the RTP socket to keep those connections opened through a firewall. Available values range from 0 s to 120 s.

When set to **0**, no keepalive packet is sent.



Note: Keepalive messages are not supported on the T.38 socket.

9. Set the frequency, in seconds, at which a FXO Gateway unit should do NAT binding discovery for its signalling protocol socket in the *NAT Binding Query Interval* field.

This is only used with units that do not register their ports. Units that register their ports do their NAT binding discovery just before registering.

10. To apply changes to more than one Mediatrix unit, click the *Set target units* button.

Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Subscriber Services Parameters

This [chapter](#) describes how to set the various subscriber services available on the users' phone. There are basic subscriber services, such as call hold and conference, as well as more advanced services, such as call forwarding.

Please refer to the Mediatrix unit *User's Manual* for more details on how to actually use the services.



Note: Subscriber services are only available for FXS units that run the SIP v4.4, SIP v4.5, or H.323 v4.0 signalling protocol.

Subscriber Services Overview

Upon selecting the *Subscriber Services* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 105: Subscriber Services Parameters Overview

Subscriber Services							
Call Waiting							
Digits to disable <empty>							
Port 1							
Services	Attended Transfer	Blind Transfer	Call Hold	Call Waiting	Conference	Second Call	
Activation	Enable	Enable	Enable	Enable	Enable	Enable	
Status	Active	Active	Active	Active	Active	Active	
Port 2							
Services	Attended Transfer	Blind Transfer	Call Hold	Call Waiting	Conference	Second Call	
Activation	Enable	Enable	Enable	Enable	Enable	Enable	
Status	Active	Active	Active	Active	Active	Active	
Port 3							
Services	Attended Transfer	Blind Transfer	Call Hold	Call Waiting	Conference	Second Call	
Activation	Enable	Enable	Enable	Enable	Enable	Enable	
Status	Active	Active	Active	Active	Active	Active	

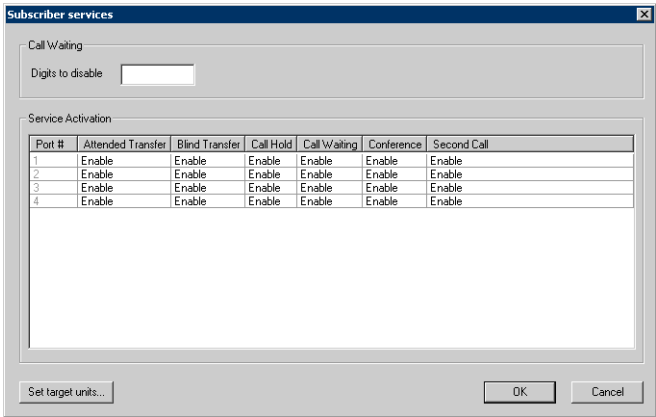
You can change the value of these parameters by accessing the *Subscriber services* window.

Subscriber Services Configuration Window

The *Subscriber services* window allows you to define and configure the services supported.

- **To access the Subscriber services window:**
- 1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
 - 2. Double-click the *Subscriber Services* category.
The *Subscriber services* window opens.

Figure 106: Subscriber Services Window



The *Subscriber services* window allows you to enable/disable the basic services once they are set. Please refer to the various services involved for more details.

The services use tables to set the relevant information. You can modify a value in the following manner:

- Select it in the row (port) you want to change.
This value becomes highlighted.
- Modify the value for the variable, and then press the <Enter> key of your keyboard.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 71: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

Call Hold

The Call Hold service allows the user to temporarily put an existing call on hold, usually by using the “flash” button of the telephone. The user can resume the call in the same way.

You must enable this service for the following services to work properly:

- ▶ Call Waiting
- ▶ Second Call
- ▶ Call Transfer – Blind Transfer
- ▶ Call Transfer – Attended Transfer
- ▶ Conference Call

▶ **To enable the call hold service:**

1. In the *Subscriber services* window, set to **enable** the *Call Hold* column corresponding to the port for which to enable the service.
2. Repeat for the other ports if applicable.
3. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Call Waiting

The call waiting tone indicates to an already active call that a new call is waiting on the second line.

Users can activate/deactivate the call waiting tone for their current call. This is especially useful when transmitting faxes. The user that is about to send a fax can thus deactivate the call waiting tone to ensure that the fax transmission will not be disrupted by an unwanted second call. When the fax transmission is completed and the line is on-hook, the call waiting tone is automatically reactivated.

▶ **To set the Call Waiting service:**

1. In the *Subscriber services* window, set to **enable** the *Call Waiting* column corresponding to the port for which to enable the service.

This permanently activates the call waiting tone. When receiving new calls during an already active call, a special tone is heard to indicate that a call is waiting on the second line. The user can then answer that call by using the “flash” button. The user can switch between the two active calls by using the “flash” button.

You must enable the call hold service for this service to work. See [“Call Hold” on page 145](#).



Note: If you are exclusively using faxes, set the column to **disable** to permanently disable the call waiting tone.

2. Repeat for the other ports if applicable.
3. In the *Call Waiting* section at the top of the window, define the digits that users must dial to disable the Call Waiting tone in the *Digits to disable* field.

This allows a user who has call waiting enabled to disable that service on the next call only. If, for any reason, the user wishes to undo the cancel, unhooking and re-hooking the telephone resets the service.

For instance, you could decide to put “*76” as the sequence a user must dial to disable the call waiting tone. This sequence must be unique. Note that dialing these digits does not have any effect unless the service’s status is “enable”.

The deactivating sequence is set for all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

4. To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Second Call

The Second Call service allows a user with an active call to put the call on hold, and then initiate a new call on the second line. This service is most useful with the transfer and conference services.

You must enable the call hold service for this service to work. See [“Call Hold” on page 145](#).

► **To enable the second call service:**

1. In the *Subscriber services* window, set to **enable** the *Second Call* column of the port for which to enable the service.
2. Repeat for the other ports if applicable.
3. To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Call Transfer – Blind Transfer

The blind call transfer service is sometimes called Transfer without Consultation or Unattended Transfer. It allows a user to transfer a call on hold to a still ringing (unanswered) call.



Note: This service is only available for units that run the SIP v4.4 or SIP v4.5 signalling protocol.

You must enable the call hold and second call services for this service to work. See [“Call Hold” on page 145](#) and [“Second Call” on page 146](#).

► **To enable the blind transfer service:**

1. In the *Subscriber services* window, set to **enable** the *Blind Transfer* column of the port for which to enable the service.
2. Repeat for the other ports if applicable.
3. To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Call Transfer – Attended Transfer

The attended call transfer service is sometimes called Transfer with Consultation. It allows a user to transfer a call on hold to an active call.

You must enable the call hold and second call services for this service to work. See [“Call Hold” on page 145](#) and [“Second Call” on page 146](#).

► **To enable the attended transfer service:**

1. In the *Subscriber services* window, set to **enable** the *Attended Transfer* column of the port for which to enable the service.
2. Repeat for the other ports if applicable.
3. To apply changes to several Mediatrix units, click the *Set target units* button.

Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Conference Call

The Conference Call service allows a user to link two or more calls together to form a single conversation, called a conference.



Note: This service is only available for units that run the SIP v4.4 or SIP v4.5 signalling protocol.

Be aware that:

- ▶ Only 3-way conferences are currently supported.
- ▶ A participant of the conference can put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. The participant who initiated the conference cannot put it on hold.

You must enable the call hold and second call services for this service to work. See [“Call Hold” on page 145](#) and [“Second Call” on page 146](#).

▶ **To enable the conference call service:**

1. In the *Subscriber services* window, set to **enable** the *Conference* column of the port for which to enable the service.
2. Repeat for the other ports if applicable.
3. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Call Forward

The Call Forward service offers various ways to forward calls:

- ▶ Call Forward – Unconditional
- ▶ Call Forward – On Busy
- ▶ Call Forward – On No Answer

Call Forward – Unconditional

The Call Forward – Unconditional feature allows users to forward all of their calls to another extension or line.

▶ **To set the Call Forward Unconditional service:**

1. Expand the *Subscriber Services* category of the selected unit by clicking the [+] icon on the left. A list of services displays.
2. Double-click the *Call forwarding unconditional* category.
The *Call Forwarding Unconditional* window opens.

Figure 107: Call Forwarding Unconditional Window

3. In the *Services Settings* section, set the *Service Status* column with one of the following:
 - inactive
 - active

This column starts the service (active) or stops the service (inactive).

If you want to let the user start or stop the service with his or her handset, you must enter a sequence of digits in steps 4 and 5. The *Service Status* column is automatically updated to reflect the activation status according to the user's setting.

4. In the *General* section, define the digits that users must dial to start the Call Forward Unconditional service in the *Digits to enable* field.

Define this field only if you want to let the user start the service with his or her handset. If you rather want to have the control over the activation/deactivation of the service, see Step 3.

For instance, you could decide to put “*70” as the sequence to activate the service. This sequence must be unique. Note that dialing these digits does not have any effect unless the service's status is “enable”. This value must also be different from the value set in Step 5.

The activating sequence applies to all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

5. Define the digits that users must dial to stop the Call Forward Unconditional service in the *Digits to disable* field.

Define this field only if you want to let the user stop the service with his or her handset. If you rather want to have the control over the activation/deactivation of the service, see Step 3.

For instance, you could decide to put “*71” as the sequence to deactivate the service. This sequence must be unique. Note that dialing these digits does not have any effect unless the service's status is “enable”. This value must also be different from the value set in Step 4.

The deactivating sequence applies to all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

6. In the *Services Settings* section, define the address to which forward incoming calls in the corresponding *Forwarding Address* column.

For units using the H.323 signalling protocol, you can use the following aliases:

Table 72: H.323 Aliases Types

Alias Type	Description
IP address	A valid IP address with a port number could be: <i>IP=10.2.25.34:1720</i> . The port information (:1720) is optional.
H.323 ID alias	A valid H.323 ID alias could be: <i>H323ID=terminal1</i> .
E.164 alias	A valid E.164 alias could be: <i>E164=5692356</i> .

Table 72: H.323 Aliases Types (Continued)

Alias Type	Description
Party Number	A valid party number (of type “public network specific number”) could be: <i>PUNSN=18003446768</i> . See the unit's Administration manual for a list of party number types supported.

For units using the SIP signalling protocol, accepted formats are:

Table 73: SIP Addresses Supported

Alias Type	Description
Telephone numbers	A valid telephone number could be: <i>5551111</i> .
SIP URLs	SIP URLs such as “scheme:user@host” are supported. For instance, “sip:user@foo.com”.

Note that this string is used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

For more information on the syntax to use, please refer to your unit's Administration manual.

7. Repeat for the other ports if applicable.
8. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
You can exclude the configuration you have set in the *Service Settings* section by checking the *Exclude service settings from multiple targets* option. You must then set the service settings on the other units.
9. Enable the Call Forward Unconditional service by setting the *Allow Call Forward digits* column to **enable**.
If you set the field to **disable**, this will not disable the call forward, but will prevent the user from activating or deactivating the service. The user will not be able to use the digits used to start and stop the service.
10. Click *OK* when all changes are done.

Call Forward – On Busy

You can automatically forward the incoming calls of your users to a pre-determined target if they are already on the line. The user does not have any feedback that a call was forwarded.

► To set the Call Forward On Busy service:

1. Expand the *Subscriber Services* category of the selected unit by clicking the [+] icon on the left.
A list of services displays.
2. Double-click the *Call forwarding on busy* category.
The *Call Forwarding On Busy* window opens.

Figure 108: Call Forwarding On Busy Window

Port #	Allow Call Forward digits	Service Status	Forwarding Address
1	Disable	Inactive	
2	Disable	Inactive	

3. In the *Services Settings* section, set the *Service Status* column with one of the following:
 - inactive
 - active

This column starts the service (active) or stops the service (inactive).

If you want to let the user start or stop the service with his or her handset, you must enter a sequence of digits in steps 4 and 5. The *Service Status* column is automatically updated to reflect the activation status according to the user's setting.

4. In the *General* section, define the digits that users must dial to start the Call Forward On Busy service in the *Digits to enable* field.

Define this field only if you want to let the user start the service with his or her handset. If you rather want to have the control over the activation/deactivation of the service, see Step 3.

For instance, you could decide to put “*72” as the sequence to activate the service. This sequence must be unique. Note that dialing these digits does not have any effect unless the service's status is “enable”. This value must also be different from the value set in Step 4.

The activating sequence applies to all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

5. Define the digits that users must dial to stop the Call Forward On Busy service in the *Digits to disable* field.

Define this field only if you want to let the user stop the service with his or her handset. If you rather want to have the control over the activation/deactivation of the service, see Step 3.

For instance, you could decide to put “*73” as the sequence to deactivate the service. This sequence must be unique. Note that dialing these digits does not have any effect unless the service's status is “enable”. This value must also be different from the value set in Step 3.

The deactivating sequence applies to all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

6. In the *Services Settings* section, define the address to which forward incoming calls in the corresponding *Forwarding Address* field.

For units using the H.323 signalling protocol, you can use the following aliases:

Table 74: H.323 Aliases Types

Alias Type	Description
IP address	A valid IP address with a port number could be: <i>IP=10.2.25.34:1720</i> . The port information (:1720) is optional.
H.323 ID alias	A valid H.323 ID alias could be: <i>H323ID=terminal1</i> .
E.164 alias	A valid E.164 alias could be: <i>E164=5692356</i> .

Table 74: H.323 Aliases Types (Continued)

Alias Type	Description
Party Number	A valid party number (of type "public network specific number") could be: <i>PUNSN=18003446768</i> . See the unit's Administration manual for a list of party number types supported.

