

NewNet Mobile Messaging MGR R04.13.04

Operator Manual

Release 17.4 Revision B
March 2019



Copyright 2011 – 2019 Newnet. All Rights Reserved.

Table of Contents

Chapter 1: Introduction.....	15
1.1 About this Document.....	16
1.2 Scope.....	16
1.3 Intended Audience.....	16
1.4 Documentation Conventions.....	16
1.5 Locate Product Documentation on the Customer Support Site.....	17
Chapter 2: Getting Started.....	19
2.1 Introduction.....	20
2.2 MGR Configuration.....	20
2.2.1 Distribution and Synchronization.....	20
2.2.2 Redundancy.....	21
2.2.3 MGR Changeover.....	22
2.3 Domains.....	23
2.4 Access the MGR.....	23
2.4.1 Web Browser Requirements.....	23
2.4.2 License Parsing.....	24
2.4.3 Logging in to the MGR.....	24
2.4.4 Notifications in MGR.....	25
2.5 Important Terminology.....	28
2.6 Limitations.....	29
Chapter 3: Using the MGR Interface.....	33
3.1 Introduction.....	34
3.2 Left Navigation Bar.....	34
3.3 Tabs.....	34
3.4 Views.....	35
3.5 Keyboard Shortcuts.....	35
3.6 Filtering.....	37
3.6.1 Filtering a List.....	37
3.6.2 Removing a Filter.....	38
3.7 Searching.....	38
3.7.1 Taking Action on Search Results.....	40
3.8 Overviews.....	40

3.8.1 Overview Types.....	41
3.8.2 Using Overviews.....	42
3.9 Action and Context Menus.....	42
3.9.1 Available Actions.....	42
3.9.2 Activate.....	44
3.9.3 Deactivate.....	44
3.9.4 Copy.....	44
3.9.5 Restart.....	44
3.9.6 Resync.....	45
3.9.7 Delete.....	45
3.9.8 Limitations.....	46
3.10 Printing Screens.....	46
3.11 Considerations.....	46
3.12 Trap Service.....	47

Chapter 4: Routing.....49

4.1 Introduction.....	50
4.2 Prerequisites for Applicable Rules.....	50
4.3 Routing Rule Condition Formats.....	50
4.4 Creating Routing Rules.....	52
4.4.1 Creating an MO Routing Rule.....	52
4.4.2 Creating an SRI-SM Request Rule.....	67
4.4.3 Creating an SRI-SM Response Rule.....	73
4.4.4 Creating an Incoming MT Routing Rule.....	80
4.4.5 Creating an Outgoing MT Routing Rule.....	89
4.4.6 Creating an AO Routing Rule.....	100
4.4.7 Creating an Incoming AT Routing Rule.....	114
4.4.8 Creating an Outgoing AT Routing Rule.....	126
4.4.9 Creating an IGM Routing Rule.....	136
4.4.10 MO Rule Conditions for SIP Originated Message.....	140
4.5 Creating External Condition Rules.....	145
4.5.1 Creating an MO External Condition Rule.....	145
4.5.2 Creating an Incoming MT External Condition Rule.....	146
4.5.3 Creating an Outgoing MT External Condition Rule.....	148
4.5.4 Creating an AO External Condition Rule.....	150
4.5.5 Creating an Incoming AT External Condition Rule.....	151
4.5.6 Creating an Outgoing AT External Condition Rule.....	152
4.5.7 Creating an IGM External Condition Rule.....	153
4.6 Creating Counting Rules.....	155
4.7 Defining External Condition Applications.....	155

4.7.1 Defining EC Application Attributes.....	155
4.7.2 Creating EC Applications.....	156
4.7.3 Defining EC Messages.....	163
4.8 Creating Modifiers.....	164
4.8.1 Modifier Priority.....	165
4.8.2 Creating MO Modifiers.....	165
4.8.3 Creating MTI Modifiers.....	166
4.8.4 Creating MTO Modifiers.....	166
4.8.5 Creating AO Modifiers.....	170
4.8.6 Creating AT Modifiers.....	172
4.8.7 Priority Values for AO and AT Modifiers.....	173
4.9 Creating Lists.....	173
4.9.1 Types of Lists.....	173
4.9.2 Creating a List.....	174
4.9.3 Referencing a List.....	175
4.9.4 Creating an ABL List.....	175
4.9.5 Referencing an ABL List.....	176
4.10 Creating Auto Black List Entries.....	177
4.10.1 Types of Blacklisting.....	177
4.10.2 Creating a Blacklisting Entry.....	177
4.11 Defining Routing Numbers.....	178
4.11.1 Creating Routing Number Groups.....	178
4.11.2 Setting Routing Number Properties.....	179
4.12 Creating Application Load Balancing Groups.....	180
4.13 Creating Address Conversion Rules.....	181
4.13.1 Configuring Area Code Properties.....	181
4.13.2 Configuring Area Codes.....	181
4.13.3 Creating GSM Address Conversion Rules.....	182
4.13.4 Creating Outgoing Address Conversion Rule Sets.....	184
4.14 Configuring Routing Schedules.....	187
4.15 Configuring Routing Properties.....	188
4.16 Configuring Unicode Conversion Table.....	189
4.16.1 Configure Translation Characters	189
4.17 Configuring Mobile Number Portability.....	192
4.17.1 MNP Action.....	192
4.18 Configuring Message Template.....	193

Chapter 5: Firewall.....197

5.1 Introduction.....	198
5.2 Configuring MO Firewall Properties.....	198

5.3 Configuring MT Firewall Properties.....	198
---	-----

Chapter 6: SMS Applications.....201

6.1 Introduction.....	202
6.2 Creating SMS Application Groups.....	202
6.3 Provision an SMS Application.....	202
6.3.1 Session Models.....	207
6.3.2 UCP Applications.....	208
6.3.3 SMPP Applications.....	215
6.3.4 CIMD Applications.....	224
6.4 Creating SMS Application Categories.....	231
6.5 Creating Originator Lists.....	232
6.6 Creating Portable Applications.....	232
6.7 Creating CIMD Tariff Classes.....	233
6.8 Creating CIMD Tariff Class Descriptions.....	233
6.9 Creating CLI Address Lists.....	234
6.10 Configuring Character Set Conversion.....	235
6.10.1 Modify a Character Conversion Set.....	235
6.10.2 Rename a Character Set.....	235
6.11 Configuring Error Mapping Tables.....	236
6.11.1 Modify a Forward Error Mapping Table.....	236
6.11.2 Add a Forward Error Mapping Table.....	237
6.11.3 Modify a Reverse Error Mapping Table.....	237
6.11.4 Add a Reverse Error Mapping Table.....	239
6.11.5 Add a Reverse Error Text Code.....	240

Chapter 7: Environment.....243

7.1 Introduction.....	244
7.2 Configuring Countries.....	244
7.3 Adding Networks.....	245
7.4 Provisioning Own IMSIs.....	247
7.5 Configuring Outside Listeners.....	247
7.6 Creating Service Classes.....	249
7.7 Configuring SMSCs.....	250
7.7.1 Create SMSC Groups.....	250
7.7.2 Configure SS7 SMSCs.....	251
7.7.3 Configure Service Centres.....	251

Chapter 8: Storage.....255

8.1 Introduction.....	256
8.2 Creating Delivery Schemes.....	256
8.3 Configuring Message Queues.....	258
8.4 Configure Error-Dependent Schemes.....	259
8.4.1 AT Error Dependent Schemes.....	259
8.4.2 SRI-SM Error-Dependent Schemes.....	259
8.4.3 MT Error-Dependent Schemes.....	260
8.5 Configuring the Icache.....	262
Chapter 9: IPSMGW.....	265
9.1 Introduction.....	266
9.2 Creating SIP Application.....	266
9.3 Creating SIP End Point.....	266
9.4 Creating SIP End Point Group.....	267
9.5 Creating SIP Headers.....	268
Chapter 10: Advanced Filters.....	269
10.1 Introduction.....	270
10.2 Create an Advanced Filter.....	270
10.3 Add Conditions to an Advanced Filter.....	271
10.3.1 Add an Expression Condition	272
10.3.2 Add a Content Condition.....	274
10.3.3 Add a Duplicates Condition.....	279
10.3.4 Add a Flooding Condition.....	280
10.3.5 Add an Enhanced Messaging (EMS) Condition.....	281
10.3.6 Add a Volume Condition.....	282
10.3.7 Add a Bulk Condition.....	283
10.3.8 Add a Spread Condition	284
10.3.9 Add a Delta Condition	285
10.4 Create an Advanced Filter List.....	286
Chapter 11: Billing.....	287
11.1 Introduction.....	288
11.2 Configuring Prepaid Billing.....	288
11.3 Configuring Post-Paid Billing.....	289
11.3.1 Creating Billing Profiles.....	289
11.3.2 Configuring Billing Properties.....	313
Chapter 12: Logging.....	315

12.1 Introduction.....	316
12.2 Message Logging.....	316
12.2.1 Creating Message Logging Profiles.....	316
12.2.2 Configuring Message Logging Properties.....	318
12.2.3 Configuring Message Log Filters.....	319
12.2.4 Configuring Message Log View Columns.....	320
12.2.5 Using Message Log Search.....	321
12.3 Event Logging.....	323
12.3.1 Creating Event Logging Profiles.....	323
12.3.2 Configuring Event Logging Properties.....	324
12.3.3 Configuring Event Log Filters.....	325
12.3.4 Using Event Log Search.....	326
12.4 Configuring Logging Properties.....	326
12.5 Background Query.....	327
12.5.1 Background Query Configuration.....	328
12.6 Flexible User Data Text Search using LGV.....	329

Chapter 13: SPF Services.....333

13.1 Introduction.....	334
13.2 User Privileges.....	334
13.3 Create a Service.....	334
13.4 Add/Modify Command Aliases.....	341
13.5 Add/Modify Parameter Aliases.....	341
13.6 Message Template String Format.....	342

Chapter 14: Batch Sending.....345

14.1 Introduction.....	346
14.2 Configuration Item Dependencies.....	346
14.3 Creating SMS Templates.....	346
14.4 Adding Distribution Lists.....	347
14.4.1 Downloading Distribution Lists.....	348
14.4.2 Distribution List File.....	349
14.5 Configuring Delivery Schemes.....	350
14.6 Viewing Batch Job Status.....	350
14.7 Creating Batch Jobs.....	351
14.8 Configuring Batch Applications.....	352
14.9 Configuring Batch SMSCs.....	353
14.10 Configuring Batch Termination Points.....	354
14.11 Configuring Batch Properties.....	355

Chapter 15: Tracing.....	357
15.1 Introduction.....	358
15.2 Application Traffic Trace Filter.....	358
15.2.1 Creating Trace Filters.....	358
15.2.2 Configuring Trace Filter Conditions.....	358
15.3 SS7 Trace Filters.....	359
15.3.1 Creating Trace Filters.....	359
15.4 SIP Tracing.....	360
15.4.1 Creating Trace Filters.....	360
15.4.2 Configuring SIP Trace Filter Conditions	361
Chapter 16: Settings.....	363
16.1 Introduction.....	364
16.2 Setting Your Preferences.....	364
16.3 User Administration.....	364
16.3.1 User Password Policy.....	365
16.3.2 Add a User.....	365
16.3.3 Unlock a User Account.....	366
16.3.4 Add a User Group.....	366
16.3.5 Remove a User Group.....	368
16.4 Viewing Error and Change Logs.....	368
16.4.1 Error Log.....	368
16.4.2 User Change Log.....	369
16.4.3 Automatic Change Log.....	369
16.5 Adding Domains.....	370
16.5.1 Domain Database Management.....	371
16.6 Configuring Servers.....	371
16.7 Configuring Devices.....	372
16.7.1 Add a Device.....	372
16.7.2 Polling Devices.....	375
16.7.3 Device States.....	375
16.7.4 DNS Query Mechanism	377
16.7.5 Device Limitations.....	377
16.8 Configuring Global Settings.....	378
16.8.1 Configuring User-Defined Fields.....	379
16.9 Pending Transactions.....	380
16.10 Verifying Device License Information.....	382
16.10.1 Verifying Local License Information for All Devices.....	382
16.10.2 Verifying Device-Specific License Information for Each Device.....	382

16.11 Customising the Application Password Generator.....	382
16.12 Configure CCI Properties.....	384

Chapter 17: Statistics.....387

17.1 Introduction.....	388
17.2 Types of Statistics.....	388
17.3 Configuring Statistics Settings.....	391
17.3.1 Set Polling Intervals.....	391
17.3.2 Set Data Retention Intervals.....	391
17.3.3 Create Pollers.....	392
17.3.4 Filter System Processes.....	392
17.3.5 Customise Polling Groups.....	393
17.3.6 Configuring Export Streams.....	396

Chapter 18: Command-Line Tools and Scripts.....403

18.1 Introduction.....	404
18.2 tp_app_throughput.....	404
18.2.1 Synopsis.....	404
18.2.2 Options.....	404
18.2.3 Operands.....	405
18.3 clean_mgr_error_logs.....	405
18.4 tp_auth.....	405
18.4.1 Synopsis.....	405
18.4.2 Commands.....	405
18.4.3 Options.....	406
18.4.4 Operands.....	407
18.4.5 Sample Usage.....	407
18.5 tp_configure_dmf.....	407
18.5.1 Synopsis.....	408
18.5.2 Options.....	408
18.6 tp_install_mgr.....	408
18.6.1 Options.....	408
18.6.2 Upgrade Process.....	410
18.6.3 Usage.....	410
18.6.4 File Format.....	411
18.7 tp_master.....	411
18.7.1 Synopsis.....	411
18.7.2 Options.....	411
18.8 tp_mgr_backup.....	412
18.8.1 Synopsis.....	412