For units using the SIP signalling protocol, accepted formats are:

Table 75: SIP Addresses Supported

Alias Type	Description
Telephone numbers	A valid telephone number could be: <i>5551111</i> .
SIP URLs	SIP URLs such as "scheme:user@host" are supported. For instance, "sip:user@foo.com".

Note that this string is used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

For more information on the syntax to use, please refer to your unit's Administration manual.

7. Repeat for the other ports if applicable.
8. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in ["Setting Multiple Units" on page 39](#). You can exclude the configuration you have set in the *Service Settings* section by checking the *Exclude service settings from multiple targets* option. You must then set the service settings on the other units.
9. Enable the Call Forward On Busy service by setting the *Allow Call Forward digits* column to **enable**.
If you set the field to **disable**, this will not disable the call forward, but will prevent the user from activating or deactivating the service. The user will not be able to use the digits used to start and stop the service.
10. Click *OK* when all changes are done.

Call Forward – On No Answer

You can forward the incoming calls of your users to a pre-determined target if they do not answer their phone. The user does not have any feedback that a call was forwarded.

► To set the Call Forward On No Answer service:

1. Expand the *Subscriber Services* category of the selected unit by clicking the [+] icon on the left. A list of services displays.
2. Double-click the *Call forwarding no answer* category.
The *Call Forwarding On No Answer* window opens.

Figure 109: Call Forwarding On No Answer Window

Port #	Allow Call Forward digits	Service Status	Timeout (ms)	Forwarding Address
1	Disable	Inactive	5000	
2	Disable	Inactive	5000	

3. In the *Services Settings* section, set the *Service Status* column with one of the following:
 - inactive
 - active

This column starts the service (active) or stops the service (inactive).

If you want to let the user start or stop the service with his or her handset, you must enter a sequence of digits in steps 4 and 5. The *Service Status* column is automatically updated to reflect the activation status according to the user's setting.

4. In the *General* section, define the digits that users must dial to start the Call Forward On No Answer service in the *Digits to enable* field.

Define this field only if you want to let the user start the service with his or her handset. If you rather want to have the control over the activation/deactivation of the service, see Step 3.

For instance, you could decide to put “*74” as the sequence to activate the service. This sequence must be unique. Note that dialing these digits does not have any effect unless the service's status is “enable”. This value must also be different from the value set in Step 5.

The activating sequence applies to all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

5. Define the digits that users must dial to stop the Call Forward On No Answer service in the *Digits to disable* field.

Define this field only if you want to let the user stop the service with his or her handset. If you rather want to have the control over the activation/deactivation of the service, see Step 3.

For instance, you could decide to put “*75” as the sequence to deactivate the service. This sequence must be unique. Note that dialing these digits does not have any effect unless the service's status is “enable”. This value must also be different from the value set in Step 4.

The deactivating sequence applies to all the ports of the Mediatrix unit. You cannot have a different sequence for each port.

6. In the *Services Settings* section, define the address to which forward incoming calls in the corresponding *Forwarding Address* field.

For units using the H.323 signalling protocol, you can use the following aliases:

Table 76: H.323 Aliases Types

Alias Type	Description
IP address	A valid IP address with a port number could be: <i>IP=10.2.25.34:1720</i> . The port information (:1720) is optional.
H.323 ID alias	A valid H.323 ID alias could be: <i>H323ID=terminal1</i> .
E.164 alias	A valid E.164 alias could be: <i>E164=5692356</i> .

Table 76: H.323 Aliases Types (Continued)

Alias Type	Description
Party Number	A valid party number (of type “public network specific number”) could be: <i>PUNSN=18003446768</i> . See the unit’s Administration manual for a list of party number types supported.

For units using the SIP signalling protocol, accepted formats are:

Table 77: SIP Addresses Supported

Alias Type	Description
Telephone numbers	A valid telephone number could be: <i>5551111</i> .
SIP URLs	SIP URLs such as “scheme:user@host” are supported. For instance, “sip:user@foo.com”.

Note that this string is used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

For more information on the syntax to use, please refer to your unit’s Administration manual.

7. Define the time, in milliseconds, the telephone keeps ringing before the call forwarding activates in the *Timeout (ms)* column.
8. Repeat for the other ports if applicable.
9. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).
You can exclude the configuration you have set in the *Service Settings* section by checking the *Exclude service settings from multiple targets* option. You must then set the service settings on the other units.
10. Enable the Call Forward On No Answer service by setting the *Allow Call Forward digits* column to **enable**.
If you set the field to **disable**, this will not disable the call forward, but will prevent the user from activating or deactivating the service. The user will not be able to use the digits used to start and stop the service.
11. Click *OK* when all changes are done.

Telephony Attributes Parameters

This **chapter** describes how to set the various telephony attributes, which are used to configure the characteristics of the telephony system being implemented.

Please refer to the Mediatrix unit *User's Manual* for more details on how to actually use the services.

Note: Telephony attributes are only available for units that run the SIP v4.4, SIP v4.5, or H.323 v4.0 signalling protocol.

Telephony Attributes Overview

Upon selecting the *Telephony Attributes* category of a Mediatrix unit, an overview of its parameters is displayed in the right pane of the Administrator window.

Figure 110: Telephony Attributes Parameters Overview

Port #	Call direction	Automatic call	Automatic call address	Hook flash processing
1-	No restriction	Disable	<empty>	Process locally
2-	No restriction	Disable	<empty>	Process locally
3-	No restriction	Disable	<empty>	Process locally
4-	No restriction	Disable	<empty>	Process locally

You can change the value of these parameters by accessing the *Telephony Attributes* window.

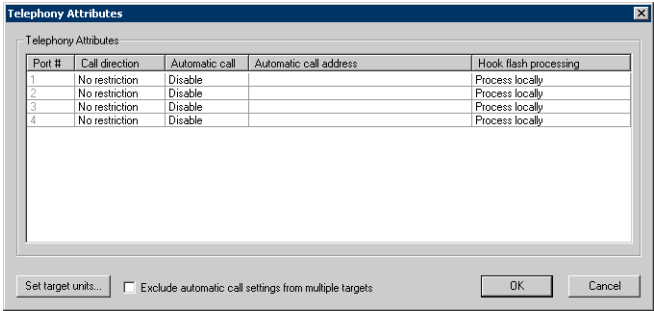
Telephony Attributes Configuration Window

The *Telephony Attributes* window allows you to define and configure the attributes supported.

► **To access the Telephony attributes window:**

- 1. Select the Mediatrix unit to modify and expand its categories by clicking the [+] icon on the left.
- 2. Double-click the *Telephony Attributes* category.
The *Telephony Attributes* window opens.

Figure 111: Telephony Attributes Window



This window allows you to set all the attributes of the selected unit. You can modify the value of an attribute in the following manner:

- Select it in the row (port) you want to change.
This value becomes highlighted.
- Modify the value for the variable, and then press the <Enter> key of your keyboard.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 78: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

Call Direction

You can define in which direction calls are allowed. The behaviour varies depending on if you are setting an FXS or FXO unit.

► **To set the call direction:**

1. In the row of the port for which to enable the service, set the *Call direction* column with the appropriate restriction on the direction of traffic.

Table 79: Call Direction Restrictions

Restriction	Description
noRestriction	Allows incoming and outgoing calls.
scnToIpOnly	FXO units: Allows only calls from the SCN to the IP network. The Mediatrix unit answers incoming calls but does not allow outgoing calls. FXS units: The Mediatrix unit allows to make calls but cannot receive calls.
ipToScnOnly	FXO units: Allows only calls from the IP network to the SCN. The Mediatrix unit allows outgoing calls but does not answer incoming calls. FXS units: The Mediatrix unit allows to receive calls but does not allow to make calls.

2. Repeat for the other ports if applicable.
3. To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Automatic Call

The automatic call feature allows you to define a telephone number that is automatically dialed when:

- The handset is taken off hook in the case of an FXS unit.
- Seizing an FXO line in the case of a SCN gateway.

This is especially useful if you want to redirect SCN calls to a specific IP number.



Note: In the case of a SCN gateway, this applies only for SCN to IP network calls.

When this service is enabled, the second line service is disabled but the call waiting feature is still functional. The user can still accept incoming calls.

► **To enable the automatic call service:**

1. In the row of the port for which to enable the service, set the *Automatic call enable* column to **enable**.
2. Enter the telephone number to dial in the *Automatic call address* column.
For units using the H.323 signalling protocol, you can use the following aliases:

Table 80: H.323 Aliases Types

Alias Type	Description
IP address	A valid IP address with a port number could be: <i>IP=10.2.25.34:1720</i> . The port information (:1720) is optional.
H.323 ID alias	A valid H.323 ID alias could be: <i>H323ID=terminal1</i> .
E.164 alias	A valid E.164 alias could be: <i>E164=5692356</i> .

Table 80: H.323 Aliases Types (Continued)

Alias Type	Description
Party Number	A valid party number (of type “public network specific number”) could be: <i>PUNSN=18003446768</i> . See the unit’s Administration manual for a list of party number types supported.

For units using the SIP signalling protocol, accepted formats are:

Table 81: SIP Addresses Supported

Alias Type	Description
Telephone numbers	A valid telephone number could be: <i>5551111</i> .
SIP URLs	SIP URLs such as “scheme:user@host” are supported. For instance, “sip:user@foo.com”.

Note that this string is used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

For more information on the syntax to use, please refer to your unit’s Administration manual.

3. Repeat for the other ports if applicable.
4. To apply changes to several Mediatix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#). You can exclude the automatic call settings you have defined by checking the *Exclude automatic call settings from multiple targets* option. You must then set the automatic call settings on the other units.

Hook Flash Processing

You can define how to process hook flash detection. Users normally press the “flash” button of the telephone during a call in progress to put this call on hold, transfer it, or even initiate a conference call. This allows the enabled subscriber services to be handled by the unit or to be delegated to a remote party.



Note: This service is only available for units that run the H.323 v4.0 signalling protocol.

► To define how to process hook flash:

1. In the row of the port for which to enable the service, set the *Hook flash processing* column with the appropriate value.

The following values are available:

Table 82: Hook Flash Settings

Setting	Definition
processLocally	The hook-flash is processed locally. The actual behaviour of the “flash” button depends on which subscriber services are enabled for this line. See “Chapter 15 - Subscriber Services Parameters” on page 143 for more details.

Table 82: Hook Flash Settings (Continued)

Setting	Definition
transmitUsingSignalingProtocol	The hook-flash is processed by a remote party. The hook-flash event is carried by a signalling protocol message. The actual behaviour of the “flash” button depends on the remote party. Note: This setting disables all subscriber services that use the “flash” button, such as the Call Hold service.

2. To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

This **chapter** describes how to work with the SNMP protocol.

Introduction

The *Simple Network Management Protocol* (SNMP) is a simple request-reply protocol for Internet network management services. It consists of *network management stations* communicating with *network elements*. Management stations are normally workstations that display relevant facts about the elements being monitored.

SNMP works over the IP (Internet Protocol) communication stack. SNMP network management consists of three pieces:

1. The protocol between the manager and the element, called the *Simple Network Management Protocol* (SNMP). This details the format of the packets exchanged. Although a wide variety of transport protocols could be used, UDP is normally used with SNMP.
2. A set of common structures and an identification scheme used to reference the variables in the MIB. This is called the *Structure of Management Information* (SMI).
3. A *Management Information Base* (MIB) that specifies what variables the network elements maintain (the information that can be queried and set by the manager).

The UMN supports three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3.

SNMPv3 Services

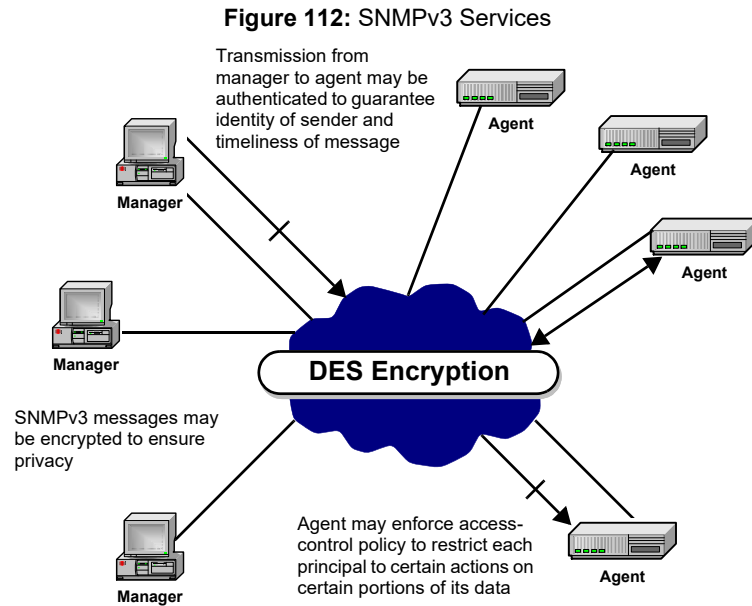
To correct the security deficiencies of SNMPv1/v2, SNMPv3 was defined with an overall SNMP architecture and a set of security capabilities. SNMPv3 includes three important services: *authentication*, *privacy*, and *access control* (Figure 112). To deliver these services in a flexible and efficient manner, SNMPv3 introduces the concept of a *principal* (user name), which is the entity on whose behalf services are provided or processing takes place.



Note: SNMPv3 settings are only available on v4.x/v5.x analog units.



Note: SNMPv3 makes extensive use of encryption, so working with it requires a large amount of resources from your PC. Media5 suggests that you use a recent PC with the appropriate CPU and memory resources.



SNMP Behaviour

When using SNMP, the following rules apply:

- ▶ Media5 recommends to copy the SNMPv3 user attributes only twice.
- ▶ The administrator may edit the SNMPv3 user attributes:
 - Authentication algorithm (none, MD5, or SHA)
 - Authentication password
 - Encryption algorithm (none or DES)
 - Encryption password
 - Security User Name
 - All SNMPv3 passwords (encryption and authentication) must be at least 8 characters long. The unit follows the SNMPv3 standard RFCs.

Furthermore, SNMP can be used in a non-secure or secure management mode.

Non-Secure Management Mode

In non-secure management mode, the unit responds to SNMP requests as follows:

- ▶ SNMPv1: read-write on all MIB tree
- ▶ SNMPv2c: read-write on all MIB tree
- ▶ SNMPv3: read-write on all MIB tree by using:
 - MD5 authentication
 - Authentication password: "Md5Password" (initial password)
 - DES encryption
 - Encryption password: "DesPassword" (initial password)
 - Security user name: "Md5DesUser"
- ▶ SNMPv3: read-write on all MIB tree by using:
 - SHA authentication
 - Authentication password: "ShaPassword" (initial password)
 - DES encryption
 - Encryption password: "DesPassword" (initial password)
 - Security user name: "ShaDesUser"

Secure Management Mode

In secure management mode, the unit responds to SNMP requests as follows:

- ▶ SNMPv1: read-only on all MIB tree (disable v1)
- ▶ SNMPv2c: read-only on all MIB tree (disable v2)
- ▶ SNMPv3: the same values as for SNMPv3 in non-secure management mode



Note: If you forget or lose a password, using the Factory Settings mode resets the unit to the non-secure management mode. See the corresponding *Administration Manual* for more details.

Setting Unit SNMP Preferences

You can set SNMP preferences for a specific unit. Each unit listed in the UMN can thus have different SNMP preferences settings. If you want to set SNMP preferences for a type of units, see [“Global SNMP Preferences” on page 11](#).

▶ To set SNMP preferences for a specific unit:

1. Right-click the Mediatrix unit for which to set the SNMP preferences.
2. In the context sensitive menu that opens, select the *SNMP Preferences* option.
The following window opens.

Figure 113: SNMP Preferences Window

3. In the *General settings* section, select the *Version* of SNMP used.
Supported values are SNMPv1, SNMPv2c, and SNMPv3.
These values are mutually exclusive. If you select SNMPv2c and you try to connect to a unit that does not support SNMPv2c, the connection will fail.
Some of the above fields and / or options may not be available depending on the software version of the selected Mediatrix unit.



Note: Digital Mediatrix units only support SNMPv1.

4. Set the *Timeout* in milliseconds.
When a SNMP request is sent to the remote unit, this unit must send an answer back within a specified period of time. This is the Timeout. If no answer is received within the Timeout value, the UMN sends the SNMP request again to the remote unit. If the unit still does not answer after the defined Number of retries, the UMN considers it as being off-line.
5. Define the *Port number* on which the remote unit listens for SNMP requests.
6. Define the *Community name*.
Media5 recommends not to change this value and keep *public*.
7. Define a *Number of retries*.

Number of times the UMN sends a SNMP request to the remote unit in case the unit does not answer within the specified Timeout. If the remote unit still does not answer after the defined Number of retries, the UMN considers it as being off-line.

You are now ready to set the GetBulk settings.

GetBulk Settings

The GetBulk operation is used to efficiently retrieve large blocks of data, such as multiple rows in a table. GetBulk settings are specific to SNMPv2c and SNMPv3. Define these settings if you want to connect to a remote unit that supports SNMPv2c or SNMPv3. They are used by the GetTable and GetWalk commands.



Note: These parameters are not available on digital Mediatrix units.

► To set GetBulk settings:

1. Access the *SNMP preferences* window and set the *Version* to *SNMPv2c* or *SNMPv3*.
2. In the *GetBulk settings* section, set the following parameters:

Table 83: GetBulk Parameters

Parameter	Description
Non repeaters	Number of pairs in the variable binding list array for which a single instance should be returned.
Maximum repetitions	Maximum number of repetitions to return.

You are now ready to set the SNMPv3 security settings.

SNMPv3 Security Settings

Set SNMPv3 security settings to successfully connect to a unit that supports SNMPv3.



Note: These parameters are not available on digital Mediatrix units.



Note: Create a user in the remote unit or SNMPv3 agent prior to defining the following settings. If not, you will not be able to connect to this remote unit or SNMPv3 agent.

► To set SNMPv3 security settings:

1. Access the *SNMP preferences* window and set the *Version* parameter to *SNMPv3*.
2. Click the *SNMPv3 Security* button.
The following window opens.

Figure 114: SNMPv3 Security Window

This window allows you to specify security information required to successfully connect to a SNMPv3 agent.

3. Set the following information:

Table 84: Security Settings Parameters

Parameter	Description
User name	SNMPv3 security user name. It is a human-readable alphanumeric string representing a user or a group of users. This field cannot be empty.
Context name	SNMPv3 context name. A MIB context is a named subset of the object instance in the local MIB.
Security level (radio buttons)	SNMPv3 security level at which SNMP messages can be sent or processed, expressed in terms of whether or not authentication and/or privacy are provided. The available values are: - No authentication or privacy - Authentication without privacy - Authentication with privacy All options are mutually exclusive.
Authentication protocol (drop-down list)	SNMPv3 authentication protocol. Available values are <i>MD5</i> or <i>SHA</i> .
Change Password - Authentication (button)	Opens the <i>Change Password</i> window to specify the SNMPv3 authentication password. You must have the proper rights granted by the SNMPv3 agent to proceed. Note: SNMPv3 passwords should not have repeating blocks of characters and must have at least 8 characters.
Privacy protocol (drop-down list)	SNMPv3 privacy protocol, for instance, DES.
Change Password - Privacy (button)	Opens the <i>Change Password</i> window to specify the SNMPv3 privacy password. You must have the proper rights granted by the SNMPv3 agent to proceed. Note: SNMPv3 passwords should not have repeating blocks of characters and must have at least 8 characters.

4. Click *OK* when all changes are done.
The SNMP information is saved in the server database. The server uses this information when communicating with the unit.
5. Click *OK* in the *SNMP preferences* window to apply all the settings.

Notes

- ▶ The Mediatrix units support Basic and Digest authentication as per RFC 3261.
- ▶ When using SNMPv3 with encryption (DES), you may experience delays when accessing MIB variables. This is normal because encrypting an IP packet takes in general longer than sending it over IP. If you experience any timeout, add a few seconds to the timeout period, and then try to reach the unit again. See [“Setting Unit SNMP Preferences” on page 163](#) for more details.
- ▶ Let's assume that the Mediatrix unit accepts requests with authentication only. If you perform requests by using encryption and authentication, assuming that the authentication password is valid, the SNMP agent still responds as if the requests were only authenticated.

SNMPv3 Unit Settings

You can set some SNMPv3 information on a unit that supports SNMPv3, provided this unit grants you the rights to do so.

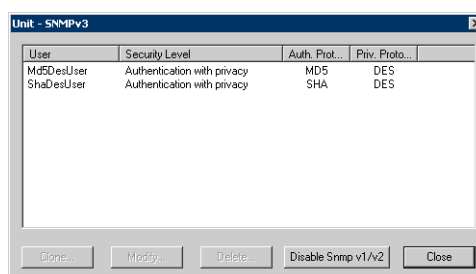


Note: These parameters are not available on digital Mediatrix units.

► **To set SNMPv3 information:**

1. Right-click the Mediatrix unit for which to set SNMPv3 information.
2. In the context sensitive menu that opens, select the *SNMPv3 Unit settings* option.
The following window opens.

Figure 115: SNMPv3 Users Window



This window lists all users currently created in the SNMP agent, including the user under which you have logged. These users are listed with their Authentication and Privacy information.

3. Disable SNMPv1 / SNMPv2 by clicking the *Disable Snmp v1/v2* button.
The Mediatrix unit will refuse any SNMPv1 or SNMPv2 request directed to it.
To re-enable SNMPv1 / SNMPv2, use the *Edit SNMP* window of the UMN to modify the permissions related to SNMPv1 / SNMPv2 (security model). These permissions are located in the *VacmAccessTable* of the SNMP-VIEW-BASED-ACM-MIB (RFC 2575).

Cloning a User

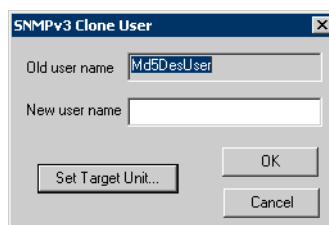
Cloning an existing user is the only way to create a new user in the SNMP agent. When cloning, all information of the original user, such as Authentication and Privacy information, is transferred to the clone.

► **To clone a user:**

1. Select a user and click the *Clone* button.

The following window opens:

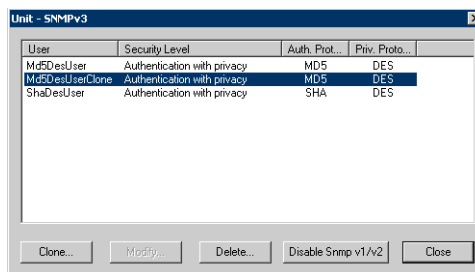
Figure 116: Clone User window



2. Type the new name of the user in the *New user name* field.
3. To apply changes to several Mediatrix units, click the *Set target units* button.
Follow the procedure described in [“Setting Multiple Units” on page 39](#).

- Click **OK**.
The new user is created.

Figure 117: New User Cloned



To modify information on this cloned user, connect to the remote unit or SNMPv3 agent with this user. See [“Working with SNMP” on page 161](#) for more details.



Note: If you clone a SNMPv3 user, and then remove its authentication or privacy, make sure that a row in *vacmGroupName* matches its new constraints (located in the *VacmAccessTable* of the SNMP-VIEW-BASED-ACM-MIB (RFC 2575)). If not, you cannot access the unit by using the new clone parameters.

Modifying a User

You can only modify the user under which you have logged. Furthermore, the rights granted to you by the SNMPv3 agent also dictate what information you can actually modify.

► To modify a user:

- Select the user under which you have logged.
The *Modify* button becomes available.
- Click the *Modify* button.
The following window opens.

Figure 118: SNMPv3 Security Window



Some settings cannot be modified.

- If applicable, modify the *Group name*.
The Group name specifies the SNMPv3 group in which the user is located.
- Select a Security level.

This is the SNMPv3 security level at which SNMP messages can be sent or processed, expressed in terms of whether or not authentication and/or privacy are provided. The available values are:

- No authentication or privacy
- Authentication without privacy
- Authentication with privacy

All options are mutually exclusive. To change the security level, choose the group corresponding to the security level selected (in the *Group name* field):

Table 85: Security Levels

For	Select
Authentication with privacy	The <i>AuthPrivGrp</i> group
Authentication without privacy	The <i>AuthNoPrivGrp</i> group
No authentication or privacy	The <i>NoAuthNoPrivGrp</i> group

You can only select options that are less secure. For instance, you cannot go from *Authentication without privacy* to *Authentication with privacy*. Furthermore, you cannot change the Authentication or Privacy protocol.

- If applicable, click the *Change Password* button of either the *Authentication* or *Privacy* section.



Note: SNMPv3 Passwords should not have repeating blocks of characters.

- Click OK to apply the changes.

The following window opens:

Figure 119: Set password window

The image shows a 'Set password' dialog box. It has three text input fields: 'Old password:', 'New password:', and 'Confirm new password:'. To the right of these fields are two buttons: 'OK' and 'Cancel'.

You can modify the password by supplying the old password and entering a new one.



Note: SNMPv3 Passwords should not have repeating blocks of characters.

- To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).

Deleting a User

You can delete an existing user.

► To delete a user:

- Select the user to delete.
- To apply changes to several Mediatrix units, click the *Set target units* button. Follow the procedure described in [“Setting Multiple Units” on page 39](#).
- Click the *Delete* button.
The selected user is removed from the list.

This chapter describes some of the problems you may experience with the UMN and how to solve them.

General Problems

DESCRIPTION: A unit I have previously autodetected is not available anymore.

POSSIBLE CAUSE: A unit must have a constant MAC address so that the UMN properly supports it. This may cause some issues with the Mediatrix 2102 residential application. If a Mediatrix 2102 enables its MAC address spoofing feature, the MAC address can thus change. For more information on the MAC address spoofing feature, please refer to the Mediatrix 2102 Administration manual.

SOLUTION: If the UMN detects a unit with MAC address XXXX and adds it to its collection, and then the unit changes its MAC address to YYYY, the UMN must detect the unit again. The unit with the new MAC address is then considered as a new unit. You must reconfigure all groups associations, SNMP preferences, friendly name, and UMN-based settings of this unit. If the unit goes back to the MAC address it used to have (and its entry in the UMN collection has not been deleted), it will retrieve its former identity.

Edit SNMP Window

Page Left Intentionally Blank

Edit SNMP Window

The *Edit SNMP* window can configure remote Mediatrix units that use the SNMPv1, SNMPv2c, or SNMPv3 protocol, no matter what the signalling protocol used. See “Chapter 17 - Working with SNMP” on page 161 for more details.

The *Edit SNMP* window allows to perform SNMP GET and SNMP SET operations on MIB variables. It contains features such as SNMP Table viewer and real-time graphical presentation of queried numerical values.

Using this window requires a knowledge of MIBs and SNMP. If you do not know SNMP, Media5 recommends that you familiarise yourself with it before attempting to modify the variables in the MIB.