18.8.2	Options.....	412
18.8.3	Operands.....	412
18.8.4	Example.....	413
18.9	tp_mgr_domain_sharing.....	413
18.9.1	Synopsis.....	413
18.9.2	Options.....	413
18.9.3	Example.....	414
18.10	tp_mgr_ecmessage_import.....	414
18.10.1	Synopsis.....	414
18.10.2	Options.....	414
18.11	tp_mgr_poll.....	415
18.11.1	Synopsis.....	415
18.11.2	Options.....	415
18.12	tp_mgr_restore.....	416
18.12.1	Synopsis.....	416
18.12.2	Options.....	416
18.12.3	Operands.....	416
18.12.4	Example.....	417
18.13	tp_mgr_start.....	417
18.13.1	Synopsis.....	417
18.13.2	Options.....	417
18.14	tp_mgr_stop.....	417
18.15	tp_mgr_table_migration	418
18.15.1	Synopsis	418
18.15.2	Options	418
18.16	tp_role.....	420
18.17	tp_shell.....	421
18.17.1	Synopsis.....	421
18.17.2	Authentication Options.....	421
18.17.3	tp_shell Commands.....	422
18.17.4	Options.....	423
18.17.5	Command File Format.....	423
18.17.6	Example Use Cases.....	424
18.18	tp_slave.....	427
18.19	tp_update_mgr_device.....	427
18.19.1	Synopsis.....	427
18.19.2	Options.....	427

Appendix A: Logging Elements.....429

A.1	Message Logging.....	430
-----	----------------------	-----

A.2 Event Logging.....	435
Appendix B: References.....	437
B.1 References.....	438
Glossary.....	439

List of Figures

Figure 1: Pending Transactions.....	25
Figure 2: Notification Message: Multiple Configuration Update.....	26
Figure 3: Notification: Configuration Synching.....	26
Figure 4: Notification: Configuration Synching in Progress.....	27
Figure 5: Notification: Device Deletion during Configuration Synching.....	27
Figure 6: Notification: Configuration Update by Same User.....	28
Figure 7: Notification: Configuration Update by Another User.....	28
Figure 8: Left navigation bar.....	34
Figure 9: Example with no filter applied.....	38
Figure 10: Example with filter applied.....	38
Figure 11: Example with filter applied and no results.....	38
Figure 12: Searching with the AND operator.....	39
Figure 13: Searching with the OR operator.....	39
Figure 14: Context menu for search results.....	40
Figure 15: Result of action selected from context menu.....	40
Figure 16: Action menu, MGR tab (with BAT installed).....	43
Figure 17: Context menu, search results.....	43
Figure 18: MGR GUI screenshot of Apply SCCP CdPA Modifier for Report SM operation checkbox in MTO Modifier properties.....	169
Figure 19: Example of configured lists.....	175
Figure 20: Forward error mapping tables.....	236
Figure 21: Sample forward error mapping table.....	236
Figure 22: Reverse error mapping tables.....	238
Figure 23: Sample reverse error mapping table.....	238
Figure 24: Sample delivery intervals.....	257
Figure 25: Sample filter with conditions.....	272
Figure 26: Prepaid billing properties.....	289
Figure 27: Post-paid billing profile.....	291
Figure 28: MGR GUI Snapshot for SCDR Billing Profile, with Default Configuration.....	311
Figure 29: LCDR Custom Format.....	311
Figure 30: CCDRG File Format.....	312
Figure 31: MessageFields->userData condition options.....	329
Figure 32: smsDeliver->userData condition options.....	330
Figure 33: smsSubmit->userData condition options.....	330
Figure 34: Filter Element userData_normalizedText for Message Filters.....	331
Figure 35: userData_normalizedText condition option.....	331
Figure 36: BAT dynamic configuration dependencies.....	346

Figure 37: Example batch job status.....	351
Figure 38: MGR privileges.....	368
Figure 39: Device states.....	376
Figure 40: Pending Transactions.....	381
Figure 41: Pending Transaction Details.....	381
Figure 42: Password generation buttons.....	383
Figure 43: Customised character sets.....	383
Figure 44: Customer Care Properties.....	384
Figure 45: Sample add/remove counter from Polling Group.....	399
Figure 46: Example Export Stream State.....	400
Figure 47: Example Export Stream Status.....	401
Figure 48: Example detailed Export Stream Status.....	401

Chapter 1

Introduction

Topics:

- *About this Document.....16*
- *Scope.....16*
- *Intended Audience.....16*
- *Documentation Conventions.....16*
- *Locate Product Documentation on the Customer Support Site.....17*

1.1 About this Document

This document provides a complete overview of the NewNet Mobile Messaging Manager, the Web-based tool for configuring, managing, and modifying a Mobile Messaging system.

The Manager (MGR) is a component of the NewNet Mobile Messaging product family of SS7 message routing and network querying products.

The functions that are available in the MGR depend on the specific implementation; therefore, some functions in this document may not apply to your system. Your MGR interface may differ from the screens shown in this document, depending on software versions and browser configurations.

1.2 Scope

This document describes the functionality of the NewNet Mobile Messaging MGR component.

1.3 Intended Audience

This document is meant for everyone who is interested in the functionality offered by the Manager, but specifically for:

- Implementation Engineers who are responsible for the pre-installation, on-site installation, and configuration of the Manager in the end-user environment.
- Maintenance and Support Engineers who are responsible for maintaining the total system environment of which the Manager is a part.
- Network Operators who are in charge of the daily operation of the NewNet Mobile Messaging systems and infrastructure.

1.4 Documentation Conventions

Typeface or Symbol	Meaning	Example
Bold	Refers to part of a graphical user interface.	Click Cancel .
Courier	Refers to a directory name, file name, command, or output.	The billing directory contains...
<pointed brackets>	Serves as a placeholder for text that the user will replace, as appropriate in context.	The file is called MGRdata.xml.<ip>.gz, where <ip> is the server's IP address.
[square brackets]	Indicates an optional command.	[--validateonly]

Typeface or Symbol	Meaning	Example
Note:	Indicates information alongside normal text, requiring extra attention.	Note: Ensure that the configuration...
\ (Unix)	Denotes line continuation; the character should be ignored as the user types the example, and ENTER should only be pressed after the last line.	% grep searchkey \ data/*.dat

1.5 Locate Product Documentation on the Customer Support Site

Access to NewNet's Customer Support site is restricted to current NewNet customers only. This section describes how to log into the NewNet Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the NewNet Customer Support site.

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

Getting Started

Topics:

- *Introduction.....20*
- *MGR Configuration.....20*
- *Domains.....23*
- *Access the MGR.....23*
- *Important Terminology.....28*
- *Limitations.....29*

2.1 Introduction

The Manager is a flexible Web-based tool for configuring, managing, and monitoring the NewNet Mobile Messaging system. In the Manager, you:

- Configure the SMS network
- Create SMS routing logic
- Configure communication to and from applications, SMSCs, and service centres
- Configure storage in the Active Message Store (AMS)
- Retrieve logs of activity
- Monitor real-time statistics

For information about installing and configuring the Manager, refer to the Full Element Installation Manual.

2.2 MGR Configuration

The MGR stores its configuration in a MySQL database. The files containing the configuration are generated when Apache starts.

The complete configuration is distributed to all nodes in the system, to ensure that all nodes are in sync. The complete configuration of a device is stored in `/usr/TextPass/etc/MGRdata.xml.<ip>.gz`, where `<ip>` is the device's IP address.

When you make configuration changes in the MGR, the configuration file is updated and distributed to the devices that are running.

The MGR also uses a file called `mgr.cnf` to store MGR settings between installations. The file contains information about the database (which is modified with the `tp_install_mgr` command-line tool), system paths, and network settings. The `mgr.cnf` file should not be edited.

2.2.1 Distribution and Synchronization

The following services manage configuration distribution and synchronization between the MGR and the devices in the system:

Service	Runs on...	Description
<code>tp_fserver</code>	MGR node	Enables the transfer of <code>MGRdata.xml.<ip>.gz</code> and provides an interface for <code>tp_fclient</code> .
<code>tp_fclient</code>	Device nodes	Requests updates from <code>tp_fserver</code> and stores <code>MGRdata.xml.<ip>.gz</code> locally.
<code>tp_mgr_poll</code>	MGR node	Writes the configuration file that devices require to start up, periodically polls the devices to determine their operational states,

Service	Runs on...	Description
		and updates the MGR database with state information. Note: 1. The polling period is not configurable. 2. <code>tp_mgr_poll</code> uses connection timeout and response timeout values configured in <code>/usr/TextPass/etc/mgr.cnf</code> file. The default value of "connect timeout" is 2 seconds and "response timeout" is 5 seconds.
<code>tp_mgrd</code>	Device nodes	Listens on TCP port 11111 for configuration updates from the MGR and executes SNMP commands locally.

When a device starts up, it reads the local configuration file, which contains all of the settings necessary for the device.

If the `tp_mgr_poll` service is not running, the device states will not be updated in the MGR.

Note:

1. The MGR services will not start if Apache is not running.
2. If multiple instances of traffic elements are configured, then `tp_mgr_poll` connection and response time should be increased so that MGR is able to get the status of devices. If more than 3 NMM users are configured in multi-instance mode then set "connect_timeout" value to 5 seconds and "response_timeout" value to 10s second in `/usr/TextPass/etc/mgr.cnf` file on OAM node.

```
<network connect_timeout="5" response_timeout="10" />
```

3. Time to auto refresh the MGR GUI screen can be configured using:

```
/usr/TextPass/etc/mgr.cnf file. Specify the "auto_refresh_interval" attribute in network tag. Default value is 5 seconds.  
<network connect_timeout="5" response_timeout="10" auto_refresh_interval="5"/>
```

2.2.1.1 Compact SMSC Requirements

In a "compact SMSC" configuration (in which the RTR, HUB, IIW, and AMS reside on the same server), `tp_fserver` and `tp_fclient` are not necessary.

However, `MGRdata.xml.<ip>.gz` must still be available to the RTR, HUB, IIW, and AMS. To make the file available, create a symbolic link to it in the `/usr/TextPass/etc` directory. The link must have the same name as the file.

2.2.2 Redundancy

Redundancy for the MGR is ensured by implementing a cold stand-by configuration in which there is one active MGR server and one stand-by MGR server. The active server is configured as master and the stand-by server is configured as subordinate (slave).

Each MGR server has a database that is subordinate to the other database, through MySQL's master/subordinate (slave) configuration. `tp_client` runs on the subordinate MGR server to ensure that the configuration files remain in sync with the master MGR server.

2.2.2.1 Host File Configuration

Each MGR server should be configured as master or subordinate MGR.

To configure a server as the master MGR:

1. Log in on the server as user root.
2. In the `/etc/hosts` file, add an entry with the name of the subordinate MGR and the `peerfserver` alias.

For example, if the master MGR is named `mbn1-mgr01` and the subordinate MGR is named `mbn1-mgr02`:

```
192.168.0.1 mbn1-mgr01
192.168.0.2 mbn1-mgr02 peerfserver
```

Note: The Master and Slave MGR addresses can be either IPv4 or IPv6 address.

To configure a server as the subordinate MGR:

1. Log in on the server as user root.
2. In the `/etc/hosts` file, add an entry with the name of the master MGR and the `peerfserver` alias.

For example, if the master MGR is named `mbn1-mgr01` and the subordinate MGR is named `mbn1-mgr02`:

```
192.168.0.1 mbn1-mgr01 peerfserver
192.168.0.2 mbn1-mgr02
```

Note: The Master and Slave MGR addresses can be either IPv4 or IPv6 address.

2.2.3 MGR Changeover

If the master MGR server fails and the `peerfserver` configuration in the host file is correct, the subordinate MGR server will take over. If the MGR server fails, the Web interface will stop responding, but there will not be a notification or SNMP trap.

If the master MGR fails:

1. Log in to the server that failed as user root and execute the `tp_slave` command.
2. Log in to the subordinate server as user root and execute the `tp_master` command.

This procedure will start all processes required for the subordinate MGR server to become the master.

Note: If the server that failed is completely unavailable (such as during a power outage), you can skip step 1.

2.3 Domains

The MGR can control multiple Mobile Messaging networks, which are called domains. For example, you may have a Firewall (FWL) setup, an Application Gateway (AGW) implementation, and a Storage (AMS) solution; domains enable you to manage all of them while centralizing user management, error detection, and other configuration items. The MGR includes one default domain, called main.

You can share the following items between domains:

- Applications
- Application groups
- Application categories
- Service centers
- Service classes
- Networks
- Countries
- Lists
- Subscriber services

It is recommended to maintain shared items in the main domain, then create a new domain for each network and adjust the configuration and user privileges in the new domains.

Routing rules, external condition rules, counting rules, and statistics are always per-domain. By default, the Customer Care Interface (CCI) is also per-domain, so that operators in a hosting environment cannot search other hosted operators' data. However, you can change the CCI to search all domains; refer to [Configure CCI Properties](#).

For information about adding MGR domains and sharing information among them, refer to [Adding Domains](#). For information about assigning MGR user privileges, refer to [User Administration](#).

2.4 Access the MGR

The MGR is a Web-based interface that you access using a Web browser. The MGR GUI is accessible on the IPv4 and IPv6 addresses configured on the MGR node.

2.4.1 Web Browser Requirements

The following Web browsers are allowed:

- Microsoft Internet Explorer version 9 or higher
- Mozilla Firefox version 12 or higher
- All other browser types

A notification will appear in the GUI if you attempt to log in using a deprecated or disallowed browser.

Note: If you are using an Internet Explorer version with Compatibility View enabled, the GUI will see the browser as an earlier Internet Explorer version and may display a warning message. Refer to <http://support.microsoft.com/kb/956197> for more information about Compatibility View.

Deprecated Browsers

The following browsers are allowed, but support is deprecated:

- Microsoft Internet Explorer version 8
- Mozilla Firefox versions 11

If you are using a deprecated browser, you will be allowed to log in; however, the GUI component is not guaranteed to work correctly. It is recommended that you switch to an allowed browser. Deprecated browsers will be phased out in the next Mobile Messaging release.

Disallowed Browsers

If you are using one of following browsers, you will not be allowed to login:

- Microsoft Internet Explorer versions prior to version 8
- Mozilla Firefox versions prior to version 6.0

To access Mobile Messaging GUI components, you must switch to an allowed browser.