Please note that:

- ▶ SNMP accesses via the *Edit SNMP* window are performed according to the preferences defined for each unit.
- ▶ The MIB file corresponding to the selected Mediatrix unit is automatically opened upon opening the *Edit SNMP* window.

Edit SNMP Window

The *Edit SNMP* window queries the Mediatrix unit's MIB structure to read or edit its parameters.

▶ **To open the *Edit SNMP* window:**

1. In the UMN's left pane, right click the Mediatrix unit to modify.
 2. Select the *Edit SNMP* option in the context sensitive menu that opens.
- The *Edit SNMP* window opens.

Figure 120: Edit SNMP Window

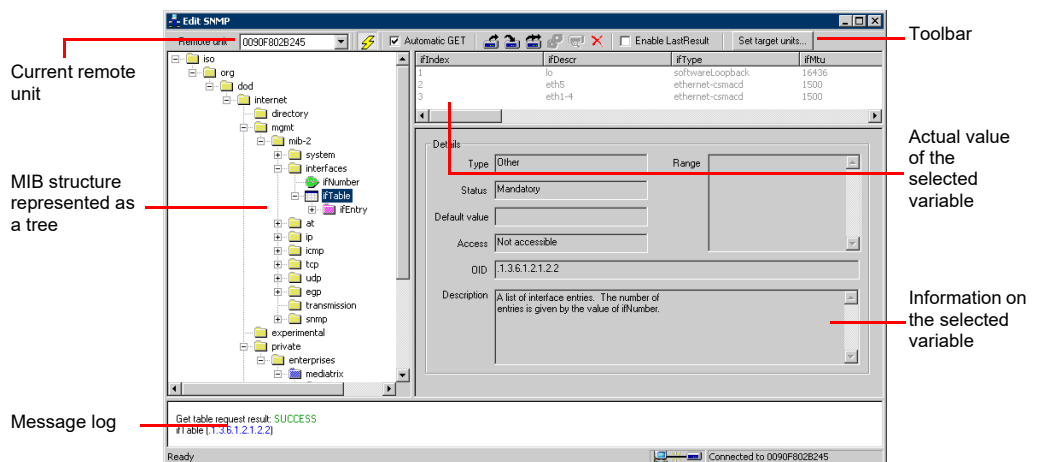


Table 86 describes each of these components.

Table 86: Edit SNMP Window Components

Component	Description
Current remote unit	MAC address of the unit to which the <i>Edit SNMP</i> window is currently connected.

Table 86: Edit SNMP Window Components (Continued)

Component	Description
MIB structure represented as a tree	Graphical representation of the opened MIB file. The MIB structure displayed in the <i>Edit SNMP</i> window differs depending on the unit selected. See “MIB File” on page 175 for more details.
Message log	Displays informative messages such as SNMP operation results, connection status, etc. See “Message Log” on page 181 for more details.
Toolbar	Tools you can use to manage the remote unit. See “Toolbar” on page 174 for more details.
Actual value of the selected variable	Clicking the  button displays the actual value of the selected variable.
Variable details	Details of the selected variable. • <i>Type</i>: string, integer, etc. • <i>Status</i>: Status of the variable (<i>Current</i>, <i>Deprecated</i>, <i>Obsolete</i>, etc.). • <i>Default value</i>: Value used by default. • <i>Access</i>: read, read-write, etc. • <i>OID</i>: Unique Object Identifier of the variable. • <i>Description</i>: Short description of the variable and its use. • <i>Range</i>: Range of values accepted. May also be <i>Index</i> or <i>Enum</i>, depending on the variable type. • <i>Index</i>: In tables, displays the column name(s) that makes up the table index. May also be <i>Range</i> or <i>Enum</i>, depending on the variable type. • <i>Enum</i>: List of choices available. May also be <i>Range</i> or <i>Index</i>, depending on the variable type.

Toolbar

The following tools help you manage remote units.

Table 87: Toolbar Icons

Tool	Description
	The <i>Edit SNMP</i> window is successfully connected to the selected remote unit.
	Performs a SNMP GET operation. See “Performing a GET Operation” on page 176 for more details.
	Performs a SNMP SET operation. See “Performing a SET Operation” on page 176 for more details.
	Performs a SNMP WALK operation. See “Performing a Walk Operation” on page 178 for more details.
	Clears the content of the message log. See “Message Log” on page 181 for more details.
☐ Enable LastResult	Allows to get the result of the last performed GET request. Available only on the Mediatrix 3300 Series units.
Set target units...	Applies settings to multiple units. See “Setting Multiple Units” on page 39 for more details.

MIB File

The MIB file contains the actual variables you can set for the selected remote unit. The MIB file corresponding to the selected Mediatrix unit is automatically opened upon opening the *Edit SNMP* window.

Refer to the *MIB Reference Manual* related to the unit you have selected for a description of the variables it supports.

MIB File Icons

The MIB information is represented by icons as described in Table 88.

Table 88: MIB Structure Icons

Icon	Description
	Group
	Module
	Variable – also called a leaf
	Table
	Table Entry
	Column in a table
	Index column in a table
	Trap

Mx Experimental MIBs

The UMN does not support MIBs that are located under the *mediatrixExperimental* branch of the MIB structure because it does not have specific tasks to manage variables in this branch.

The *mediatrixExperimental* branch is the area where objects and events in MIBs under development can be placed without fear of conflicting with other MIBs. When the items rooted under an experimental sub-tree are ready for release, they will be moved under a permanent branch.

Even though experimental MIBs can be viewed, SNMP operations may not work properly on them.

Refer to the *MIB Reference Manual* for more details.

MIB Cache

When opening a MIB file for the first time, it is stored in a cache. You can clear this cache and force the UMN to download the required MIB from the server, ensuring you have the proper MIB.

► **To clear the contents of the MIB cache:**

1. Exit the *Edit SNMP* window.
2. In the *Tools* menu of the Administrator window, select the *Clear MIB Cache* task.

Performing SNMP Operations

Once a remote unit has been successfully contacted and a proper MIB file opened, you can perform the following SNMP operations:

- ▶ GET
- ▶ SET
- ▶ WALK

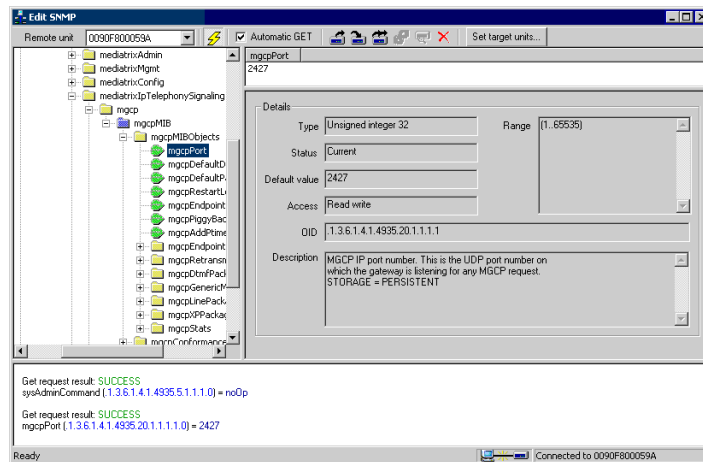
Performing a GET Operation

The GET operation allows you to poll the actual value of the selected variable.

▶ **To perform a GET operation:**

1. Select the variable to poll by expanding and collapsing tree branches as required with the [+] and [-] icons.
The variable details are displayed in the corresponding fields on the right. **Figure 121** illustrates a selected variable.

Figure 121: Selecting a Variable



2. Click the  tool to display the current value of the selected variable.
You can also:
 - right-click the variable and select the *Get* option in the context-sensitive menu that appears
 - select the *SNMP: Get* option in the menu bar

The value is displayed in the Actual value section as well as in the message log section.

Automatic GET

You can specify that the *Edit SNMP* window automatically GETs the value of a variable when browsing through the MIB by checking the *Automatic GET* option in the window. The *Edit SNMP* window automatically sends a GET request result in the message log and the variable's value is displayed in the Actual value section.

Performing a SET Operation

The SET operation allows you to modify the value of the selected variable.

► **To modify (SET) a variable value:**

1. Select the variable to modify by expanding and collapsing tree branches as required with the [+] and [-] icons.

The variable details are displayed in the corresponding fields on the right.

2. Click the  tool to display the current value of the selected variable.

The value is displayed in the Actual value section. If you have enabled the *Automatic GET* option, the value is displayed when selecting the variable.

3. Select the value in the Actual value section.

This value becomes highlighted.

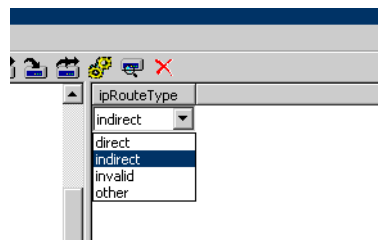
4. Modify the value for the variable, and then click the  tool.

You can also:

- right-click the variable and select the *Set* option in the context-sensitive menu that appears
- select the *SNMP Query:Set* option in the menu bar
- press the <Enter> key of your keyboard

If the value type is *Enum*, you can click twice on the variable at a one second interval and a drop-down menu with all the available values is displayed. Select the proper value.

Figure 122: Drop-Down Menu



Make sure that:

- The variable is not read-only
- The value you are setting falls within the range of accepted values

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 89: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.



Note: If you perform a set operation on a Mediatrix digital unit, a message asking you if you want to save the unit's configuration to the startup configuration displays when closing the *Edit SNMP* window. See [“Synchronizing vs Refreshing the List” on page 66](#) for more details.

Performing a Walk Operation

The Walk operation is usually performed on a node (group). It repeatedly queries the remote unit by using the GETNEXT operation.

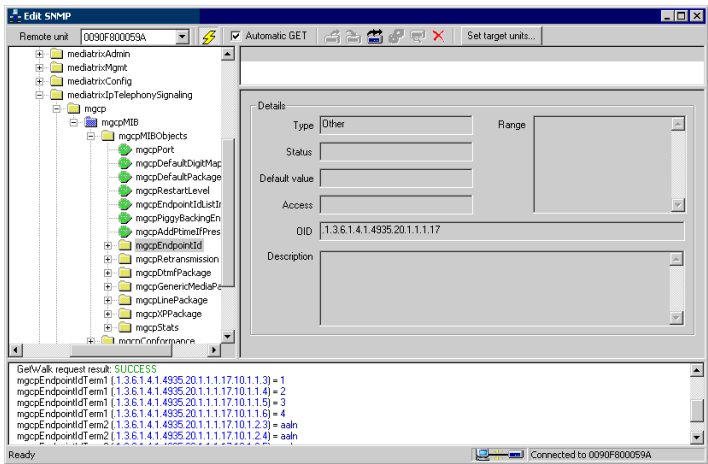
► **To perform a Walk operation:**

1. Select a node (group) for which to get the value of all sub-groups and variables.
Expand and collapse tree branches as required with the [+] and [-] icons to find the group to modify.

**Note:** Performing a Walk operation on one variable is the same as performing a GET operation on this variable.

2. Click the  button.
You can also:
 - right-click the node and select the *GetWalk* option in the context-sensitive menu that appears
 - select the *SNMP:GetWalk* option in the menu barThe value of all sub-groups and variables is listed in the message log.

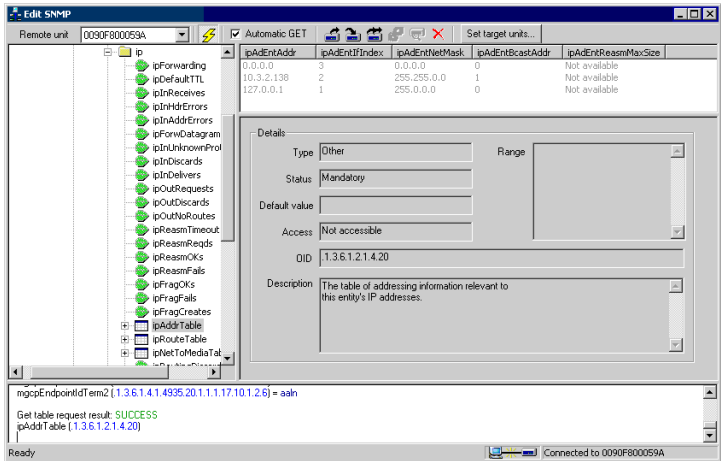
Figure 123: SNMP Walk Operation



SNMP Table Viewer

The *Edit SNMP* window has an integrated table viewer to display the tables of a MIB file. The following figure illustrates a table in a MIB file.

Figure 124: SNMP Table Viewer

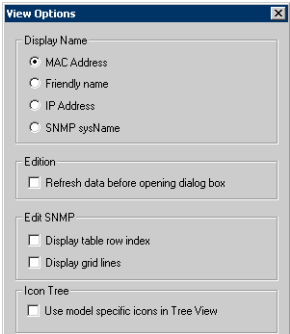


Options

The UMN offers you the possibility to show or hide the table row index and the table grid lines. You must exit the *Edit SNMP* window in order to change its settings.

- To change table viewing options:
 1. Exit the *Edit SNMP* window.
 2. In the *View* menu of the Administrator window, select the *Options* task.
The *View Options* window opens.

Figure 125: View Options Window



3. In the *Edit SNMP* section, select if you want to show/hide the table row index and grid lines by checking the proper choices.
4. Click *OK* to set the changes.

The changes will be displayed on screen the next time you open the *Edit SNMP* window, select a table and GET its values.

Figure 126: Table Viewing Options Examples

Options off

ifIndex	ifDescr	ifType
1	ETH860	ethernet-csmacd
2	LOOPBACK	softwareLoopback

Options on

	ifIndex	ifDescr	ifType
1	1	ETH860	ethernet-csmacd
2	2	LOOPBACK	softwareLoopback

Table row index

Table grid lines

Performing a GET Operation in a Table

You can perform a GET operation as described in [“Performing a GET Operation” on page 176](#). However, you can perform two types of GET operations:

- ▶ On the Table itself: all values of the table are displayed in the Actual value section.
- ▶ On a column of the Table: all values in this column are displayed in the Actual value section.

Performing a SET Operation in a Table

You can perform a SET operation as described in [“Performing a SET Operation” on page 176](#). This SET operation is performed on a value (cell) of the table.

Before making any change in a table, make sure the new value falls within the range of the variable.

You can modify more than one value before performing the actual SET operation.

You can apply a value in different ways by right-clicking the value and selecting a method in the context-sensitive menu that opens:

Table 90: Apply Value Methods

Method	Description
Apply value to all	Applies the value of the selected cell to all other cells in the same column.
Apply value to remaining	Applies the value of the selected cell to the cells located below the selected cell in the same column.
Apply row to all	Applies the values of the row with the selected cell to all other rows in the table.
Apply row to remaining	Applies the value of the row with the selected cell to the rows located below.

Forcing a SET

You can specify values in a table that you absolutely want to be set, even if they have not been modified. This is especially useful when using multiple target units to make sure all the desired values are set to all units, even if they do not need to be changed in the source unit.

To do so, right-click a value and select *Force set* in the context-sensitive menu that appears. You have the choice to force a set operation on:

- ▶ a single cell
- ▶ a column
- ▶ a row
- ▶ the entire table

Values with a force set state are displayed in red. They are set when performing the next SET operation.

Performing a Walk Operation in a Table

You can perform a WALK operation as described in [“Performing a Walk Operation” on page 178](#). However, you can perform two types of WALK operations:

- ▶ On the Table itself: all values of the table are displayed in the message log section.
- ▶ On a column of the Table: all values in this column are displayed in the message log section.

Miscellaneous Options

The following options are very useful when working with a MIB.

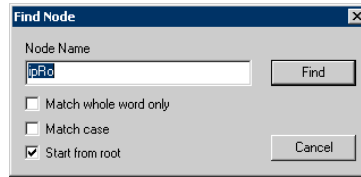
Using the Find Option

You can use the *Find* option to look for a variable name or a string of characters.

► To use the find option:

1. Right-click in the MIB tree where you want the search to start.
 2. Select *Find* in the context sensitive menu that appears.
- The following window opens:

Figure 127: Find Node Window



3. Type the variable name or character string to find in the *Node Name* field.
4. Select one or more of the following options:
 - Match whole word only
 - Match case
 - Start from root

Media5 recommends to always check the *Start from root* option, because the Find option only works in a descending way.
5. Click *Find* when ready.
6. If you want to find the next occurrence of the same string, right-click in the MIB tree where you want the search to start and select *Find Next* in the context sensitive menu that appears.

Expanding and Collapsing the MIB Tree

You can expand or collapse all of the MIB tree by right-clicking anywhere in the MIB structure and selecting either *Expand* or *Collapse* in the context sensitive menu that appears.

Message Log

The message log section displays informative messages that are generated when working with a remote unit or the opened MIB. These messages may include connection status, SNMP operation results, etc.

A successful SNMP operation result message has the following syntax:

```
Get/Set/GetWalk request result:SUCCESS
VariableName(OID)=value
```

For example:

```
Get request result: SUCCESS
sysUpTime (.1.3.6.1.2.1.1.3.0) = 7:17:35:27.00
```

You can clear the message log window by clicking the  button or selecting the *Log:Clear* option of the menu bar.

Appendices

Page Left Intentionally Blank



Managing Large Scale Deployment of Numerous Units

This [Appendix](#) describes methods you can use to manage numerous Mediatrix units at the same time.

Before Configuring

Media5 recommends to follow these steps before actually configuring Mediatrix units.

► **To prepare for unit configuration:**

1. Configure your DHCP server with the IP address of the UMN. Refer to the chapter “*Network Configuration*” in the Administration manual of one of your Mediatrix units for details.
2. Plug the Mediatrix units to configure into the network.
 - a. Connect the power cord to its corresponding connector.
 - b. Connect a 10/100 BaseT Ethernet RJ-45 cable into the Ethernet connector of the unit and connect the other end to a compatible Ethernet interface that supplies TCP/IP network access. Use a standard telecommunication cord with a minimum of 26 AWG wire size.
 - c. Connect the power cord to an electrical outlet. The electrical outlet must be installed near the unit so that it is easily accessible.

These units will be added automatically into the UMN collection. Refer to the chapter “*Installation*” in the Administration manual of one of your Mediatrix units for more installation details.

You can configure the units in two ways:

- Use the UMN’s GUI (dialog boxes and/or Edit SNMP).
- Use configuration files

Choice # 1: Use GUI (Dialog Boxes and/or Edit SNMP)

Choice #1 uses the GUI of the UMN to configure several units at the same time. See:

- “[Internal Editor](#)” on [page 21](#) for details on the GUI dialog boxes.
- “[Edit SNMP Window](#)” on [page 171](#) for details on MIB editing.

► **To use the UMN GUI:**

1. In the UMN, select one unit and configure the parameters you need. Click the *Set target units* button to select the units to configure with the same settings.

Most of the UMN windows allow you to apply settings to several units at the same time. See “[Setting Multiple Units](#)” on [page 39](#) for more details.

Choice # 2: Use Configuration Files

Choice #2 uses configuration files to manage Mediatrix units. These configuration files can be used in different ways.

The UMN accepts configuration files modified by users with a size between 0 and 512 KB. If the file size is null or over 512 KB, the UMN displays an error message in the *Status* section of the unit's *Overview* page.

When sending this file, the UMN converts it to XML format, which increases the file size. The unit that receives the configuration file may thus reject it, even if it is not over 512 KB when you edit it.

Before using a configuration file, you must first create one from an existing Mediatix unit.



Warning: You cannot change a SNMPv3 password via the configuration file because Mediatix units cannot interpret the OIDs of the standard MIBs (SNMP-USER-BASED-USM-MIB) from the configuration file. Furthermore, SNMP forbids to retrieve the existing password on the unit for security reasons, so the SNMPv3 password in the configuration file is always empty.

► **To create a configuration file:**

1. In the UMN, configure one unit with the GUI as described in [“Choice # 1: Use GUI \(Dialog Boxes and/or Edit SNMP\)” on page 185](#).
2. Right-click the unit you just configured.
3. In the context sensitive menu that opens, select the *Configuration File > Transfer from unit* option. This action generates a configuration file named *XXX.cfg* in the *Unit Manager Network 3.2\UnitManager\CfgFile* directory, where *XXX* represents the MAC address of the unit. See [“Uploading a Configuration File” on page 62](#) for more details.

You can use this generated configuration file in three ways:

- Modify the Existing Configuration File
- Create a New Configuration File
- Use the Default Configuration File as a Template

Modify the Existing Configuration File

Modifying the existing configuration file implies that you will be configuring the same unit.

► **To modify the existing configuration file:**

1. Open the generated configuration file in a text editor and modify the values you want.

For instance, you could take the following line:

```
APAIIII-PROVISIONNING-MIB::interfaceUseDhcp : .1.3.6.1.4.1.4935.1.1.1.4.1.10.4 :
.0 : 15="1"
```

and replace it by this line:

```
APAIIII-PROVISIONNING-MIB::interfaceUseDhcp : .1.3.6.1.4.1.4935.1.1.1.4.1.10.4 :
.0 : 15="0"
```



Caution: Do not change the actual OID or the Mediatix unit will not be able to read the configuration file.

2. In the UMN, right-click the unit corresponding to the configuration file you just modified.
3. In the context sensitive menu that opens, select the *Configuration File > Transfer to unit* option. See [“Downloading a Configuration File” on page 60](#) for more details.

Create a New Configuration File

Creating a new configuration file implies that you will be configuring other specific units.

► **To create a new configuration file:**

1. Create a new configuration file with the specific name *XXX.cfg*, where *XXX* represents the MAC address of another unit.
2. Using a text editor, copy the content of the generated configuration file into this new file.

Do not copy the unit's IP address information; this will avoid to have two units with the same IP address.

3. In the UMN, right-click the unit corresponding to the configuration file you just created.
4. In the context sensitive menu that opens, select the *Configuration File > Transfer to unit* option. See ["Downloading a Configuration File" on page 60](#) for more details.

Use the Default Configuration File as a Template

The default configuration file is used when the unit has no specific configuration file. It is used to get a new default configuration for units of the same type.

To use this default file, delete or rename the specific configuration files *XXX.cfg* in the *Unit Manager Network 3.2\UnitManager\CfgFile* directory.

► To use the default configuration file as a template:

1. Use the default configuration file that corresponds to your product.
The default configuration files are located in the *Unit Manager Network 3.2\UnitManager\DefaultCfgFile* directory. Each configuration file is named as follows:
`DefaultConfigFile_[SoftwareVersion]_[ProductNumber][ProductType].cfg`
For instance, the default configuration file for a Mediatix 1104 unit version 4.3.x is:
`DefaultConfigFile_43_404FXS.cfg`
2. Copy the content of the generated configuration file into this file.
Do not copy the unit's IP address information; this will avoid to have two units with the same IP address.
When performing a download action on a group of units, all Mediatix 1104 v4.3.x units that do not have a specific configuration file will receive this configuration file. After this action, the UMN will create a specific configuration file for all those units from the default configuration file.

Unit Collection Methods

This [Appendix](#) describes the two methods you can use to connect a Mediatrix unit with the UMN (referred to as management server in the MIB documentation). These methods work for SIP v2.x units, SIP/MGCP v4.x/v5.x units, and Dgw v1.1/2.0 units that are on your administrative domain.

Introduction

There are two methods to connect a Mediatrix unit with the UMN:

- ▶ Automatically by contacting the UMN (see [“Automatic Collection Method \(MIB\)” on page 192](#))
You can instruct the Mediatrix unit to look for a specific UMN and connect to it. To use this automated process, you shall properly set some parameters in the MIB structure of the Mediatrix unit. These MIB parameters differ depending on the unit version. See [“MIB Parameters to Set” on page 189](#) for more details.
For more information on the MIB variables, refer to your Mediatrix unit *Administration Manual* and the *MIB Reference Manual*.
- ▶ Manually with the UMN (see [“Manual Collection Method \(Autodetect\)” on page 195](#))
The UMN is used to detect Mediatrix units on the network.

MIB Parameters to Set

The MIB parameters differ depending on the version of units present on your domain.

MIB Parameters for SIP v2.x Units

[Table 91](#) lists the MIB parameters to modify in the Provisioning MIB for SIP v2.x units.

Table 91: MIB Variables in Mediatrix SIP v2.x Unit Connection

Variable	Description
apaManagerEnable	Instructs the Mediatrix unit to look for a specific UMN and connect to it. Once the variable is set, restart the unit to make the change effective. 0 = Disable 1 = Enable Default Value: 1
apaCmdRequest Configuration	Defines how the Mediatrix unit requests its configuration. 0 = Do not need to transfer the Configuration File 1 = Request the Configuration File through TFTP Default Value: 1

Table 91: MIB Variables in Mediatrix SIP v2.x Unit Connection (Continued)

Variable	Description
apaCmdConfiguration Mode	Select the Mediatrix unit configuration mode. -1 = Request and wait for the Configuration File. A Configuration File Trap Info is sent to the UMN to request a configuration file upload. The value is set back to 0 after the file is received. NOTE: Set the mode to 1 to apply new settings. 0 = Record changes (TFTP or SNMP) - Changes are recorded but will not be applied until the mode is set back to Commit. 1 = Commit all changes - Changes are automatically applied. NOTE: Some changes may require to restart the unit to take effect. 2 = Undo all recorded changes - All changes recorded will be dismissed. The mode is set back to 1 afterward. Default Value: -1
apaManagerTrap RetransmissionRetry Count	Number of times the Mediatrix unit sends a trap request to the UMN in case it does not answer within the specified period of time. If the UMN still does not answer after the defined number of retries, the unit continues its initialization process. -1 = infinite - always retransmit Default Value: 10
apaManagerTrap RetransmissionPeriod	When a trap request is sent to the UMN, it shall answer back within a specified period of time. This is the Retransmission Period. If no answer is received within this period, the Mediatrix unit will retry to send the SNMP request to the UMN. If the UMN still does not answer after the defined number of retries, the unit continues its initialization process.
apaManagerDhcpPrim Host (read-only)	UMN IP address or domain name provided by the DHCP server. Default Value: 192.168.0.10
apaManagerStaticPrim Host	Static UMN IP address or domain name. Default Value: 192.168.0.10

MIB Parameters for SIP/MGCP v4.x/5.x Units

Table 92 lists the MIB parameters to modify in the MIB structure for SIP/MGCP v4.x/v5.x units.