2.4.2 License Parsing

Parsing of licenses in MGR is different from other components. MGR will consider the license file (of a node/Traffic Element) with higher expiry time.

Example: If two license files are present for same node, one with unlimited and the other with specific expiry time, then the MGR will consider the license file with unlimited expiry time, irrespective of their license numbers. All the permissions and links are displayed according to the considered license file.

While copying the licenses in the MGR, make sure the operator is copying the correct license files.

2.4.3 Logging in to the MGR

To log in to the MGR:

1. In a Web browser, go to: `http://<MGR host>/tpm`

Where <MGR host> is the IPv4 address, IPv6 address or host name of the MGR node.

2. Enter your user name in the **User name** box.
3. Enter your password in the **Password** box.

Note: User names and passwords are case-sensitive.

4. Select the domain from the **Domain** list.
5. Click **Login**.

Note: An administrator can set the number of subsequent failed log-in attempts that you are allowed before your account is locked (the default is three). If your account is locked, an administrator must unlock it before you can log in.

2.4.3.1 Logging in for the First Time

By default, the MGR includes two preinstalled user accounts called admin and tester. Neither account has a password set for the first log-in. Until a password is set, neither account can be used to accomplish any task except editing user preferences.

When you log in to the MGR for the first time, you must change your password. To change your password:

1. In the left navigation bar, select **Settings**, then **My Preferences**.

The My Preferences tab appears.

2. In the **User Password** box, type a new password.
3. Re-type the password in the **Confirm Password** box.
4. Click **Save**.

The My Preferences tab closes.

5. In the upper right corner of the MGR interface, click **Logout**.
6. Log in using your new password.

2.4.4 Notifications in MGR

The MGR GUI displays certain notification messages and other relevant information regarding ongoing transactions, as described in this section.

1. When a user creates/modifies any configuration in MGR, the updated configuration which needs to be synced with other nodes (e.g. Traffic elements) will be saved in the database table and can be viewed in the pending transactions screens '**Settings > Pending Transactions**' screen (refer to [Pending Transactions](#) for more information).

Mobile Messaging | Unsupported Browser! | Search | Logout | Support | www reserved for customer's k

Global Settings/syncing

Index	Table	Action	IP	Device Name	Table Index
3228	listConditionTable	set	172.16.133.103	RTR2	5.2959
3229	listConditionTable	set	172.16.133.33	RTR_instance1	5.2959
3230	listConditionTable	set	172.16.133.33	RTR	5.2959
3231	listConditionTable	set	172.16.133.103	RTR2	5.2959
3232	listConditionTable	set	172.16.133.33	RTR_instance1	5.2959
3233	listConditionTable	set	172.16.133.33	RTR	5.2959
3234	listTable	set	172.16.133.33	RTR_instance1	5
3235	listTable	set	172.16.133.103	RTR2	5
3236	listTable	set	172.16.133.33	RTR	5

Refresh

Figure 1: Pending Transactions

2. Only one configuration update operation is allowed throughout all the active sessions of MGR GUI. If a user tries to perform a configuration update operation while another such operation

initiated by the same/another user is already in progress, then the following notification message is displayed on the screen: **“Another operation is in progress. Please try after some time.”**

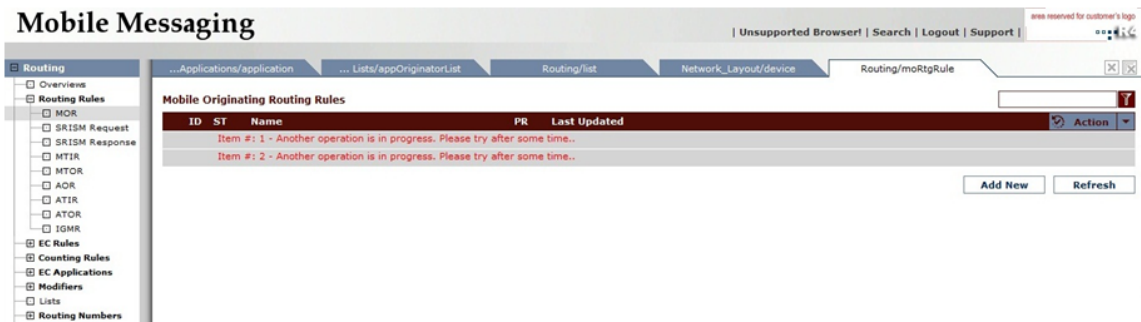


Figure 2: Notification Message: Multiple Configuration Update

3. If some entries are present on 'Settings-> Pending Transactions' screen (refer Figure 1), and a user wants to perform any configuration update operation pertaining to the table(s) present in the list of Pending Transactions, then the notification message **“Configuration syncing currently in progress, hence updates are not allowed. Please try after some time”** is displayed on the screen.

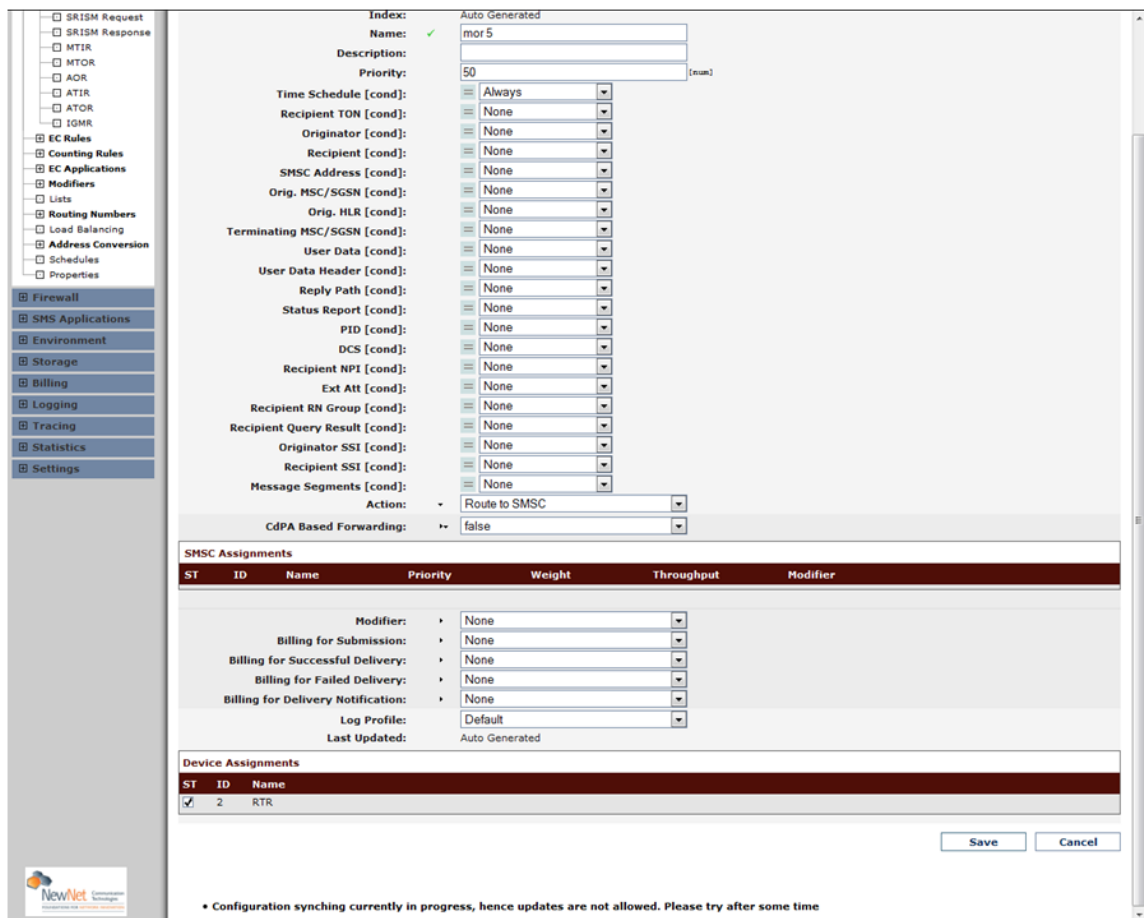


Figure 3: Notification: Configuration Syncing

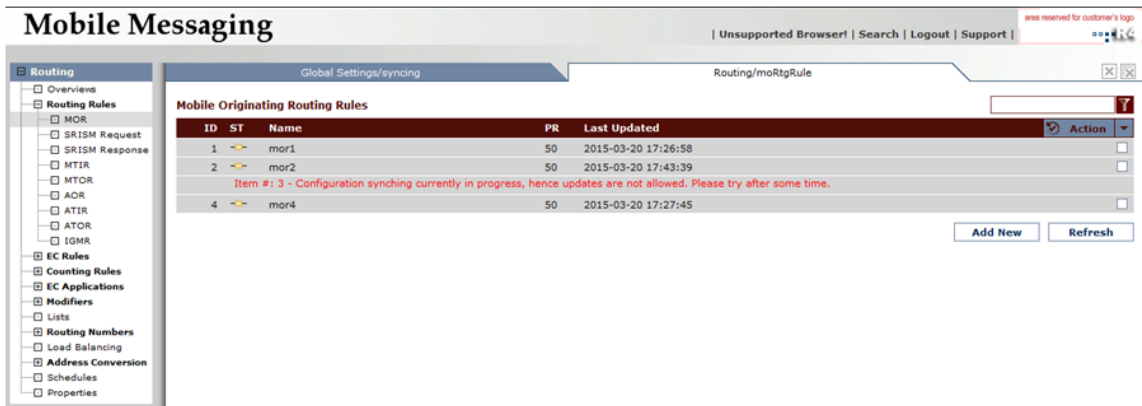


Figure 4: Notification: Configuration Syncing in Progress

- Users also cannot delete any device when one or more records are present in the list of **Pending Transactions**.

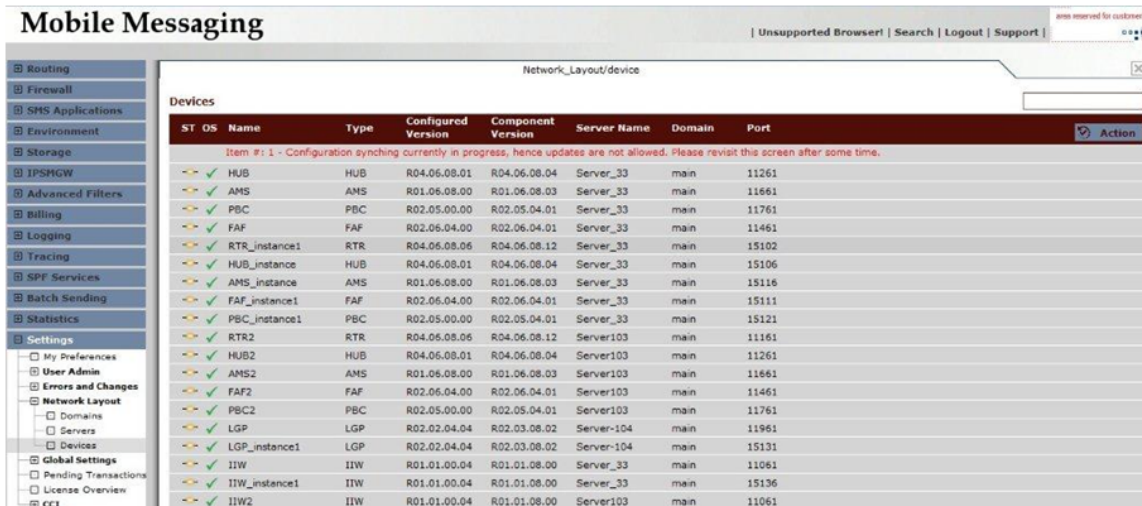


Figure 5: Notification: Device Deletion during Configuration Syncing

- When a user will access any GUI tab from the left-hand navigation menu, the notification message "Configuration update operation currently in progress, hence latest updated data is not being displayed. Please refresh or revisit this screen after some time" will be displayed on the screen if the corresponding table is present in the **Pending Transactions** screen or if another user is performing a configuration update operation on that table..

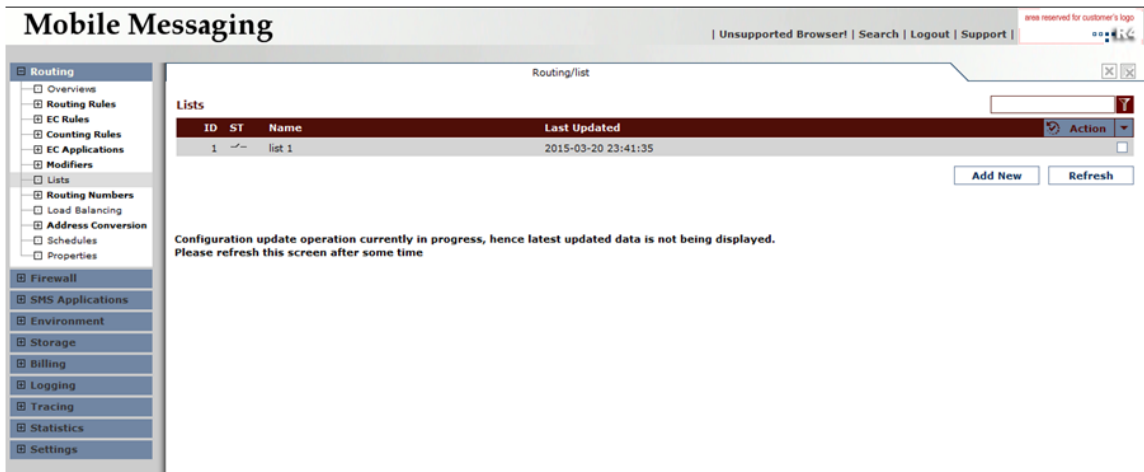


Figure 6: Notification: Configuration Update by Same User

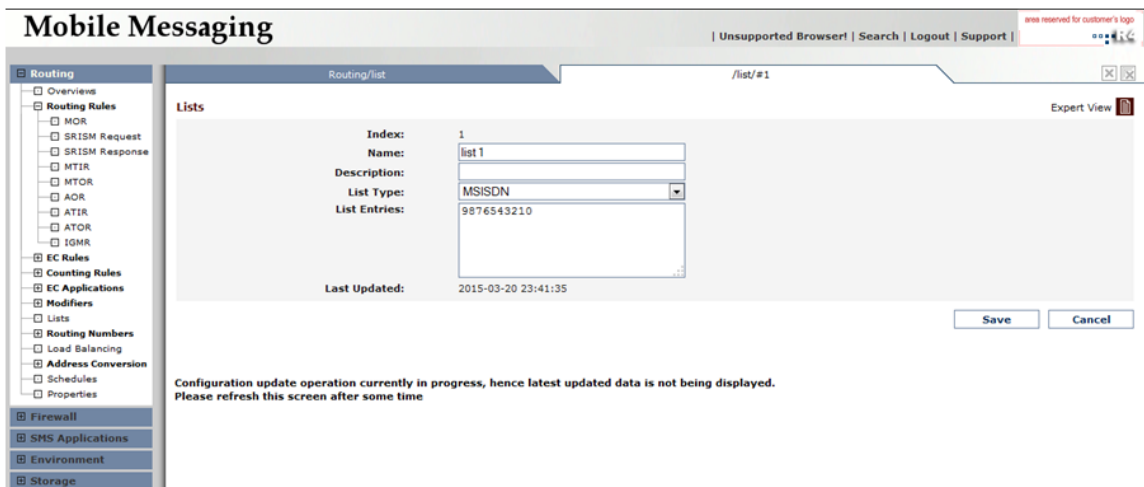


Figure 7: Notification: Configuration Update by Another User

Note: Configuration updates are not allowed when configuration of same table is pending for synchronization. User will get "Configuration synching currently in progress, hence updates are not allowed. Please try after some time" notification message.