Table 92: MIB Variables in Mediatrix SIP/MGCP v4.x/v5.x Unit Connection

Variable	Description
msEnable	Enables the management server. - disable(0) - enable(1) Default Value: enable
msSelectConfigSource	Indicates the source to be used for the provisioning of the management server MIB objects. Default Value: dhcp
msTrapRetransmission Period	TRAP retransmission period in ms. Default Value: 60000

Table 92: MIB Variables in Mediatrix SIP/MGCP v4.x/v5.x Unit Connection (Continued)

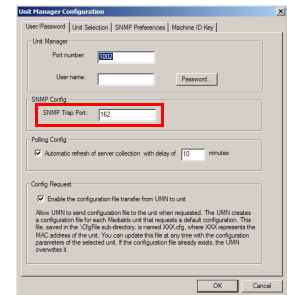
Variable	Description
msTrapRetransmission RetryCount	TRAP retransmission retry count. -1 = infinite (always retransmit) Default Value: 10
sysAdminDownloadConfig FileStatus (read-only)	Indicates the status of the last configuration file download. - idle(0) - fail(1) - success(2) - inProgress(3) - listening(4) Default Value: idle
msConfigSource (read-only)	Indicates the source used for the provisioning of the management server MIB objects. Default Value: dhcp
msHost (read-only)	Management server IP address or domain name. Default Value: 192.168.0.10
msTrapPort (read-only)	Management server IP port number. Default Value: 162

MIB Parameters for Dgw v1.1/2.0 Units

Table 92 lists the MIB parameters to modify in the MIB structure for Dgw v1.1/v2.x units.

Table 93: MIB Variables in Mediatrix Dgw v1.1/2.0 Unit Connection

Variable	Description
Snmp.trapDest	Address/port where to send traps. You must enter the address of the UMN server. The port must be the one defined in the <i>Unit Manager Configuration</i> window, <i>User/Password</i> tab, <i>SNMP Trap Port</i> parameter. See “User / Password Information” on page 9 for more details. Default Value: 192.168.10.10:162
Snmp.enableTrap	Specifies if traps can be sent. The Linkup trap is specifically used to detect the Mediatrix unit. Default Value: enable



Furthermore, if SNMPv3 is used the SNMP preferences of the unit and UMN must be the same (“[Global SNMP Preferences](#)” on page 11). Be sure to select the **Unit Dgw** type of units.

Automatic Collection Method (MIB)

A Mediatrix unit can be set to automatically connect to the UMN when it powers up.

Collection Method for SIP v2.x Units

When proceeding with the automatic collection method with SIP v2.x units, make sure that:

- ▶ the *apaManagerEnable* variable is set to **1** (Enable)
- ▶ the IP address and port number of the UMN are properly entered in the MIB file of the Mediatrix unit (*apaManagerStaticPrimHost* variable)

Once this configuration is done, the Mediatrix unit generates a SNMP trap to the UMN and communicates the value of the *apaCmdRequestConfiguration* variable. If this variable is set to:

- ▶ **0**, the unit does not ask for the default configuration
- ▶ **1**, the unit wants to receive a default configuration file via TFTP

The *apaCmdConfigurationMode* variable starts the traps process of the Mediatrix unit if its value is set to **-1**.

Each time the Mediatrix unit starts, it sends a SNMP trap to the UMN. If the unit does not receive an answer after a period of time (in ms) defined in the *apaManagerTrapRetransmissionPeriod* variable, it re-sends the same trap. The maximum number of times the unit repeats this operation is defined in the *apaManagerTrapRetransmissionRetryCount* variable. If the maximum number of retries is reached, the Mediatrix unit sets the *apaCmdConfigurationMode* variable to **0** and continues its initialisation process.

If the value of the *apaManagerTrapRetransmissionRetryCount* variable is set to **-1**, the Mediatrix unit re-sends the same trap indefinitely.

▶ Initialization sequence of the Mediatrix unit by using the DHCP:

1. The Mediatrix unit gets its IP address and the address of the UMN via DHCP.
 2. The Mediatrix unit sends a SNMP trap (700) to the UMN by setting the *apaCmdRequestConfiguration* value to **1**.
 3. The UMN sets the *apaCmdConfiguration Mode* variable to **0**.
 4. The Mediatrix unit sends a SNMP trap (800) confirming that the *apaCmdConfigurationMode* value is **0**.
 5. The UMN sends the configuration file associated with the Mediatrix unit via TFTP (*\CfgFile\XXX.cfg*).
This file is created if no other file is already associated to this Mediatrix unit. It is created from the default configuration file (*\DefaultCfgFile\DefaultConfigApaYYY.cfg*), where *YYY* corresponds to the type of unit.
 6. The Mediatrix unit sends a SNMP trap (900) that confirms the file transfer status (SUCCESS or FAIL). If FAIL, another file transfer is started.
 7. The UMN sets the *apaCmdConfiguration Mode* variable to **1** and *apaCmdRequestConfiguration* variable to **0**.
 8. The Mediatrix unit sends a SNMP trap (800) that confirms the value of the *apaCmdConfigurationMode* variable to **1**.
 9. The UMN finishes the configuration.
- The following diagram illustrates the DHCP initialization sequence.

Figure 128: DHCP Initialization Sequence

Collection Method for SIP/MGCP v4.x/v5.x Units

When proceeding with the automatic collection method with SIP/MGCP v4.x/v5.x units, make sure that:

- ▶ the *msEnable* variable is set to **Enable**
- ▶ the IP address and port number of the UMN are properly entered in the MIB file of the Mediatrix unit

This information may be entered in two ways:

- via DHCP: set the DHCP server with the IP address and port number of the computer hosting the UMN. The information sent by the DHCP server can be viewed in the *msHost* and *msPort* read-only variables. How to set the DHCP server is not the scope of this document. See the Mediatrix unit *Administration Manual* for more information.
- manually (static): set the *msStaticHost* and *msStaticPort* variables with the IP address and port number of the computer hosting the UMN.

Once this configuration is done, the Mediatrix unit generates a SNMP trap to the UMN and communicates the value of the *sysConfigDownloadConfigFile* variable. If this variable is set to:

- ▶ **noFileDownload**, the unit does not ask for the default configuration
- ▶ **fileDownload**, the unit wants to receive a default configuration file via TFTP

The *sysConfigDownloadConfigMode* variable starts the traps process of the Mediatrix unit if its value is set to **request**.

Each time the Mediatrix unit starts, it sends a SNMP trap to the UMN. If the unit does not receive an answer after a period of time (in ms) defined in the *msTrapRetransmissionPeriod* variable, it re-sends the same trap. The maximum number of times the unit repeats this operation is defined in the *msTrapRetransmissionRetryCount* variable. If the maximum number of retries is reached, the Mediatrix unit sets the *sysConfigDownloadConfigMode* variable to **record** and continues its initialisation process.

If the value of the *msTrapRetransmissionRetryCount* variable is set to **-1**, the Mediatrix unit re-sends the same trap indefinitely.

▶ Initialization sequence of the Mediatrix unit by using the DHCP:

1. The Mediatrix unit gets its IP address and the address of the UMN via DHCP.
2. The Mediatrix unit sends a SNMP trap (700) to the UMN by setting the *sysConfigDownloadConfigFile* value to **fileDownload**.
3. The UMN sets the *sysConfigDownloadConfigMode* variable to **record**.

4. The Mediatrix unit sends a SNMP trap (800) confirming that the *sysConfigDownloadConfigMode* value is **record**.
 5. The UMN sends the configuration file associated with the Mediatrix unit via TFTP (*\CfgFile\XXX.cfg*).
This file is created if no other file is already associated to this Mediatrix unit. It is created from the default configuration file (*\DefaultCfgFile\DefaultConfigApaYYY.cfg*), where *YYY* corresponds to the type of unit.
 6. The Mediatrix unit sends a SNMP trap (900) that confirms the file transfer status (SUCCESS or FAIL). If FAIL, another file transfer is started.
 7. The UMN sets the *sysConfigDownload ConfigMode* variable to **commit** and *sysConfigDownload ConfigFile* variable to **noFileDownload**.
 8. The Mediatrix unit sends a SNMP trap (800) that confirms the value of the *sysConfigDownloadConfigMode* variable to **commit**.
 9. The UMN finishes the configuration.
- The following diagram illustrates the DHCP initialization sequence.

Figure 129: DHCP Initialization Sequence



Collection Method for Dgw v1.1/v2.0 Units

When proceeding with the automatic collection method with Dgw v1.1/v2.0 units, make sure that the IP address and port number of the UMN are properly entered in the MIB file of the Mediatrix unit.

Each time the Mediatrix unit starts, it sends a SNMP Linkup trap to the UMN.

Manual Collection Method (Autodetect)

The manual collection method implies that you use the UMN to locate Mediatrix units. Those units are detected according to the unit versions selected in the *Unit Manager Configuration* window. See [“Units Selection” on page 10](#) for more details.

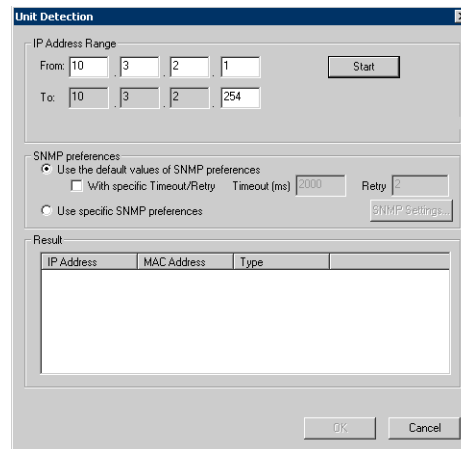
► Initialization sequence of the Mediatrix unit by using the Autodetect:

1. Click the  icon in the UMN tool bar.

You can also right-click the *Unit Manager* level and select the *AutoDetect* option in the context sensitive menu that opens.

The *Unit Detection* window opens:

Figure 130: Unit Detection Window

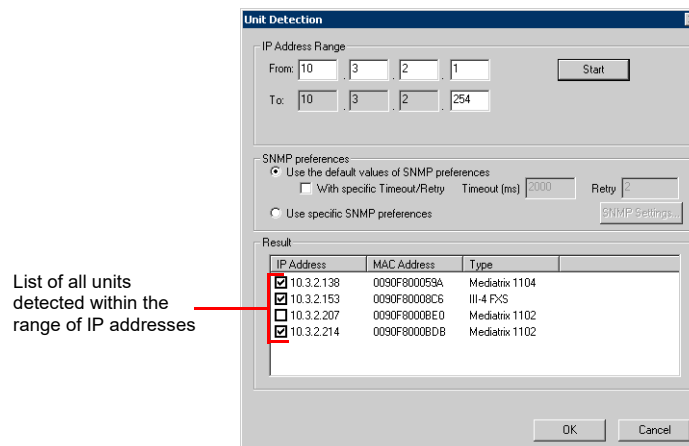


2. Set the range of IP addresses within which to detect units.

3. Click the *Start* button.

The UMN goes through all IP addresses within the specified range and lists the Mediatrix units detected in the *Result* section.

Figure 131: Results of Autodetect



Units with a check mark were not present in the previous autodetect process. You can check/uncheck units as you want.

4. Click *OK* to add units with a check mark.

The list of Mediatrix units in the UMN is automatically refreshed.

5. In the *Administration* window of the selected Mediatrix unit, configure the UMN by selecting the *Enable* option and specifying its IP address (see [“Unit Manager Server” on page 72](#) for more details).
6. Download a configuration file into a selected Mediatrix unit by right-clicking it and selecting the *Configuration File > Transfer to unit* option in the menu that opens.

See [“Downloading a Configuration File” on page 60](#) for more details.

For SIP v2.x and SIP/MGCP v4.x/5.x units: Once the initial configuration of the Mediatrix unit is started, the unit sends a SNMP trap at each restart by specifying that it does not need configuration (*sysConfigDownloadConfigFile* = noFileDownload). This allows the UMN to update the Mediatrix unit IP address.

Using a Configuration File

Each type of Mediatrix unit has a default configuration file. These files are saved in the `\DefaultCfgFile` directory.



Caution: Do not change the file names. However, you can modify their contents to define specific configurations for each type of Mediatrix unit according to your needs.

This configuration file shall only contain variables that have read/write access, that is with a Max Access of *read-write*.

The UMN creates a configuration file for each Mediatrix unit that requests a default configuration. This file, saved in the `\CfgFile` directory, is named `XXX.cfg`, where `XXX` represents the MAC address of the unit. You can update the configuration file of a unit by right-clicking it and selecting the *Configuration File > Transfer to unit* option. See ["Uploading a Configuration File" on page 62](#) for more details.

In the default configuration file, each data line is structured as follows:

```
Name of the MIB module:Version of the MIB module:Label of the
variable:PrefixOid:SuffixOid:Type of the variable="value"
```

For example:

```
APAIIII-SIP-PROV-MIB::interfaceQoSsignalingDSFieldValue :
.1.3.6.1.4.1.4935.1.1.1.1.1.1.1.3.1 : .0 : 3="186"
```

Table 94: Configuration File Format

Field	Description
Name of the MIB module	Official name of the module
Version of the MIB module	Can be empty.
Label of the variable	Name of the variable in the MIB structure.
SuffixOid	.0 for simple variables .x for instances of a table (x represents the index)
PrefixOid	- oid of the variable for simple variables - oid of the column for instances in a table



Note: To avoid making syntax errors in the file, Media5 suggests to upload the file first, and then modify it.

Traplog.txt File

The UMN saves all the SNMP traps sent by the Mediatrix units in the *Traplog.txt* file located in the `\TrapLog` directory. The size of the file is limited to 2 Mb. Once this limit is reached, the UMN renames this file and creates a new *Traplog.txt* file.

Data in the *Traplog.txt* file is structured as follows:

```
<MAC Address><IP Address><Type of trap><Specific Trap><Up Time><Version SNMP> --
><Time and date of trap arrival>
```

In this file, each line of data represents a SNMP trap according to the format defined above.