2.5 Important Terminology

Term	Description
AOC	Application-originating (AO) counting rule
AOR	Application-originating (AO) routing rule
AOX	Application-originating (AO) external condition (EC) rule

Term	Description
ATIC	Incoming application-terminating (ATI) counting rule
ATIR	Incoming application-terminating (ATI) routing rule
ATIX	Incoming application-terminating (ATI) external condition (EC) rule
ATOC	Outgoing application-terminating (ATO) counting rule
ATOR	Outgoing application-terminating (ATO) routing rule
ATOX	Outgoing application-terminating (ATO) external condition (EC) rule
ECI	External Condition Interface, the interface that the Router (RTR) uses to communicate with external condition (EC) applications; runs on top of a TCP/IP network stack
Inside session	A session in the HUB, set up toward or coming from an SMS application
MOC	Mobile-originating (MO) counting rule
MOR	Mobile-originating (MO) routing rule
MOX	Mobile-originating (MO) external condition (EC) rule
MTIC	Incoming mobile-terminating (MTI) counting rule
MTIR	Incoming mobile-terminating (MTI) routing rule
MTIX	Incoming mobile-terminating (MTI) external condition (EC) rule
MTOC	Outgoing mobile-terminating (MTO) counting rule
MTOR	Outgoing mobile-terminating (MTO) routing rule
MTOX	Outgoing mobile-terminating (MTO) external condition (EC) rule
Outside listener	The HUB's TCP listening port for SMS applications
Outside session	A session in the HUB, set up toward or coming from an SMSC or a RTR
Service class	The quality-of-service mechanism for SMS applications

2.6 Limitations

The following table summarizes the maximum number of items that can be configured in the MGR.

Item	Limitation
AMS delivery schemes	500
AMS queue entities	1000
Application categories	1000
Application groups	1000
Application originator lists	10,000

Item	Limitation
Application-originating counting rules (AOC)	500
Application-originating EC rules (AOX)	500
Application-originating modifiers	100
Application-originating routing rules (AOR)	500
Billing profiles	1000
Categories	1000
CIMD tariff class descriptions	100
CIMD tariff classes	100
CLI source addresses for all applications that use CLI only authentication or CLI or password authentication	10,000
CLI source address per application	100
Conditions per FAF filter	100
Countries	500
Devices	Refer to Device Limitations
Entries per FAF list	1000
Entries per list	10,000
Entries per SMS application originator list	10,000
External attributes	32
External condition (EC) applications	100
FAF filters	100
FAF filters: content conditions	100
FAF filters: delta conditions	10
FAF filters: duplicates conditions	100
FAF filters: EMS conditions	100
FAF filters: flooding conditions	10
FAF filters: spread conditions	10
FAF lists	100
GSM Address Conversion Rules	1000
IMSI scrambling prefixes	50
Incoming application-terminating counting rules (ATIC)	500
Incoming application-terminating EC rules (ATIX)	500

Item	Limitation
Incoming application-terminating routing rules (ATIR)	500
Incoming mobile-terminating counting rules (MTIC)	500
Incoming mobile-terminating EC rules (MTIX)	500
Incoming mobile-terminating modifiers	100
Incoming mobile-terminating routing rules (MTIR)	500
Inside sessions per HUB per application per service center	255
Intervals per AMS delivery scheme	100
Lists	1000
Load balancing groups	1000
Log profiles	100
Mobile-originating counting rules (MOC)	500
Mobile-originating EC rules (MOX)	500
Mobile-originating routing rules (MOR)	500
Mobile-originating modifiers	100
Networks	1000
Outgoing Address Conversion Rule Set	500
Outgoing Address Conversion Rules	1000
Outgoing application-terminating counting rules (ATOC)	500
Outgoing application-terminating EC rules (ATOX)	500
Outgoing application-terminating routing rules (ATOR)	500
Outgoing mobile-terminating counting rules (MTOC)	500
Outgoing mobile-terminating EC rules (MTOX)	500
Outgoing mobile-terminating modifiers	100
Outgoing mobile-terminating routing rules (MTOR)	500
Outside listeners	250
Routing number groups	100
Routing numbers per group	100
Service center nodes	500
Service center termination points	1000
Service centers	250
Service classes	1000

Item	Limitation
SMS applications	10,000
SMSC groups	500
SMSCs (SS7)	500
TCP/IP connections (including outside and inside sessions)	12,000

Chapter 3

Using the MGR Interface

Topics:

- *Introduction.....34*
- *Left Navigation Bar.....34*
- *Tabs.....34*
- *Views.....35*
- *Keyboard Shortcuts.....35*
- *Filtering.....37*
- *Searching.....38*
- *Overviews.....40*
- *Action and Context Menus.....42*
- *Printing Screens.....46*
- *Considerations.....46*
- *Trap Service.....47*

3.1 Introduction

The MGR interface enables you to quickly and easily configure, modify, and manage your system.

3.2 Left Navigation Bar

Use the left navigation bar to access the MGR's functionality. The functions that appear in the left navigation bar depend on the licensed products in the system and on your authorization level.

The MGR does not link licensed functionality to a specific device. If multiple license files (for multiple devices) are present on the MGR node and, upon start-up, the MGR finds at least one license containing a specific feature, then the MGR will enable that feature for all devices.

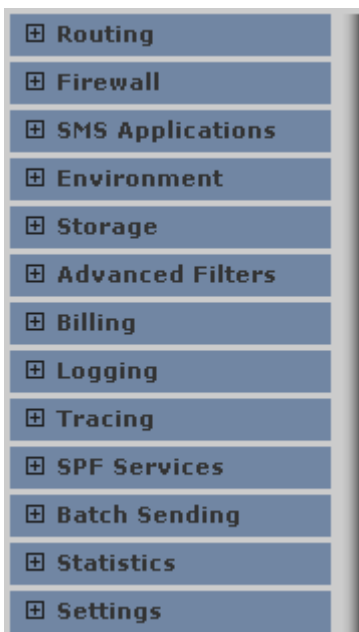


Figure 8: Left navigation bar

3.3 Tabs

Items open in tabs in the MGR. Change to a tab by clicking it or by selecting the same item from the left navigation bar.

To close the current tab, click



in the upper right corner of the MGR interface.

To close all tabs, click



in the upper right corner of the MGR interface.

Note: If you close a tab without saving the changes that you made on that tab, the MGR discards the changes.

3.4 Views

The MGR offers three different views:

- Basic view—Shows the basic parameters that are required to create a configuration. Parameters with suitable defaults are hidden.
- Standard view—Shows basic parameters plus parameters that are often adjusted when creating a configuration.
- Expert view—Shows basic and standard parameters plus parameters that are related to advanced features (such as features that involve multiple device types).

The name of the current view appears in the upper right corner of the MGR interface. To switch among basic, standard, and expert views, click



WARNING: Switching to a different view while creating a new configuration item will clear any parameters that you have already set for that item. Switching views while modifying an existing configuration item will not clear any of that item's settings.

An administrator sets your initial default view level when creating your account. You can change your default view level in **Settings ► My Preferences**.

3.5 Keyboard Shortcuts

The MGR supports the following keyboard shortcuts in the Microsoft Internet Explorer and Mozilla Firefox browsers.

Navigation Menu

Shortcut	Description
TAB	Highlight the next menu item
SHIFT + TAB	Highlight the previous menu item
ENTER	Expand/Collapse highlighted menu items
UP/DOWN ARROW	Scroll vertically up/down
CTRL + ALT + M	Move to the first menu item

Tabs

Shortcut	Description
TAB	Highlight the next field (including check boxes and form buttons)
SHIFT + TAB	Highlight the previous field (including check boxes and form buttons)
UP/DOWN ARROW	Scroll vertically up/down
SPACE BAR	Toggle check box value. In Statistics tables, pressing SPACE BAR will mimic the single-click option to select a row.
CTRL + ALT + T	Move to the first field in active tab
CTRL + ALT + N	Add new (if available)
CTRL + ALT + F	Move to the Filter/Search input field (if available)
CTRL + ALT + S	Save and close current tab
CTRL + ALT + R	Refresh active list
CTRL + ALT + A	Select all options (check boxes)
CTRL + ALT + U	Clear all options (check boxes)
CTRL + ALT + C	Cancel and close current tab
CTRL + ALT + X	Close all tabs
CTRL + ALT + PAGE UP	Move to previous tab
CTRL + ALT + PAGE DOWN	Move to next tab
ENTER	When a form button (for example, Save or Cancel) is highlighted, pressing ENTER will perform the action assigned to the button. When the cursor is in the Filter/Search input field, pressing ENTER will activate the Filter/Search. In Statistics tables, pressing ENTER will mimic the double-click option to view more detailed information of a certain row.
ESC	Cancel and close current tab

Drop-Down Lists

Shortcut	Description
UP/DOWN ARROW	Scroll vertically within a drop-down list
PAGE UP	Jump to the top of the currently displayed page in the drop-down list
PAGE DOWN	Jump to the bottom of the currently displayed page in the drop-down list
Any character key	In a drop-down list that contains a large number of entries, you can jump to the next entry in a alphabetical list by typing the first few characters of the desired entry. For example, if the drop-down list contains: <ul style="list-style-type: none"> Anaheim

Shortcut	Description
	<ul style="list-style-type: none"> • San Francisco • Santa Ana • Santa Barbara • Santa Claus <p>Typing "sant" will move the cursor to the "Santa Ana" entry.</p> <p>Note: If there is more than a one second delay between the typed characters, the system assumes that the next character is a new command. In other words, typing "s" and "a" with a long pause between the characters will cause the cursor to first jump to the "San Francisco" entry and then to the "Anaheim" entry.</p>

3.6 Filtering

You can filter a list of configuration items based on a letter, a number, a term, or a phrase. Filtering is case-sensitive and applies to:

- ID
- Name
- Priority (if applicable for the type of configuration item)
- Last updated date

The filter box appears at the upper right of the Manager interface.

Note: Filtering only applies to the fields that are currently visible. Some fields might not be visible, depending on the current view (see [Views](#)).

3.6.1 Filtering a List

To filter a list of items:

1. Enter a filter term in the filter box.
2. Click



If the filter term matches one or more items in the list, they appear. If the term does not match an item in the list, an error message appears.

3.6.1.1 Filtering Example

The following is an example of the external condition (EC) applications tab with no filter applied.



ID	ST	Name	Last Updated	Action
1	→	PBC 1	2009-10-02 15:01:21	<input type="checkbox"/>
2	↔	PBC 2	2009-10-02 15:01:35	<input type="checkbox"/>
3	→	XS-SPA	2009-10-02 15:02:44	<input type="checkbox"/>
4	↔	XS-MOD	2009-10-02 15:07:28	<input type="checkbox"/>
5	→	PBC 3	2009-10-02 15:17:09	<input type="checkbox"/>
6	→	XS-DIL	2009-10-02 15:17:23	<input type="checkbox"/>

Figure 9: Example with no filter applied

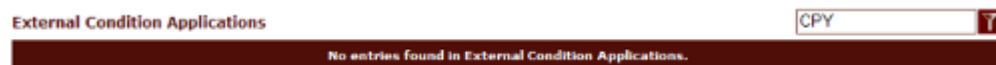
Now, the EC applications are filtered so only applications containing “PBC” appear.



ID	ST	Name	Last Updated	Action
1	→	PBC 1	2009-10-02 15:01:21	<input type="checkbox"/>
2	↔	PBC 2	2009-10-02 15:01:35	<input type="checkbox"/>
5	→	PBC 3	2009-10-02 15:17:09	<input type="checkbox"/>

Figure 10: Example with filter applied

If no item in the list matches the filter, an error message appears.




ID	ST	Name	Last Updated	Action
No entries found in External Condition Applications.				

Figure 11: Example with filter applied and no results

3.6.2 Removing a Filter

To remove a filter:

1. Clear the filter box.
2. Do one of the following:
 - a) Click 
 - b) Click **Refresh**.

The complete, un-filtered list of items appears.

3.7 Searching

To search for items across the entire MGR configuration:

1. Click **Search** in the upper right corner of the interface.
The Search tab appears.
2. Select a category from the first list.
Based on your selection, a box or a second list appears.
3. If a box appears, enter a letter, number, term, or phrase and continue with step 6.
If a list appears, select an attribute from the list. A list of conditions and a box appear.

4. Select a condition from the third list:

- Equal to
- Less than or equal to
- Greater than or equal to
- Less than
- Greater than
- Not equal to
- Contains

You may also be able to select a check box; for example, if the first list is set to **Devices** and the second list is set to **Allow Connection**. If you select the check box, the MGR will search for devices in which the **Allow Connection** property is selected. If you do not select the check box, the MGR will search for devices in which the **Allow Connection** property is not selected.

5. Enter a letter, number, term, or phrase in the fourth box.

6. To search:

- With only one criterion, click **Search**.
- With multiple criteria, click **AND** or **OR** and add another criterion (or multiple other criteria), and then click **Search**.

When you search with the **AND** operator, you can only search within a single category.

Search Criteria

MO Routing Rules	Name	Contains	SMSC	AND
MO Routing Rules	--Select Attribute--	AND OR		
MO Routing Rules				

Reset Search

Figure 12: Searching with the AND operator

When you search with the **OR** operator, you can search across multiple categories.

Search Criteria

MO Routing Rules	Name	Contains	SMSC	OR
All (common fields only)		AND OR		
All (common fields only)				
AO Counting Rules				
AO External Conditions				
AO Modifiers				
AO Routing Rules				
AT Counting Rules				
AT External Conditions				
AT Routing Rules				
Advanced Filters				
Application Categories				
Application Groups				
Applications				
Billing Profiles				
CLI Source Address List				
Countries				
Devices				
Domains				
EC Applications				
Event Logging Profiles				
External Attributes				

Reset Search

Figure 13: Searching with the OR operator

At any time, to clear all criteria that you have added, click **Reset**.

Note: After searching, you can filter search results in the same way that you filter items in a list.

Note: All items created in the Manager use index numbers. Index numbers are unique numbers within the item category. Though after deletion of an entry the index number is re-used when a new item is created. *Searches on index number are therefore not recommended*, as incorrect results can be returned. System users should therefore search on the item name value.

3.7.1 Taking Action on Search Results

To take action on search results, such as activating or deleting items, you can:

- Select the item(s) by clicking the check box in its row, and then select the desired action from the **Action** menu
- Right-click a single item, and then select the desired action from the context menu

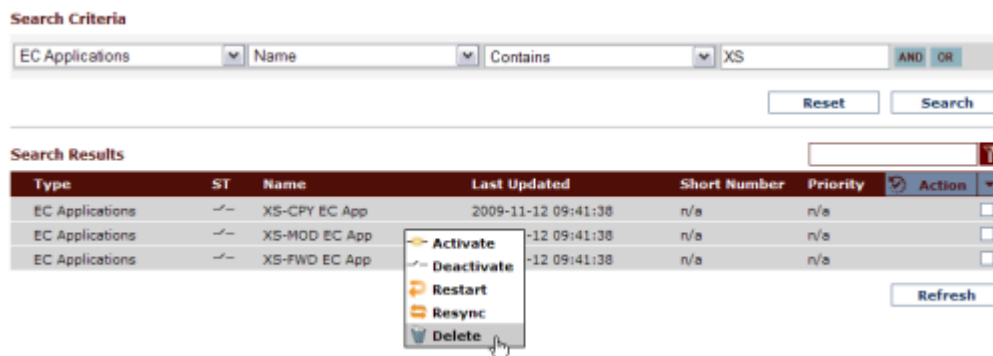


Figure 14: Context menu for search results

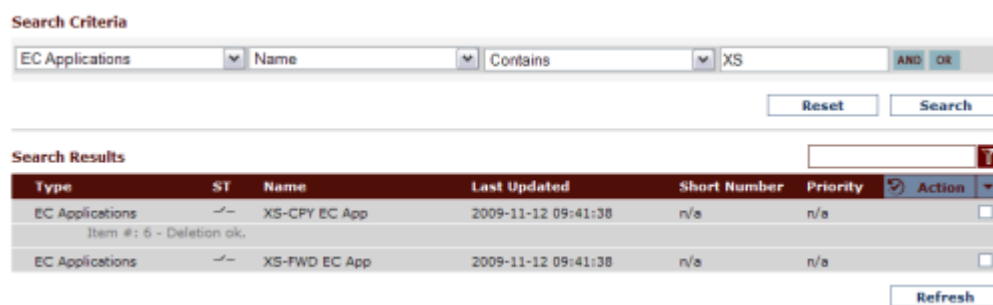


Figure 15: Result of action selected from context menu

To refresh the Search Results view after you have taken action on an item(s), click **Refresh**.

3.8 Overviews

Overviews provide information about the relationships among configuration items.

3.8.1 Overview Types

Overviews are available for the following categories of items:

- Routing
- SMS applications
- Environment

3.8.1.1 Routing

Overviews are available to compare the following items to routing rules:

- Countries
- Networks
- Applications
- Categories
- Groups
- External applications
- Service classes
- SS7 SMSCs
- SMSC groups
- Service centers
- Outside listeners
- Lists
- Modifiers
- Application-originating (AT) modifiers
- Mobile-originating (MO) modifiers
- Incoming mobile-terminating (MTI) modifiers
- Outgoing mobile-terminating (MTO) modifiers
- Billing profiles
- Logging profiles

3.8.1.2 SMS Applications

Overviews are available to compare the following items to SMS applications:

- Groups
- Categories
- CIMD tariff classes
- CIMD tariff class descriptions
- Service classes

3.8.1.3 Environment

An overview is available to compare SMSC groups to SMSCs.

3.8.2 Using Overviews

To use an overview:

1. Expand a category in the left navigation bar and click **Overviews**.
The Overviews tab appears.
2. Select a type of overview from the **Select Overview Type** list and click **Show**.
The overview appears. If data is not available for the overview type, an error message appears.
3. To see more information about an item in the overview list, click the item to expand it.
4. To view a specific item, click it.
The item opens in a new tab.

To close the Overviews tab, click **Cancel**.

3.9 Action and Context Menus

Use the **Action** and context (right-click) menus to take action on configuration items. You can use the **Action** menu to take action on one or more items and use the context menu to take action on a single item.

3.9.1 Available Actions

The actions that are available in the Action and right-click menus depend on whether you are working in a:

- MGR tab—Tab that you reach by clicking an item in the left navigation bar
- Search results tab—Tab that appears after you search

When you are working in a MGR tab, the available actions are:

- Action menu:
 - Activate
 - Deactivate
 - Restart (if BAT is installed)
 - Copy
 - Resync
 - Delete
 - Select All
 - Deselect All
- Context menu:
 - Activate
 - Deactivate
 - Restart (if BAT is installed)
 - Copy
 - Resync

- Delete

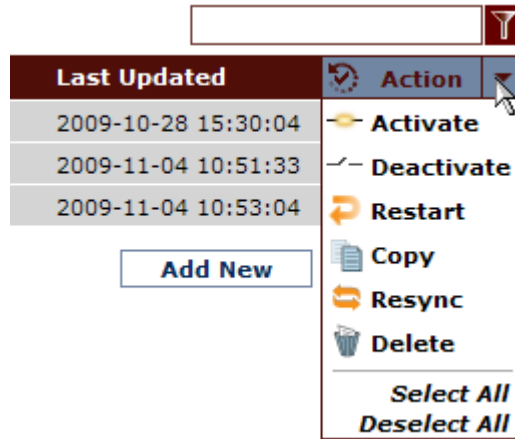


Figure 16: Action menu, MGR tab (with BAT installed)

When you are working in the search results tab, the available actions are:

- Action menu:
 - Activate
 - Deactivate
 - Restart
 - Resync
 - Delete
- Context menu:
 - Activate
 - Deactivate
 - Restart
 - Resync
 - Delete

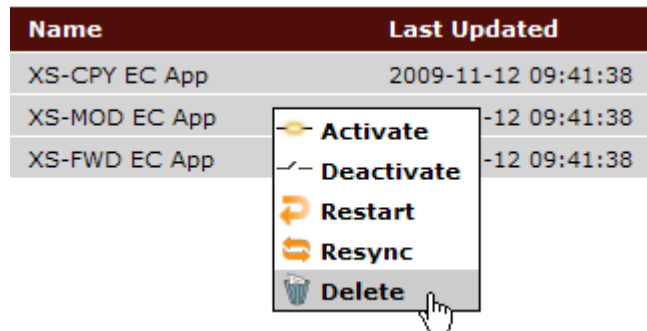


Figure 17: Context menu, search results

3.9.2 Activate

You must activate configuration items before you can use them in the system. The



icon indicates that an item is inactive.

To activate a configuration item:

1. Select the item by clicking the check box in its row.
2. From the **Action** menu, select **Activate**.

The item is activated and the icon changes to



3.9.3 Deactivate

You must deactivate configuration items before you can delete them from the MGR. The



icon indicates that an item is active.

To deactivate a configuration item:

1. Select the item by clicking the check box in its row.
2. From the **Action** menu, select **Deactivate**.

The item is deactivated and the icon changes to



3.9.4 Copy

To copy a configuration item:

1. Select the item by clicking the check box in its row.
2. From the **Action** menu, select **Copy**.

A new tab opens for the new configuration item with settings based on the exiting item.

3.9.5 Restart

Use the **Restart** action to restart Batch Server (BAT) batch jobs.

The **Restart** action is only available in the **Action** and context menus for MGR tabs when BAT is installed. It is always present in the menus for search results.

To restart a batch job:

1. Select the batch job by clicking the check box in its row.
2. From the **Action** menu, select **Restart**.

The MGR restarts the batch job.

3.9.6 Resync

The MGR's resync process compares the MGR's database to a configuration item's online SNMP configuration and corrects it, if necessary. Synchronization issues can be recognized by SNMP errors displayed in the MGR Web interface.

If the resync is started on a:

- Configuration item, then the MGR will try and set every configurable attribute for that configuration item on each device.
- Device, then the MGR will try and execute in order all the failed settings for that device. This happens automatically during reconnection if a device has been unreachable for a while.

Synchronization can require a significant amount of time, depending on the size of your configuration (especially if you want to synchronize several devices at one time). An alternative, faster method to synchronize all device configurations with the MGR is to stop and restart each device. In a redundant configuration, devices can be stopped and started one at a time, to prevent service interruption. If there are many SNMP errors, the best remedy may be to stop and restart the device.

To resync a configuration item:

1. Select the item by clicking the check box in its row.
2. From the **Action** menu, select **Resync**.

The MGR begins to resynchronize the configuration item and the operational state changes to



After the MGR finishes synchronizing and the device polling interval (as set in **Settings > Global Settings**) has passed, the operational state changes to



3.9.6.1 Resync System Log Errors

During synchronization, the `tp_mgr_poll` process may report messages such as the following in the system log:

```
Received noSuchName(2) error-status at error-index 1
```

These messages occur when the `tp_mgr_poll` process attempts to locate objects that do not exist on the device being polled. Such messages are normal.

Note: The system log is located at `/var/log/messages`.

3.9.7 Delete

To delete a configuration item:

1. Ensure that the item is not associated with any active rule.
Use the overview for the type of item to verify that the item is not associated with an active rule.
2. If the item is active, deactivate it.
3. Select the item by clicking the check box in its row.
4. From the **Action** menu, select **Delete**.

A message appears, asking you to confirm that you want to delete the item.

5. Click **OK** to confirm the deletion or click **Cancel** to cancel the deletion and return to the list of items.

3.9.8 Limitations

The limitations on the **Action** and context menus are:

- If you search and the results span multiple pages, you can only take action on items that are on the current page. For example, if you select two items, progress to the next page of search results, select three more items, and then click select **Delete** from the **Action** menu, the MGR will only delete the three items that are on the current page.
- If a rule is tied to an SMS application, you must deactivate the rule before you can deactivate the application.
- If a routing rule is assigned to an SMSC (SS7) or a service centre (IP) and you deactivate the rule, you cannot deactivate the SMSC or service centre until you remove it from the **SMSC Assignment** section of the rule's properties.
- Users will get the notification message “**Configuration synching currently in progress, hence updates are not allowed. Please try after some time**” while performing the actions (Activate, Deactivate, Restart, Resync and Delete) with the ‘**Select All**’ option.

Note: This notification message will not appear in case no device is associated with the relevant configuration.

3.10 Printing Screens

To print a currently displayed tab or overview, navigate to the **Print** (CTRL+P) or **Print Preview** option of your browser. The screen is automatic nicely fitted on 'US Letter' format, which also fits on an 'A4' format printout.

3.11 Considerations

While doing the configurations, the following points should be taken into consideration:

- Before saving the configuration in the database, the MGR removes the leading and trailing whitespaces from the text entered in the textarea input field. In this case, the whitespaces are not visible in the textarea, and are also not saved in the database.
- For input fields with text boxes, the MGR removes the leading and trailing whitespaces. In this case, the user is not able to view the whitespaces in the text boxes, but can view them in the database.

3.12 Trap Service

Up to eight SNMP Managers can subscribe to the trap service. When a trap condition occurs, the MGR sends an SNMP trap to any SNMP Management Station that is subscribed to the trap service. To subscribe an SNMP Manager to the trap service, add an entry to the 'Alarm Station' table that contains:

- An IP address (IPv4 or IPv6) or Hostname of the SNMP Manager.
- A UDP port number to which SNMP traps should be sent for that particular SNMP Manager.

The 'Alarm Station' table is also SNMP manageable; refer to the TEXTPASS-GEN MIB for more information about this table.

The MGR always originates SNMP traps from 14362 UDP port and terminates them in the UDP ports that are specified in the 'Alarm Station' table. The community string that the MGR specifies in SNMP traps is always equal to public.

The MGR uses an SMNP trap daemon to log generated SNMP traps locally in `/var/log/messages`. The daemon uses 11173 UDP port by default.

Note:

1. If 'snmpPropAlarmOwnIpv6Address' parameter in semi-static configuration file is set to valid IPv6 address or hostname, then specified address is used as source address for sending SNMP traps to SNMP Manager with address of type IPv6.
2. If 'snmpPropAlarmOwnIpAddress' parameter in semi-static configuration file is set to valid IPv4 address, then specified address is used as source address for sending SNMP traps to SNMP Manager with address of type IPv4.
3. 'ipaddress' parameter in semi-static configuration file is used as an agent address. If this parameter is not configured then local address is used as agent address.