Example:

```
0090F8000522 192.168.0.11 6 800 2113642 v1 --> 9:12:19-2/11/2000
```

For SIP v2.x and SIP/MGCP v4.x/5.x units: The specific traps that could be found in this file are:

- ▶ 700: SNMP trap generated by the Mediatrix unit each time it restarts or each time you modify the following MIB variable:

- For SIP v2.x units, the *apaCmdConfigurationMode* variable to **-1**.
 - For SIP/MGCP v4.x/v5.x units, the *sysConfigDownloadConfig Mode* variable to **record**.
- ▶ 800: SNMP trap that confirms the actual configuration mode of the Mediatrix unit.
 - ▶ 900: SNMP trap that sends the status (SUCCESS or FAILED) of the configuration file transfer via TFTP.

For Dgw v1.1/2.0 units: Only the Linkup trap is used. The Linkup trap is specifically used to detect the Mediatrix unit.

**10 BaseT**

An Ethernet local area network which works on twisted pair wiring.

100 BaseT

A newer version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet.

A-Law

A-Law is the ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (μ)-law standard. See also *Mu (μ)-Law*.

Area Code (AC)

The preliminary digits a user must dial to be connected to a particular outgoing trunk group or line. In North America, an area code has three digits and is used with a NXX (office code) number. For example, in the North American telephone number 561-955-1212, the numbers are defined as follows:

Table 95: North American Numbering Plan

No.	Description
561	Area code, corresponding to a geographical zone in a non-LNP (Local Number Portability) network.
955	NXX (office code), which corresponds to a specific area such as a city region.
1212	Unique number to reach a specific destination.

Outside North America, the area code may have any number of digits, depending on the national telecommunication regulation of the country. In France, for instance, the numbering terminology is defined as xZABPQ 12 34:

Table 96: France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can have four digits.
Z	Geographical (regional) zone of the number (in France, there are five zones). It has two digits.
ABPQ	First four digits corresponding to a local zone defined by central offices.
12 34	Unique number to reach a specific destination.

In this context, the area code corresponds to the Z portion of the numbering plan. Since virtually every country has a different dialing plan nomenclature, it is recommended to identify the equivalent of an area code for the location of your unit.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Call Agent (Connection Manager)

The Call Agent manages the connection state of the Mediatrix unit. The Call Agent provides Basic Call Processing and MGCP/NCS Gateway Support.

Comma-Separated Values (CSV)

A CSV (comma-separated values) file contains the values in a table as a series of ASCII text lines organized so that each column value is separated by a comma from the next column's value and each row starts a new line. A CSV file is a way to collect data from any table so that it can be conveyed as input to another table-oriented application such as a spreadsheet application. A CSV file is sometimes referred to as a flat file.

Country Code (CC)

In international direct telephone dialing, a country code is a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

Data Encryption Standard (DES)

DES (Data Encryption Standard) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Domain Name Server (DNS)

A DNS (Domain Name Server) is an internet service that translates domain names into IP addresses. For example, the domain name *www.example.com* might translate to 198.105.232.4.

Dual-Tone Multi-Frequency (DTMF)

In telephone systems, DTMF is multi-frequency signalling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol “#” or “*”, the “*” being reserved for special purposes.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

E.164 Alias

E.164 is a standard that defines normal telephone numbers. They may contain digits from 0-9, * and #. H.323 differentiates between these numbers and “H.323 addresses”, which may contain alphanumeric characters.

Encryption

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Foreign Exchange Office (FXO)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area's central office. This is the office end of an FX circuit (frequently a PBX).

Foreign Exchange Service/Station (FXS)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area's central office. This is the station (telephone) end of an FX circuit. An FXS port will provide dial tone and ring voltage.

G.711

G.711 is an ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48, 56, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.723.1

G.723 is a codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.

G.729/G.729A

G.729 is a codec that provides near toll quality at a low delay which uses compression of 8 kbps (8:1 compression rate).

Gatekeeper

A gatekeeper identifies, controls, counts, and supervises the traffic or flow through the network. It also provides functions such as terminal and gateway registration, address resolution, bandwidth control, and admission control.

Gateway

A gateway is a device that links two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

H.323

H.323 is an umbrella standard for audio/video conferencing over unreliable networks; architecture and procedures are covered by this standard; H.323 relies on H.225 and H.245.

Internet Protocol (IP)

The IP protocol is a standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognises incoming messages.

Jitter

Jitter is a distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.

Latency

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another.

Local Area Network (LAN)

A LAN is a data-only communications network confined to a limited geographic area, with moderate to high data rates. See also WAN.

Management Information Base (MIB)

A MIB (Management Information Base) is a structured collection of all the managed objects maintained by a device. The managed objects are structured in the form of a hierarchical tree. At the top of the tree is the most general information available about a network. Each branch of the tree then gets more detailed into a specific network area, with the leaves of the tree as specific as the MIB can get.

MD5

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is intended for use with digital signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321.

Media Access Control (MAC) Address

A MAC address is a layer 2 address, 6 bytes long, associated with a particular network device. It is used to identify devices in a network. It is also called hardware or physical address.

Media Gateway Control Protocol (MGCP)

MGCP is an application programming interface and a protocol for controlling Voice over IP (VoIP) Gateways from external call control elements, where the intelligence is.

Mu (μ)-Law

Mu (μ)-Law is the PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also *A-Law*.

Network

A network is a group of computers, terminals, and other devices, as well as the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

Network-based Call Signalling (NCS)

NCS is a profile of the Media Gateway Control Protocol (MGCP). The scope of NCS is currently only embedded Voice-Over-IP client devices.

Object Identifier (OID)

Object Identifiers (OID) are strings of numbers. They are allocated in a hierarchical manner, so that, for instance, the authority for "1.2.3" is the only one that can say what "1.2.3.4" means. They are used in a variety of protocols. The formal definition of OIDs comes from ITU-T recommendation X.208 (ASN.1), which is available from the ITU.

Packet

A packet includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection.

Port

A port is a network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

Private Branch Exchange (PBX)

A PBX is a small- to medium-sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Protocol

A protocol is a formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. It is a set of conventions dealing with transmissions between two systems. It typically defines how to implement a group of services in one or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between application programs.

Proxy Server

A proxy server is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.

Public Switched Telephone Network (PSTN)

The PSTN is the local telephone company network that carries voice data over analog telephone lines.

Quality of Service (QoS)

Quality of Service is a measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).

Registrar Server

A registrar server is a server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.

Router

A router is a specialized switching device which allows customers to link different geographically dispersed local area networks and computer systems. This is achieved even though it encompasses different types of traffic under different protocols, creating a single, more efficient, enterprise-wide network.

Running Configuration

In digital Mediatrix units, the currently running configuration (running-config) for the firmware, which is executed from the volatile memory (*system:*) on the Mediatrix unit.

Server

A server is a computer or device on a network that works in conjunction with a client to perform some operation.

Session Initiation Protocol (SIP)

SIP is a protocol for transporting call setup, routing, authentication, and other feature messages to endpoints within the IP domain, whether those messages originate from outside the IP cloud over PSTN resources or within the cloud.

Simple Network Management Protocol (SNMP)

SNMP is the protocol governing network management and the monitoring of network devices and their functions.

Startup Configuration

In digital Mediatrix units, the startup configuration is stored in the persistent memory (*nvr:*) and is always copied for execution to the running configuration in the volatile memory (*system:*) after a system start-up.

Structure of Management Information (SMI)

The SMI is the set of rules for specifying the management information that a device maintains. To be more precise, the management information is actually a collection of managed objects, and these rules are used to both name and define these managed objects. The SMI is used in v4.x/v5.x Mediatrix units only.

Subnet

A subnet is a means of splitting packets into two fields to separate packets for local destinations from packets for remote destinations in TCP/IP networks. This makes small networks more efficient.

Switched Circuit Network (SCN)

A SCN is a communication network, such as the public switched telephone network (PSTN), in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.

T.38

T.38 is an ITU-T Recommendation for Real-time fax over IP. T.38 addresses IP fax transmissions for IP-enabled fax devices and fax gateways, defining the translation of T.30 fax signals and Internet Fax Protocols (IFP) packets.

Telephony

Telephony is the science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

Terminal

A terminal is a device capable of sending or receiving data over a data communications channel.

Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

Trivial File Transfer Protocol (TFTP)

TFTP is a simplified version of FTP that transfers files but does not provide password protection, provide directory capability, or allow transmission of multiple files with one command.

User Datagram Protocol (UDP)

UDP is an efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

Voice Over IP (VoIP)

VoIP is the technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Wide Area Network (WAN)

A WAN is a large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

List of Acronyms

A	
AC	Area Code
C	
CC	Country Code
D	
dB	Decibel
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DTMF	Dual-Tone Multi Frequency
F	
FQDN	Fully Qualified Domain Name
FXO	Foreign eXchange Office
FXS	Foreign eXchange Service
G	
GUI	Graphical User Interface
I	
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
K	
kbps	Kilobits Per Second
L	
LAN	Local Area Network
LNP	Local Number Portability
M	
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
N	
NCS	Network-based Call Signalling
P	
PBX	Private Branch eXchange
PCM	Pulse Code Modulation
PSTN	Public Switched Telephone Network
R	
RFC	Request for Comment
RSIP	Restart In Progress
S	
SCN	Switched Circuit Network
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
STUN	Simple Traversal of User Datagram Protocol (UDP) through Network Address Translation (NAT)
T	
TFTP	Trivial File Transfer Protocol

U	
UDP	User Datagram Protocol
V	
VoIP	Voice Over IP
W	
WAN	Wide Area Network

Index

Numerics

- 10 BaseT [185](#)
 - defined [199](#)
- 100 BaseT [185](#)
 - defined [199](#)

A

- acronyms [205](#)
- Administration parameters
 - default gateway [76](#)
 - DNS [77](#)
 - host [75](#)
 - IP Configuration
 - default router [70](#)
 - local IP address [70](#)
 - primary DNS [70](#)
 - secondary DNS [71](#)
 - subnet mask [70](#)
 - SNTP [73](#), [75](#)
 - Software and Emergency Download [71](#)
 - Syslog daemon [72](#)
 - Unit Manager Server [72](#)
 - uplink (WAN) [74](#)
- Administrator module [18](#)
 - connection on startup behaviour [17](#)
 - defining [16](#)
 - opening [16](#)
- aliases
 - in H.323 [98](#)
- allowed numbers, gateway permission [87](#)
- analog units [24](#)
- area code, setting [107](#)
- authentication
 - configuration file download [122](#)
 - in SIP [108](#)
 - in SNMPv3 [14](#), [165](#)
 - software download [130](#)
- Autodetect, toolbar icon [23](#)
- automatic
 - configuration update [124](#)
 - software update [132](#)
- automatic call, telephony attribute [157](#)

C

- call
 - automatic [157](#)
 - conference [147](#)
 - direction of [156](#)
 - forward
 - on busy [149](#)
 - on no answer [151](#)
 - unconditional [147](#)
 - hold [145](#)
 - local
 - in a different AC [88](#), [89](#)
 - in the same AC [88](#), [89](#)
 - long distance
 - in a different AC [88](#), [89](#)

- in a different Country Code (CC) [88, 90](#)
 - in the same AC [88, 89](#)
- second [146](#)
- transfer
 - attended [146](#)
 - blind [146](#)
- waiting [145](#)
- call agent
 - MGCP [101](#)
 - NCS [104](#)
- codec activation parameters [94](#)
- conference call, settings [147](#)
- configuration file
 - analog units
 - default [187](#)
 - downloading [60, 186](#)
 - modifying [186](#)
 - uploading [62, 185](#)
 - automatic update [124](#)
 - digital units
 - downloading [61](#)
 - uploading startup [62](#)
 - download server [122](#)
 - configuration source [122](#)
 - HTTP server, configuring [119](#)
 - SNTP server, configuring [119](#)
 - TFTP server, configuring [119](#)
 - download, setting [122, 123](#)
 - enabling transfer from the UMN to the unit [10](#)
 - encryption
 - decrypting generic [126](#)
 - decrypting specific [126](#)
 - defined [126](#)
 - saving to Dgw config script [65](#)
 - saving to XML format [64](#)
 - transfer protocol [122](#)
- Connect, toolbar icon [23](#)
- connection on startup behaviour [17](#)
- CorNet-IP
 - E.164 alias [110](#)
 - emergency number [111](#)
 - location identification number [111](#)
 - subscriber number [110](#)
- country code (CC) [88, 107](#)

D

- default gateway parameters, setting [76](#)
- default router, setting [70](#)
- deleting
 - filter [55](#)
 - hierarchy [50](#)
 - instance in the tree list [48](#)
 - instances in group [44](#)
 - SNMP user [168](#)
 - units from the list [31](#)
 - virtual group [46](#)
- DES, privacy protocol [14, 162, 165](#)
 - defined [200](#)
- DHCP
 - removing all options [67](#)
- dial map
 - # and * characters [83](#)
 - allowed [80](#)
 - combining two expressions [83](#)
 - defined [82](#)

- refused [80](#)
 - setting [81](#)
 - special characters [82](#)
 - timer [83](#)
 - using [83](#)
 - validating [84](#)
- Dial Map parameters
 - dial map [81](#)
 - number of prefixed digits to remove [81](#)
 - prefix digits [81](#)
 - rules [81](#)
 - suffix to remove [81](#)
- dial prefix, gateway permission [87](#)
- digital units [25](#)
- direct gateway call, in H.323 [99](#)
- DNS
 - parameters, setting [77](#)
 - primary [70](#)
 - secondary [71](#)
- downloading
 - configuration file
 - analog units [60](#), [186](#)
 - digital units, startup [61](#)
 - software version
 - analog units, SIP v2.x [57](#)
 - analog units, SIP/MGCP v4.x/v5.x [57](#)
 - digital units [58](#)
- downloading software
 - automatic update [132](#)
 - firmware packs configuration [136](#)
 - HTTP server, configuring [127](#)
 - server path [130](#)
 - SNTP server, configuring [127](#)
 - TFTP server, configuring [127](#)
 - transfer configuration [135](#)
 - zip file [127](#)