Chapter 4

Routing

Topics:

- *Introduction.....50*
- *Prerequisites for Applicable Rules.....50*
- *Routing Rule Condition Formats.....50*
- *Creating Routing Rules.....52*
- *Creating External Condition Rules.....145*
- *Creating Counting Rules.....155*
- *Defining External Condition Applications.....155*
- *Creating Modifiers.....164*
- *Creating Lists.....173*
- *Creating Auto Black List Entries.....177*
- *Defining Routing Numbers.....178*
- *Creating Application Load Balancing Groups..180*
- *Creating Address Conversion Rules.....181*
- *Configuring Routing Schedules.....187*
- *Configuring Routing Properties.....188*
- *Configuring Unicode Conversion Table.....189*
- *Configuring Mobile Number Portability.....192*
- *Configuring Message Template.....193*

4.1 Introduction

The Router (RTR) can route SMS traffic from anywhere to virtually everywhere. The RTR provides weighted load distribution and throughput control to reduce SMS bottlenecks. The RTR's highly flexible and configurable rule engine is responsible for routing SMS traffic.

Routing settings are configured via the **Routing** menu in the MGR.

4.2 Prerequisites for Applicable Rules

The logging profile can be applied to all routing rules except the SRI-SM response (SRIP) and internally generated message (IGM) routing rules.

Before you create routing, external condition (EC) routing, and counting rules, you should create the other items that you will use to configure the rules' logic. Although you can create rules without these items, they are prerequisites for taking advantage of the advanced routing features. In this chapter, each type of rule includes a list of the prerequisite items that you can use to create rule logic.

Note: The logging profile cannot be applied to MTIX (Mobile Terminating External Conditions) and MTIC (Mobile Terminating Counting) rules.

The following items are common prerequisites for all types of rules:

- Country
- Device
- List
- Logging profile
- Network

4.3 Routing Rule Condition Formats

Many routing rule conditions can have different formats. The available formats are:

Format	Description	Matches when...
Application	An SMS application entity.	The pertaining address field in the message exactly matches the application's short number.
Country	A country entity. If it is required, the message's address field is converted to international format before the matching process takes place.	The pertaining address field in the message begins with the E164 country code of the country.

Format	Description	Matches when...
IMSI prefix	An IMSI prefix, specified by zero to 15 digits, followed by an asterisk (for example "20420*"). Note: Note: The IMSI may not always be available in the message.	The IMSI is known and the specified digits match the starting digits of the IMSI. Note that if the IMSI is unknown and the IMSI prefix condition is negated, the condition will evaluate to TRUE.
IMSI range	An IMSI range, specified in international format (for example, 204204004000-204204005000). Note: The IMSI may not always be available in the message.	The pertaining address field in the message falls within the specified range.
MSISDN prefix	The prefix of a single MSISDN, specified in international format, excluding the international prefix 00 (for example, 316123). The prefix can be up to 15 digits in length. If it is required, the message's address field is converted to international format before the matching process takes place.	The first part of the pertaining address field in the message exactly matches the specified prefix.
MSISDN range	An MSISDN range. The first MSISDN and the last MSISDN must have the same number of digits and must be encoded in international format, excluding the international prefix 00. If it is required, the message's address field is converted to international format before the matching process takes place.	The pertaining address field in the message falls within the specified range.
Network	A network entity. If it is required, the message's address field is converted to international format before the matching process takes place.	The pertaining address field in the message falls within one of the number ranges or is part of one of the network prefixes specified for the network entity.
Short number prefix	The prefix of a single short number, specified as an E164 address with a TON of unknown, national, or international (that is, 123). The prefix can be up to 14 digits in length. Note: Conditions for a single short number, a short number range, and a short number prefix can be combined in a list. However, short number prefixes cannot be combined with any other type of condition.	The pertaining destination field in the message exactly matches the specified short number.

Format	Description	Matches when...
Short number range	A short number range. The first short number and the last short number must have the same number of digits.	The pertaining address field in the message falls within the specified range.
Single IMSI	A single IMSI, specified in international format (for example, 2041245454545). Note: The IMSI may not always be available in the message.	The pertaining address field in the message exactly matches the specified IMSI.
Single MSISDN	A single MSISDN, specified in international format, excluding the international prefix 00 (for example, 31653123456). If it is required, the message's address field is converted to international format before the matching process takes place.	The pertaining address field in the message exactly matches the MSISDN specified in the condition format.
Single short number	A single short number.	The pertaining destination field in the message exactly matches the specified short number.

4.4 Creating Routing Rules

The RTR uses routing rules to route SMS traffic to a variety of destinations. The types of routing rules are:

- Mobile-originating routing rules (MOR)
- SRI-SM request routing rules
- SRI-SM response routing rules
- Incoming mobile-terminating routing rules (MTIR)
- Outgoing mobile-terminating routing rules (MTOR)
- Application-originating routing rules (AOR)
- Incoming application-terminating routing rules (ATIR)
- Outgoing application-terminating routing rules (ATOR)
- Internally generated message routing rules (IGMR)

The MGR automatically assigns an index to each rule when it is created. When you use the `tp_walk` command-line tool to view rule-related counters, the index indicates which rule applies. For example, `moRtgRuleAppliedCounter.3` provides the number of times that the MO routing rule with index 3 was applied.

Note: In the MIB, MTOR rules are called MTR rules and ATOR rules are called ATR rules.

4.4.1 Creating an MO Routing Rule

Prerequisites:

- AMS queue

- Application
- Application load balancing group
- Billing profile
- Device
- External attribute
- Modifier
- Routing number group
- SMSC

To create a mobile-originating routing (MOR) rule:

1. In the left navigation bar, select **Routing ► Routing Rules ► MOR**.
The Mobile Originating Routing Rules tab appears.
2. Click **Add New**.
A new Mobile Originating Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The MOR rule with the highest priority is evaluated first.
6. Set conditions for the rule.
7. From the **Action** list, select a routing action for the rule.
If an MO message does not match any rule, the RTR discards the message and returns a NACK to the originator.
8. Set the parameters for the routing action, if required.
9. Optionally select a log profile from the **Log Profile** list.
10. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
11. Click **Save**.
The MGR creates the rule and closes the tab.
12. Activate the rule.

4.4.1.1 MO Rule Conditions

The following table details the conditions that are available for MO rules.

Condition	Values	Description
Time Schedule	<ul style="list-style-type: none"> • Always • Schedule 	Condition on the evaluation time of the message: <ul style="list-style-type: none"> • Always: The condition is always true. • Schedule: The condition is true if the current time falls within the schedule as specified by the selected routing schedule, defined in Routing ► Schedules.
Recipient TON	<ul style="list-style-type: none"> • None 	Type of number (TON) specified in the recipient address of the message.

Condition	Values	Description
	<ul style="list-style-type: none"> • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	
Originator	<ul style="list-style-type: none"> • MSISDN • MSISDN range • MSISDN prefix • Country • IMSI Prefix • IMSI range • IMSI • List 	<p>Originator specified in the message.</p> <p>Note: When an IMSI-related condition is used but the originator IMSI is not known at the moment of rule evaluation, the condition will evaluate to FALSE if not negated or TRUE if negated. To ensure that the originator IMSI is always retrieved before the rule evaluation, set the <code>alwaysretrieveoriginatorimsi</code> attribute in the common configuration file to true.</p>
Recipient	<ul style="list-style-type: none"> • MSISDN • MSISDN range • MSISDN prefix • Country • IMSI prefix • IMSI range • IMSI • List • Short number • Short number range • Short number prefix • Application • Network • Alphanumeric 	<p>Recipient specified in the message.</p> <p>Note: When an IMSI-related condition is used but the recipient IMSI is not known at the moment of rule evaluation, the condition will evaluate to FALSE if not negated or TRUE if negated. For MOR and MOX rules, this condition requires the recipient number to be an MSISDN and the HLR query to be performed before the rule evaluation (to obtain the recipient IMSI). The Early SRI-SM for MO/SM attribute in the (MGR Routing > Properties) controls when the HLR query is performed.</p> <p>Note: The Network configuration may include provisioned network number ranges and/or network prefixes.</p>
SMSC Address	<ul style="list-style-type: none"> • MSISDN • MSISDN range • MSISDN prefix • List 	SMSC address specified in the message.

Condition	Values	Description
Orig. MSC/SGSN	<ul style="list-style-type: none"> • MSISDN • MSISDN range • MSISDN prefix • List • Point code • Point code range • Country • Network 	<p>Originating MSC and/or SGSN specified in the message.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If global title (GT) routing is used and this condition is specified in terms of Point code or Point code range, then a non-inverted condition always evaluates to false and an inverted condition always evaluates to true. 2. If PC/SSN routing is used instead of GT routing and this condition is specified in terms of Country or Network, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer. 3. The Network configuration may include provisioned network number ranges and/or network prefixes.
Orig. MSC/SGSN Translation Type	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	<p>Translation Type specified in Originating MSC/SGSN Address.</p>
Terminating MSC/SGSN	<ul style="list-style-type: none"> • MSISDN • MSISDN Range • MSISDN Prefix • Country • Network • List 	<p>Destination MSC and/or SGSN. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before MO rule evaluation (to obtain the MSC and/or SGSN). The Early SRI-SM for MO/SM attribute in the MGR (Routing ► Properties) controls when the HLR query is performed. If both the MSC and SGSN are present, the <code>preferredmtdestination</code> attribute determines which will be used for rules evaluation. If the HLR query fails, the condition will evaluate to "false", whether it is a negative or positive condition.</p> <p>Note: The Network configuration may include provisioned network number ranges and/or network prefixes.</p> <p>Note: If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), The 'Preferred MT Destination' in the Network configuration overrides the semi-static attribute '<code>preferredmtdestination</code>' for the rules evaluation.</p>

Condition	Values	Description
SCCP Called Party Address	<ul style="list-style-type: none"> • MSISDN • MSISDN range • MSISDN prefix • List • Point code • Point code range • Country • Network 	<p>SCCP Called Party Address specified in the message.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If global title (GT) routing is used and this condition is specified in terms of Point code or Point code range, then a non-inverted condition always evaluates to false and an inverted condition always evaluates to true. 2. If PC/SSN routing is used instead of GT routing and this condition is specified in terms of Country or Network, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer. 3. The Network configuration may include provisioned network number ranges and/or network prefixes.
Called Party Translation Type	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	Translation Type specified in SCCP Called Party Address.
Orig. HLR	<ul style="list-style-type: none"> • MSISDN • MSISDN range • MSISDN prefix • List • Point code • Point code range • Country • Network 	<p>HLR that serves the message originator. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before MO rule evaluation (to obtain the HLR). The Early SRI-SM for MO/SM attribute in the MGR (Routing ► Properties) controls when the HLR query is performed.</p> <p>Note: The Network configuration may include provisioned network number ranges and/or network prefixes.</p>
User Data	<ul style="list-style-type: none"> • None • Full text • Text tag • Subtext (contains) • Text length 	<p>Content of the message:</p> <ul style="list-style-type: none"> • Full text: Compares the entire message content with a defined string. Only evaluates positively if there is an exact match with the user data (message content). • Text tag: Compares the first part of the message content with a defined tag-string. Only evaluates positively if the message starts exactly with the defined tag-string. Useful to define a rule on keywords (e.g. *LONG# for CMG SMSCs). • Subtext (contains): Compares if the message content contains a defined tag-string. To optimise the search, a start position (default 1) and an end

Condition	Values	Description
		<p>position (default 160) must be specified in which the string is to be found.</p> <p>Note: All message content scanning is case-insensitive.</p>
User Data Header	<ul style="list-style-type: none"> • None • Byte value 	<p>Value specified in one of the information element identifiers (IEIs) of the user data header (UDH) of the message. Only evaluates positively if there is an exact match with the information element identifier (00-FF, hexadecimal) of the UDH. Refer to technical specification 3GPP 23.040 for more information. Most common IEI values:</p> <ul style="list-style-type: none"> • 00: Concatenated short message • 01: Special SMS message indication • 04: Application port addressing scheme, 8-bit address • 05: Application port addressing scheme, 16-bit address • 06: SMSC control parameters • 07: UDH Source Indicator
Reply Path	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0: Off • 1: On 	Reply path bit in the message.
Status Report Request	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0: Off • 1: On 	Status report request bit in the message.
Protocol Identifier (PID)	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	Protocol ID specified in the message.
Data Coding Scheme (DCS)	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	Data coding scheme (DCS) specified in the message.

Condition	Values	Description
Recipient NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN/telephone numbering plan • 2: Reserved • 3: Data numbering plan (X.121) • 4: Telex numbering plan • 5: Service centre-specific plan • 6: Service centre-specific plan • 7: Reserved • 8: National numbering plan • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	Number plan identifier (NPI) specified in the recipient address of the message.
Ext Att	<ul style="list-style-type: none"> • None • External attributes 	A set of 32 attributes (defined in Routing ► EC Applications ► Attributes), the value of which can be controlled by external condition (EC) applications.
Recipient RN Group	<ul style="list-style-type: none"> • None • SNMP index 	Routing number (RN) group to which the RN in the recipient address belongs.
Recipient Query Result	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • Any permanent error • Any temporary error • Timeout • System failure • Data missing 	Result of the HLR query for the recipient. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before MO rule evaluation (to obtain the HLR query result). The Early SRI-SM for MO/SM Whitelist and Early SRI-SM for MO/SM attributes in the MGR (Routing ► Properties) control when the HLR query is performed.

Condition	Values	Description
	<ul style="list-style-type: none"> • Unexpected data value • Facility not supported • Unknown subscriber • Absent subscriber • Call barred • Teleservice not provisioned • TCAP aborted • SCCP aborted • MS deregistered • MS purged • Other errors 	
Originator SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual originator subscriber services (defined in SPF Services ► SPF Services). The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.
Recipient SSI	<ul style="list-style-type: none"> • None • Subscriber Services) 	Perform a positive or negative test on one or more individual recipient subscriber services. The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.
Message Segments	<ul style="list-style-type: none"> • None • Bit String <ul style="list-style-type: none"> • First Segment • Last Segment • Not First Nor Last 	Segment sequence number of a concatenated message.
SIP Header	<ul style="list-style-type: none"> • None • SIP Header 	<p>If set as "SIP Header", the sub-conditions will be matched against the SIP header received in the incoming SIP Originated message.</p> <p>Four sub-conditions can be provisioned. Please refer the section <i>MO Rule Conditions for SIP Originated Message</i> for configuring the sub-conditions.</p>

4.4.1.2 MO Routing Action Parameters

This section describes the parameters for MO routing actions.

Multiple MO Routing Actions

Parameter	Description	Default
Submission	Billing profile to use for submission; applies to all MO routing actions.	None
Successful Delivery	Billing profile to use when the routing action succeeds. Applies to: <ul style="list-style-type: none"> • Route to SMSC • Route to application • Route to MS fallback to SMSC • Discard with acknowledgment • Route to MS fallback to application • Route to MS fallback to storage • Route to application fallback to storage • Route to SMSC Group as AO • Route to MS fallback to SMSC Group as AO • Route to SMSC Application as AO • Route to MS fallback to SMSC Application as AO 	None
Failed Delivery	Billing profile to use when the routing action fails. Applies to: <ul style="list-style-type: none"> • Route to SMSC • Route to application • Route to MS fallback to SMSC • Discard with acknowledgment • Route to MS fallback to application • Route to MS fallback to storage • Route to application fallback to storage • Route to SMSC Group as AO • Route to MS fallback to SMSC Group as AO • Route to SMSC Application as AO • Route to MS fallback to SMSC Application as AO 	None
Delivery Notification	Billing profile to use for delivery notification. Applies to: <ul style="list-style-type: none"> • Route to SMSC • Route to application 	None

Parameter	Description	Default
	<ul style="list-style-type: none"> Route to MS fallback to SMSC Discard with acknowledgment Route to MS fallback to application Route to MS fallback to storage Route to application fallback to storage Route to SMSC Group as AO Route to MS fallback to SMSC Group as AO Route to SMSC Application as AO Route to MS fallback to SMSC Application as AO 	
Billing for Discarded Messages	Billing profile to use for Discarded messages Applies to: <ul style="list-style-type: none"> Discard with negative acknowledgement. Discard without response. 	None
Return Message	Return Message template to use for this discarded messages Applies to: <ul style="list-style-type: none"> Discard with negative acknowledgement. Discard without response. 	None

Route to SMSC and Route to MS, Fallback to SMSC

Parameter	Description	Default
SMSC Assignments	SMSC(s) to which this rule applies.	None
Priority	Priority of the SMSC (between 1 and 100).	50
Weight	Relative weight of messages to send to the SMSC (for example, an SMSC with a weight of 2 will receive twice as many messages as an SMSC with a weight of 1).	1
Throughput	Throughput for the SMSC (messages per second); if set to 0, throughput will be unlimited.	10,000
CdPA Based Forwarding	Enables forwarding based on the SCCP called party address (CdPA) of received messages; if enabled, the MOR rule not be associated with any provisioned SMSC.	False
Keep MSC/SGSN SCCP CdPA	Enables transparent routing: <ul style="list-style-type: none"> False: The RTR will start a new TCAP dialogue when forwarding messages to the external SMSC. 	Use global setting

Parameter	Description	Default
	<ul style="list-style-type: none"> • True: The RTR will reuse the existing TCAP dialogue when forwarding messages to the external SMSC. • Use global setting: The RTR will use the value of the <code>optimisedmorouting</code> parameter in its semi-static configuration file (which defaults to "false"). 	
Modifier	Modifier to apply to the message.	None

Route to Application

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application Selection	<p>Controls how the destination application is to be determined:</p> <ul style="list-style-type: none"> • Specify Application: The destination application is an application specified by the routing rule itself, by means of the Application parameter. • Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. • Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match. 	Specify Application
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None

Parameter	Description	Default
Decimation	Controls how many messages must be delivered to the application.	1/1

Store for Delivery to MS

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue

Route to MS

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None

Route to MS, Fallback to Application

Parameter	Description	Default
Application Selection	<p>Controls how the destination application is to be determined:</p> <ul style="list-style-type: none"> Specify Application: The destination application is an application specified by the routing rule itself, by means of the Application parameter. Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match. 	Specify Application

Parameter	Description	Default
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds.	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

Route to MS, Fallback to Storage

Parameter	Description	Default
Modifier	Modifier to apply to the message	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

Store for Delivery to Application

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
Application Selection	<p>Controls how the destination application is to be determined:</p> <ul style="list-style-type: none"> Specify Application: The destination application is an application specified by the routing rule itself, by means of the Application parameter. Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the 	Specify Application

Parameter	Description	Default
	SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match.	
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue

Route to Application, Fallback to Storage

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application Selection	Controls how the destination application is to be determined: <ul style="list-style-type: none"> Specify Application: The destination application is an application specified by the routing rule itself, by means of the Application parameter. Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match. 	Specify Application
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application").	First application on the list

Parameter	Description	Default
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue
Decimation	Controls how many messages must be delivered to the application.	1/1
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

Route to SMSC Group as AO

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application"). The application must have a session model of Inside only - All SCs or Inside only - SC List .	None
SMSC Load Balancing Group	SMSC group to which to route the MO message.	None

Route to MS, Fallback to SMSC Group as AO

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application"). The application must have a session model of Inside only - All SCs or Inside only - SC List .	None
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds.	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None
SMSC Load Balancing Group	SMSC group to which to route the MO message.	None

Route to SMSC Application as AO

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application"). The application must have a session model of Inside only - All SCs or Inside only - SC List .	None

Route to MS, Fallback to SMSC Application as AO

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when Application Selection is set to "Specify Application"). The application must have a session model of Inside only - All SCs or Inside only - SC List .	None
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds.	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

4.4.2 Creating an SRI-SM Request Rule

To create an SRI-SM Request rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **SRI-SM Req.**. The SRISM Request Routing Rules tab appears.
2. Click **Add New**. A new SRISM Request Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box. The priority must be between 0 (lowest) and 99 (highest); the default is 50. The SRI-SM Request rule with the highest priority is evaluated first.
6. Set the conditions for the rule.
7. Enter the rule matching ratio in the **Rule Matching Ratio** box.
8. From the **Action** list, select a routing action for the rule.
9. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
10. Click **Save**.

The MGR creates the rule and closes the tab.

11. Activate the rule.

4.4.2.1 SRI-SM Request Rule Conditions

The SRI-SM Request rule set supports conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received SRI-SM request, but is evaluated against the time at which the rule is evaluated.
Originator	General	This condition is evaluated against the address included in the SRI-SM request's optional RP-SMEA parameter. When the parameter is absent, but this condition is specified, the condition evaluates to false if not inverted and to true if inverted.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the normalised MSISDN, if the RP-SMEA address is categorized as MSISDN.
	Single short number, short number range, or short number prefix	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes, if the RP-SMEA address is categorized as MSISDN. ¹
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs, if the RP-SMEA address is categorized as MSISDN. This enables logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a TON of "unknown"; otherwise, it evaluates to false.

¹ In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a NPI of "unknown"; otherwise, it evaluates to false.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified. If the originator is not available, or if it is not categorized as MSISDN, the SSI will be empty (no services).
Recipient	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the MSISDN received at the MAP layer of the SRI-SM request. It refers to the recipient of the subsequent MT messages.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the received MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the MSISDN against the provisioned mobile network number ranges and/or network prefixes. ²
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the received MSISDN against a list of MSISDNs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.

² In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the SMSC address received at the MAP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
SCCP Calling Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Calling Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. Note: If PC/SSN routing is used instead of GT routing then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. Note: <ol style="list-style-type: none">1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true.2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Calling Party Translation Type	• None	Translation Type specified in SCCP Calling Party Address received in the SRI-SM request.

Condition	Format	Description
	<ul style="list-style-type: none"> Byte value (value between 00 and FF, hexadecimal) 	
SCCP Called Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Called Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	<p>This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries.</p> <p>Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.</p>
	Network	<p>This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes.</p> <p>Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.</p>
	List	This condition evaluates the Called Party address received at the SCCP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	<p>This condition evaluates the PC included in Called Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range.</p> <p>Note:</p> <ol style="list-style-type: none"> If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Called Party Translation Type	<ul style="list-style-type: none"> None Byte value (value between 00 and FF, hexadecimal) 	Translation Type specified in SCCP Called Party Address received in the SRI-SM request.

Condition	Format	Description
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that issued the SRI-SM request. Refer to the Firewall Guide for information about how this categorization is done.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs. If there is a match, the recipient is considered to be a portable application.

4.4.2.2 SRI-SM Request Rule Matching Ratio

The SRI-SM Request **Rule Matching Ratio** parameter enables you to provision a matching fraction. This is a fraction of two integers, M and N; N must be equal to or greater than M, and both integers must be between 1 and 9999. The matching fraction causes the rule to:

- Only match M out of N times
- Not match N minus M of N times

Non-matching due to the matching fraction only occurs if all other provisioned conditions evaluate to true.

4.4.2.3 SRI-SM Request Rule Routing Action

The sole effect of the evaluation of the SRI-SM Request rule set is that the RTR applies the resulting routing action to the SendRoutingInfoForSm operation. The possible actions are:

Action	Effect
Send to HLR	Send the SRI-SM request to the RTR's outbound SRI-SM request processing, with the intent to forward the SRI-SM to the HLR in such a way that the response will be routed back to the RTR (using a new TCAP dialogue).
Discard with temporary error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for temporary errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute <code>mttemporarydiscarderrorforhlr</code> . In this case, the SRI-SM Response rule set is not evaluated.
Discard with permanent error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for permanent errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute <code>mtpermanentdiscarderrorforhlr</code> . In this case, the SRI-SM Response rule set is not evaluated.
Discard with no response	Drop the SRI-SM request, without sending a response back to the external SMSC. In this case, the SRI-SM Response rule set is not evaluated.
Accept and respond to SMSC immediately	Do not send the SRI-SM request on to the RTR's outbound SRI-SM request processing, but proceed with the evaluation of the SRI-SM response rules.
Have HLR respond to SMSC directly	Send the SRI-SM request to the RTR's outbound SRI-SM request processing, with the intent to relay the SRI-SM to the HLR in such a way that the

Action	Effect
	response will be routed directly back to the external SMSC (using the same TCAP dialogue). In this case, the SRI-SM Response rule set is not evaluated.

4.4.3 Creating an SRI-SM Response Rule

To create an SRI-SM Response rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **SRI-SM Resp..**
The SRI-SM Response Routing Rules tab appears.
2. Click **Add New**.
A new SRI-SM Response Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The SRI-SM Response rule with the highest priority is evaluated first.
6. Set the conditions for the rule.
7. Enter the rule matching ration in the **Rule Matching Ratio** box.
8. From the **Action** list, select a routing action for the rule.
9. Set the parameters for the routing action, if required.
10. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
11. Click **Save**.
The MGR creates the rule and closes the tab.
12. Activate the rule.

4.4.3.1 SRI-SM Response Rule Conditions

The SRI-SM Response rule set supports conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received SRI-SM request or response, but is evaluated against the time at which the rule is evaluated.
Originator	General	This condition is evaluated against the address included in the SRI-SM request's optional RP-SMEA parameter. When the parameter is absent, but this condition is specified, the condition evaluates to false if not inverted and to true if inverted.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN.

Condition	Format	Description
	Single short number, short number range or short number prefix	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes, if the RP-SMEA address is categorized as MSISDN ³ .
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs if the RP-SMEA address is categorized as MSISDN. This enables logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a TON of "unknown"; otherwise, it evaluates to false.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a NPI of "unknown"; otherwise, it evaluates to false.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified. If the originator is not available, or if it is not categorized as MSISDN, the SSI will be empty (no services).
Recipient	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the MSISDN received at the MAP layer of the SRI-SM request. It refers to the recipient of the subsequent MT messages.

³ In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the received MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the MSISDN against the provisioned mobile network number ranges and/or network prefixes ⁴ .
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the "real" IMSI for the recipient of the subsequent MT messages, as returned by the HLR or retrieved from the portable application provisioning data. If no "real" IMSI is available, the condition evaluates to false if not inverted and to true if inverted.
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the received MSISDN against a list of MSISDNs or the recipient IMSI against a list of IMSIs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the SMSC address received at the MAP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.

⁴ In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
Dest. MSC or SGSN	General	<p>This condition is evaluated against the MSC or SGSN address as returned by the HLR. If the HLR returns both addresses, the rule set is evaluated against either the MSC or the SGSN address, as selected by the semi-static attribute <code>preferredmtdestination</code>. If neither an MSC nor SGSN address is available when the SRI-SM Response rule set is evaluated, a non-inverted condition evaluates to false and an inverted condition evaluates to true.</p> <p>Note: If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), The 'Preferred MT Destination' in the Network configuration overrides the semi-static attribute '<code>preferredmtdestination</code>' for the rules evaluation.</p>
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the selected MSC or SGSN address received at the MAP layer of the SRI-SM response from the HLR.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the selected MSC or SGSN address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the selected MSC or SGSN address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the selected MSC or SGSN address against a list of E.164 numbers. This enables logical OR operation.
SCCP Calling Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Calling Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	<p>This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries.</p> <p>Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.</p>

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. Note: 1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. 2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Calling Party Translation Type	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	Translation Type specified in SCCP Calling Party Address received in the SRI-SM request.
SCCP Called Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Called Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Called Party address received at the SCCP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Called Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. Note: 1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. 2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Called Party Translation Type	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	Translation Type specified in SCCP Called Party Address received in the SRI-SM request.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that issued the SRI-SM request. Refer to the Firewall Guide for information about how this categorization is done.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs. If there is a match, the recipient is considered to be a portable application.