E

- E.164 alias
 - defined [200](#)
 - setting [110](#)
- Edit SNMP window
 - collapsing the MIB tree [181](#)
 - expanding the MIB tree [181](#)
 - find, option [180](#)
 - GET operation [176](#), [180](#)
 - automatic [176](#)
 - interface
 - actual variable value [174](#)
 - message log [174](#)
 - MIB structure [174](#)
 - toolbar [174](#)
 - variable details [174](#)
 - message log [181](#)
 - MIB icons [175](#)
 - opening a MIB file [175](#)
 - SET operation [176](#), [180](#)
 - force SET [180](#)
 - table viewer [178](#)
 - options [179](#)
 - toolbar icons
 - Clear Log [174](#)
 - Connected [174](#)
 - GET [174](#)
 - Last Result [174](#)

- SET [174](#)
- set target units [174](#)
- WALK [174](#)
- Walk operation [178](#), [180](#)
- emergency number, setting [111](#)
- encryption, of configuration files
 - decrypt generic [126](#)
 - decrypt specific [126](#)
 - defined [126](#)

F

- fax
 - disabling call waiting tone [145](#)
- filter
 - applying [53](#)
 - copying existing [55](#)
 - creating new [51](#)
 - deleting [55](#)
 - logical expressions [50](#)
 - modifying existing [54](#)
- Find Units, toolbar icon [24](#)
- find, option in Edit SNMP window [180](#)
- finding units [38](#)
- firmware packs configuration [136](#)
- FQDN
 - in MGCP [102](#)
 - in NCS [104](#)
- friendly name, of unit [35](#)

G

- gatekeepers
 - defined [201](#)
 - H.323 [98](#)
- Gateway parameters
 - allowed numbers [87](#)
 - dial prefix [87](#)
 - general dial prefix [87](#)
 - incoming PSTN call [87](#)
 - local call in different AC [88](#), [89](#)
 - local call in same AC [88](#), [89](#)
 - long distance call in different AC [88](#), [89](#)
 - long distance call in different CC [88](#), [90](#)
 - long distance call in same AC [88](#), [89](#)
 - mode [86](#)
- general dial prefix, setting [87](#)
- GET operation [176](#), [180](#)
 - automatic [176](#)
- GetBulk, SNMP preferences [12](#), [164](#)
- groups
 - static [46](#)
 - virtual
 - creating [43](#)
 - deleting [46](#)
 - editing [46](#)
 - instances [44](#)

H

- H.323
 - defined [201](#)
 - parameters
 - aliases [98](#)
 - direct gateway call [99](#)
 - gatekeepers [98](#)

- registration method [98](#)
- hierarchy
 - applying to list of units [48](#)
 - copying existing [49](#)
 - creating new [47](#)
 - deleting [50](#)
 - modifying existing [48](#)
- Hierarchy, toolbar icon [23](#)
- hold, putting a call on [145](#)
- hook flash processing [158](#)
- HTTP
 - server
 - configuring [119](#), [127](#)

I

- input sound level, setting [93](#)
- instance
 - associating units to [44](#)
 - deleting in the tree list [48](#)
 - in virtual groups [44](#)
- intended audience [xi](#)
- Internet browser
 - opening [30](#)

L

- license key, in installation [4](#), [15](#), [18](#)
- local call
 - in a different AC [88](#), [89](#)
 - in the same AC [88](#), [89](#)
- local IP address, setting [70](#)
- location identification number, setting [111](#)
- long distance call
 - in a different AC [88](#), [89](#)
 - in a different Country Code (CC) [88](#), [90](#)
 - in the same AC [88](#), [89](#)

M

- Machine ID Key [4](#), [18](#)
- Manage Filters, toolbar icon [24](#)
- Manage Hierarchies, toolbar icon [23](#)
- MD5, authentication [14](#), [162](#), [165](#)
 - defined [201](#)
- MGCP parameters
 - call agent [101](#)
 - endpoint name [102](#)
 - FQDN [102](#)
 - listening port [102](#)
 - RSIPs restart level [102](#)
- MIB
 - cache, clearing [175](#)
 - icons [175](#)
 - in SNMP protocol [161](#)
 - opening a file [175](#)

N

- NCS parameters
 - call agent [104](#)
 - endpoint name [105](#)
 - FQDN [104](#)
 - listening port [104](#)
 - RSIPs restart level [104](#)

O

OID

- cache, clearing [34](#)
- output sound level, setting [93](#)

P

- polling, units status [31](#)
- ports, used for communication [20](#)
- primary DNS, setting [70](#)
- privacy, in SNMPv3 [14](#), [165](#)
- properties of server [24](#)
- properties of units. *see units*
- protocols, used for communication [20](#)

R

- Refresh tree, toolbar icon [23](#)
- Refresh, toolbar icon [23](#)
- refreshing, units [66](#)
- registration method, in H.323 [98](#)
- related documentation [xii](#)
- reports
 - description [40](#)
 - detailed [41](#)
 - saving to a file [40](#)
 - summary [41](#)
 - toolbar icon [23](#)
- restarting a unit [66](#)

S

- secondary DNS, setting [71](#)
- security level, in SNMPv3 [14](#), [165](#)
- Select Filter, toolbar icon [24](#)
- server properties [24](#)
- SET operation [176](#), [180](#)
 - force SET [180](#)
- setting
 - default router [70](#)
 - input sound level [93](#)
 - local IP address [70](#)
 - multiple units [39](#)
 - output sound level [93](#)
 - primary DNS [70](#)
 - secondary DNS [71](#)
 - silence detection/suppression level [94](#)
 - subnet mask [70](#)
 - voice coding algorithm [93](#)
- SHA, authentication [14](#), [162](#), [165](#)
- Show Units, toolbar icon [24](#)
- silence detection/suppression level, setting [94](#)
- SIP parameters
 - area code [107](#)
 - authentication [108](#)
 - country code [107](#)
 - friendly name [108](#)
 - prefix [107](#)
 - SIP Proxy/Redirect server [107](#)
 - SIP registrar [107](#)
 - user name [108](#)
- SNMP
 - behaviour [162](#)
 - non-secure management mode [162](#)
 - secure management mode [163](#)
 - defined [161](#)

- MIB [161](#)
- operations
 - GET [176](#), [180](#)
 - GET, automatic [176](#)
 - SET [176](#), [180](#)
 - Walk [178](#), [180](#)
- preferences [163](#)
 - community name [12](#), [163](#)
 - GetBulk settings [12](#), [164](#)
 - maximum repetitions [12](#), [164](#)
 - non repeaters [12](#), [164](#)
 - number of retries [12](#), [163](#)
 - port number [12](#), [163](#)
 - SNMPv3
 - authentication [14](#), [165](#)
 - context name [14](#), [165](#)
 - privacy [14](#), [165](#)
 - security level [14](#), [165](#)
 - user name [14](#), [165](#)
 - timeout [12](#), [163](#)
 - version [12](#), [163](#)
- SNMPv3 settings
 - cloning a user [166](#)
 - deleting a user [168](#)
 - modifying a user [167](#)
- SNTP
 - parameters, setting [73](#), [75](#)
 - server
 - configuring [119](#), [127](#)
- Software and Emergency Download parameters
 - primary server [71](#)
 - secondary server [71](#)
- software download
 - analog units, SIP v2.x [57](#)
 - analog units, SIP/MGCP v4.x/v5.x [57](#)
 - analog units, v4.x
 - zip file [58](#), [59](#)
 - automatic update [132](#)
 - digital units [58](#)
 - firmware packs configuration [136](#)
 - HTTP server, configuring [127](#)
 - server path [130](#)
 - SNTP server, configuring [127](#)
 - TFTP server, configuring [127](#)
 - transfer configuration [135](#)
 - zip file [127](#)
- sound level
 - input [93](#)
 - output [93](#)
- SSH session
 - opening [29](#)
- static groups. *see groups*
- STUN
 - configuring [140](#)
- subnet mask, setting [70](#)
- subscriber number, setting [110](#)
- subscriber services
 - call forward
 - on busy [149](#)
 - on no answer [151](#)
 - unconditional [147](#)
 - call transfer - attended transfer [146](#)
 - call transfer - blind transfer [146](#)
 - call waiting [145](#)
 - conference call [147](#)
 - configuration window [144](#)

- hold [145](#)
- overview [143](#)
- second call [146](#)
- synchronizing, units [66](#)
- syslog daemon parameters [72](#)

T

- T.38, faxing with [93](#)
- table viewer, in Edit SNMP window [178](#), [179](#)
- telephony attributes
 - automatic call [157](#)
 - call direction [156](#)
 - configuration window [156](#)
 - hook flash processing [158](#)
 - overview [155](#)
- Telnet session
 - opening [29](#)
 - settings [28](#)
- TFTP
 - server
 - configuring [119](#), [127](#)
- toolbar
 - in Edit SNMP window
 - See *Edit SNMP window*
 - in Unit Manager Network
 - See *Unit Manager Network*
- troubleshooting
 - general
 - autodetect units [169](#)

U

- UmnMibPack, installing [5](#)
- uninstalling [7](#)
- Unit detection, toolbar icon [23](#)
- Unit Manager Network
 - configuration file download
 - analog units [60](#)
 - digital units, startup [61](#)
 - saving to Dgw config script [65](#)
 - saving to XML format [64](#)
 - configuration file upload
 - analog units [62](#), [185](#)
 - digital units, startup [62](#)
 - configuring [9](#)
 - SNMP preferences [11](#)
 - unit selection [10](#)
 - user / password [9](#)
 - defining [15](#)
 - deleting units from [31](#)
 - Edit SNMP window [173](#)
 - finding new units [25](#), [195](#)
 - troubleshooting [169](#)
 - installing [3](#)
 - license key [4](#)
 - modifying existing [6](#)
 - UmnMibPack [5](#)
 - upgrading databases [6](#)
 - Internal Editor [19](#)
 - Administration parameters [69](#)
 - codec activation [94](#)
 - codec activation parameters [94](#)
 - configuration file download [119](#)
 - CorNet-IP parameters [110](#)
 - Fault Management [114](#)

- system services [112](#)
 - Dial Map parameters [79](#)
 - finding units [38](#)
 - Gateway parameters [85](#)
 - H.323 parameters [97](#)
 - IP addresses [35](#)
 - MGCP parameters [101](#)
 - NCS parameters [103](#)
 - overview [34](#)
 - parameters [36](#)
 - Ports parameters [91](#)
 - SIP parameters [106](#)
 - software download [127](#)
 - STUN [139](#)
- Internet browser
 - opening [30](#)
- license key [4](#), [15](#), [18](#)
- MIB browser [19](#)
- modules
 - Administrator [18](#)
 - Unit Manager [18](#)
- removing all DHCP options [67](#)
- restarting unit [66](#)
- software download
 - analog units [57](#)
 - Dgw v1.1/2.0 units [59](#)
 - digital units [58](#)
- SSH session
 - opening [29](#)
- states of units [31](#)
- Telnet session
 - opening [29](#)
 - settings [28](#)
- toolbar icons
 - About information [23](#)
 - Autodetect [23](#)
 - Connect [23](#)
 - Find Units [24](#)
 - Manage Filters [24](#)
 - Manage Hierarchies [23](#)
 - Refresh [23](#)
 - Refresh tree hierarchy [23](#)
 - Reports [23](#)
 - Select Filter [24](#)
 - Select Hierarchy [23](#)
 - Show Units [24](#)
 - Unit detection [23](#)
 - Virtual groups [23](#)
- uninstalling [7](#)
- versions [4](#), [15](#), [18](#)
- units
 - analog [24](#)
 - configuration file download [60](#)
 - configuration file upload [62](#), [185](#)
 - software download [57](#)
 - associating to an instance [44](#)
 - collection process [19](#)
 - configuration file download
 - saving to Dgw config script [65](#)
 - saving to XML format [64](#)
 - deleting from list [31](#)
 - Dgw v1.1/2.0
 - software download [59](#)
 - digital [25](#)
 - software download [58](#)
 - startup configuration download [61](#)

- startup configuration upload [62](#)
- finding [38](#)
- finding new [25](#), [195](#)
 - troubleshooting [169](#)
- large scale deployment
 - creating configuration file [185](#)
 - creating new configuration file [186](#)
 - introducing [185](#)
 - modifying existing configuration file [186](#)
 - using default configuration file [187](#)
 - using GUI [185](#)
- list of connected [19](#), [192](#)
- polling status [31](#)
- properties [34](#)
 - friendly name [35](#)
 - SNMP sysContact [35](#)
 - SNMP sysLocation [35](#)
 - SNMP sysName [35](#)
- refreshing [66](#)
- restarting [66](#)
- setting multiple [39](#)
- states [31](#)
- synchronizing [66](#)
- types [24](#)
- uplink parameters, setting [74](#)
- uploading
 - configuration file
 - analog units [62](#), [185](#)
 - digital units, startup [62](#)
- using this manual [xi](#)

V

- viewing options
 - friendly name [32](#)
 - IP address [32](#)
 - MAC address [32](#)
 - model-specific icons [32](#)
 - SNMP MIB-2 sysName [32](#)
- Virtual groups, toolbar icon [23](#)
- virtual groups. see *groups*
- voice coding algorithm, setting [93](#)

W

- Walk operation [178](#), [180](#)
- WAN parameters, setting [74](#)