4.4.3.2 SRI-SM Response Rule Matching Ratio

The SRI-SM Response **Rule Matching Ratio** parameter enables you to provision a matching fraction. This is a fraction of two integers, M and N; N must be equal to or greater than M, and both integers must be between 1 and 9999. The matching fraction causes the rule to:

- Only match M out of N times
- Not match N-M of N times

Non-matching due to the matching fraction only occurs if all other provisioned conditions evaluate to true.

For example, to Home-Route only 30% of the Home-Routable messages, all SRI-SM Response rules with the "Home Route" action should have a **Rule Matching Ratio** of 3/10.

4.4.3.3 SRI-SM Response Rule Routing Action

The primary effect of evaluating the SRI-SM Response rule set is that the RTR determines whether subsequent MT messages should be Home Routed or not, which is implemented through the matching SRI-SM rule's routing action. The possible actions are:

Action	Effect
Home Routing	Return a successful SRI-SM response to the external SMSC so that when the returned routing data is used, subsequent MT messages will be routed to the RTR. A rule with this action can only match if: <ul style="list-style-type: none"> • A real IMSI is available (from the HLR or the portable application provisioning data), or • The rule specifies a range of IMSIs from which an IMSI can be generated
Discard with temporary error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for temporary errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute <code>mttemporarydiscarderrorforhlr</code> .
Discard with permanent error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for permanent errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute <code>mtpermanentdiscarderrorforhlr</code> .
Discard with no response	Drop the SRI-SM request, without sending a response back to the external SMSC.
No Home Routing	Return a successful SRI-SM response to the external SMSC that includes the IMSI and MSC and/or SGSN address as returned by the HLR. This causes the SMSC to direct subsequent MT delivery attempts for that recipient directly to the MSC or SGSN. A rule with this action can only match if the RTR successfully queried the HLR previously, so there is real routing data to return to the external SMSC.

4.4.4 Creating an Incoming MT Routing Rule

Prerequisites:

- Billing profile
- External attribute
- Modifier
- SMSC group

To create an incoming mobile-terminating routing (MTIR) rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **MTIR**.
The Incoming Mobile Terminating Routing Rules tab appears.
2. Click **Add New**.
A new Incoming Mobile Terminating Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The MTIR rule with the highest priority is evaluated first.
6. Set conditions for the rule.
7. From the **Action** list, select a routing action for the rule.
8. Set the parameters for the routing action, if required.
9. Optionally select a log profile from the **Log Profile** list.
10. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
11. Click **Save**.
The MGR creates the rule and closes the tab.
12. Activate the rule.

4.4.4.1 MTI Rule Conditions

The MTI rule sets support conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received MT message, but is evaluated against the time at which the rule is evaluated.
Originator	General	By originator, we generally refer to the TP-OA parameter of a Deliver-SM message or the TP-RA parameter of a Status-Report message.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the originator address, if the originator address is categorized as MSISDN.
	Single short number, short number range or short number prefix	This condition is evaluated against the originator address, if the originator address is categorized as a short number.

Condition	Format	Description
	Alphanumeric	This condition is evaluated against the originator address, if the originator address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized originator address, if the originator address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes, if the originator address is categorized as MSISDN.
	List	This condition evaluates the normalized address against a list of MSISDNs or short numbers, enabling logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the TP-OA or TP-RA parameter.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the TP-OA or TP-RA parameter.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the MTI rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified.
Recipient	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the recipient MSISDN retrieved from the correlation record.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the recipient MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the recipient MSISDN against the provisioned mobile network number ranges and network prefixes ⁵ .
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the "real" IMSI for the recipient of the subsequent MT messages, as returned by the HLR or retrieved from the portable application provisioning data. If no "real" IMSI is available, the

⁵ In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
		condition evaluates to false if not inverted, and to true if inverted.
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the recipient MSISDN against a list of MSISDNs, or the "real" recipient IMSI against a list of IMSIs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the MTI rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
DCS		This condition is evaluated against the Deliver-SM's TP-DCS parameter. If the MT message is a Status Report, the condition evaluates as if the TP-DCS parameter were set to 0.
Message Type		This condition is evaluated against the MT message type, which is a Deliver-SM or a Status Report.
User Data		This condition is evaluated against the user data portion of the MT message. In the case of a Status Report, this condition behaves as if the user data portion were empty.
User Data Header		This condition is evaluated against the list of user data header information element identifiers that are present in the MT message.
Ext Att		This condition is evaluated against the external attributes as set and reset by the EC application consulted during the evaluation of the MTIX rules. This condition is not supported in the MTIX rule set.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the SMSC address received at the MAP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
Originator - SMSC Addr. Match		<p>This condition is evaluated by comparing the Originator address and the SMSC Address on the basis of their country and network parameters. The respective country is derived by extracting the E.164 country code from the Originator and the SMSC address and matching the same against the provisioned countries. Similarly, the respective network is derived by matching the Originator and the SMSC address against the provisioned mobile network number ranges/prefixes. In case no provisioned country or network number range/prefix is matched, then the corresponding country or network is considered as "unknown".</p> <p>The comparison of the Originator and the SMSC address is based on the following criteria, which are configurable on the MGR:</p> <ul style="list-style-type: none"> • 0 - Originator Country equals SMSC • 1 - Originator Country strictly equals SMSC • 2 - Originator Network equals SMSC • 3 - Originator Network strictly equals SMSC <p>The 'strictly equals' criterion requires an exact match of the two values being compared, and it is a special case of the 'equals' criterion which can be satisfied even if one (or both) of the values being compared is (are) 'unknown'. Note that only one criterion can be configured at a time. In case none of the criteria is configured, the non-inverted condition always evaluates to FALSE and the inverted condition always evaluates to TRUE.</p>
Dest. MSC or SGSN	General	This condition is evaluated against the real MSC or SGSN address as retrieved from the correlation record. If addresses are available, the rule set is evaluated against either the MSC or the SGSN address, as selected by the SSN included in the SCCP CDPA. If neither an MSC nor SGSN address is available in the correlation record, a non-inverted condition evaluates to FALSE, and an inverted condition evaluates to TRUE.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the selected MSC or SGSN address retrieved from the correlation record.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the selected MSC or SGSN address. Successful extraction of the country code depends on the provisioned countries.

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the selected MSC or SGSN address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the selected MSC or SGSN address against a list of E.164 numbers. This enables logical OR operation.
SCCP Calling Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Calling Party Address in E.164 format received at the SCCP layer of the inbound MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layers.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the inbound MT message against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the inbound MT message against a Point Code or a Point Code Range. Note: 1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. 2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.

Condition	Format	Description
SCCP Called Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Called Party Address in E.164 format received at the SCCP layer of the inbound MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Called Party address received at the SCCP layer of the inbound MT message against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Called Party address received at the SCCP layer of the inbound MT message against a Point Code or a Point Code Range. Note: 1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. 2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Reply Path		This condition is evaluated against the MT message's TP-RP flag.
Status Report		This condition is evaluated against the MT message's TP-SRI flag.
PID		This condition is evaluated against the Deliver-SM's TP-PID parameter. If the MT message is a Status Report, the condition evaluates as if the TP-PID parameter were set to 0.

Condition	Format	Description
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that which issued the MT message.
Message Segments		This condition is evaluated against the interpreted user data header information element, indicating that the message is segmented. Note: A condition with neither the first, nor the last, nor the intermediate segment flags turned on will evaluate to false if the MT message is not segmented. To match on unsegmented messages only, turn on all three flags and invert the condition.
Recipient RN Group		During the processing of the preceding SRI-SM request, the HLR may have returned an IMSI that was prefixed with a provisioned routing number. If a routing number was recognized, it was stripped off the real IMSI, associated with a routing number group, and added to the correlation record. This condition is evaluated against that routing number group.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs during the processing of the SRI-SM request. If there was a match, the recipient is considered to be a portable application.

4.4.4.2 MTIR Routing Action

The primary effect of the evaluation of the MTIR rule set is that the RTR determines where the MT message will be routed, which is implemented through the matching MTIR rule's routing action. The possible actions are:

Action	Effect
Discard with temporary error	Reject the MT message by sending a ReturnError response that contains the configurable error code for temporary errors of the MSC/SGSN back to the external SMSC. You can configure the error code using the semi-static configuration attribute <code>mttemporarydiscarderrorformscorsgsn</code> .
Discard with permanent error	Reject the MT message by sending a ReturnError response that contains the configurable error code for permanent errors of the MSC/SGSN back to the external SMSC. You can configure the error code using the semi-static configuration attribute <code>mtpermanentdiscarderrorformscorsgsn</code> .
Discard with no response	Drop the MT message without sending a response back to the external SMSC.

Action	Effect
Discard with acknowledgment	Discard the MT message after sending a response to the external SMSC that indicates delivery success. The external SMSC will proceed as if the MT messages was delivered successfully.
Store for delivery to MS	Store the MT message in the specified AMS queue and return a response depending only on the storage result. At a later point in time, the AMS will request that the RTR deliver the MT message, which may lead to multiple retries. You must specify the AMS queue in which to temporarily store the MT message in the MTIR rule. A rule with this routing action only matches if, at the time of the rule evaluation, at least one AMS is available, which indicates the capability for storing messages (as opposed to Icache functionality only).
Route to mobile	<p>Directly send the inbound MT message on to the MSC or SGSN with which the recipient is currently registered. If no routing data is available from the correlation record (because the HLR was not queried during the preceding SRI-SM processing), the HLR query is executed before the MT message is sent to the MSC or SGSN.</p> <p>Note: In this case of a "late" HLR query, the transparent nature of MT-MT forwarding is lost, the RTR recreates the outbound MT message, and the RTR typically uses its own global title (GT) to identify the SMSC toward the terminating MSC or SGSN. Likewise, the transparent nature of the MT response forwarding toward the external SMSC is lost. Depending on the categorization of the MT response from the MSC or SGSN, the error code that is sent back to the SMSC is determined in the same way as for the "discard with temporary error" or "discard with permanent error" action. In the case of a late HLR query, the MTO rules are evaluated during the outbound SRI-SM processing in the same way as they are evaluated for an outbound SRI-SM during the inbound SRI-SM processing, with one exception: the MTOR rule set does not follow the <code>firewallenablemtrtgruleevaluationforsrismresponse</code> attribute, but rather is never evaluated for SRI-SM responses.</p>
Route to application	<p>Route the inbound MT message as an AT message to an application. The target application can be determined in three ways:</p> <ul style="list-style-type: none"> • By the rule. The MTIR rule explicitly refers to a provisioned application. All MT messages matching this rule are delivered as AT messages to that application. Such MTIR rules only match if, at the time of the rule evaluation, the target application is available for receiving AT messages. • By recipient address. The recipient address can refer to a provisioned application by means of the provisioned portable applications. If that is the case of the inbound MT message, such an MTIR rule can only match if at the time of the rule evaluation, the application associated with the recipient address is available for receiving AT messages. • By load balancing group. Refer to the description of AT load balancing groups. The MTIR rule explicitly refers to a provisioned load balancing group. All MT messages matching this rule are delivered as AT messages to one of the applications in that load balancing group. Such MTIR rules

Action	Effect
	<p>only match if at the time of the rule evaluation, at least one of the applications in the load balancing group is available for receiving AT messages.</p> <p>When an temporary/permanent error is returned, the error code can be configured using the semi-static configuration attributes:</p> <ul style="list-style-type: none"> • mttemporarydiscarderrorformscorsgsn • mtpermanentdiscarderrorformscorsgsn
Route to SMSC as AO	<p>Route the inbound MT message as an AO message to an external SMSC so that the SMSC will take care of the (further) delivery of the message. The rule explicitly specifies:</p> <ul style="list-style-type: none"> • Which application should be used to submit the AO message to the SMSC • Which SMSC group the AO message should be forwarded to <p>For such an MTIR rule to match, the following additional conditions must be met:</p> <ul style="list-style-type: none"> • The MT message must be a Deliver-SM (it is not possible to route Status Report messages as AO) • At the time of the rule evaluation, at least one of the SMSCs in the SMSC group must be available to receive AO messages from the designated application <p>When an temporary/permanent error is returned, the error code can be configured using the semi-static configuration attributes:</p> <ul style="list-style-type: none"> • mttemporarydiscarderrorformscorsgsn • mtpermanentdiscarderrorformscorsgsn

Note:

CDRs will be generated using the billing profile (if configured) for Discarded Messages when the message is discarded due to the application of any of the following routing action:

1. Discard with permanent error
2. Discard with no response

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Apart from the above stated condition, if the semi-static parameter `rtrcreatemtcdrforscenarios` is configured as true, CDRs will also be generated using the billing profile (if configured) for Discarded Messages when the configured billing profile is of 3G CDR format and the message is discarded due to the application of any of the following routing actions:

1. Discard with permanent error
2. Discard with no response
3. Discard with temporary error

If no MTIR rule matches, the RTR applies the following logic:

```

If the recipient MSISDN is associated with an application by means of the portable
application provisioning data, then
  If that application is available to receive AT messages
    Route the MT message as AT to that application
  Else
    Behave as if a MTIR rule with action "discard with temporary error" had
    matched
Else
  Behave as if a MTIR rule with action "route to MS" had matched

```

4.4.4.3 MTIR Routing Action Parameters

This section describes the parameters for MTIR routing actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> Discard with permanent error Discard without response 	None
Billing for Blocked Messages	Billing Profile to use for block message records. Applies to: <ul style="list-style-type: none"> Discard with temporary error 	None
Billing for Failed Delivery	Billing Profile to use for failed Delivery. Applies to: <ul style="list-style-type: none"> Route to Mobile 	None
Billing for Acceptance	Identifier specifying which billing profile should be used for submission records. Applies to: <ul style="list-style-type: none"> Route to Mobile Store for Delivery to MS Discard with acknowledgement Route to application Route to SMSC as AO 	None

4.4.5 Creating an Outgoing MT Routing Rule

Prerequisites:

- Billing profile

- External attribute
- Modifier

To create an outgoing mobile-terminating routing (MTOR) rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **MTOR**.
The Outgoing Mobile Terminating Routing Rules tab appears.
2. Click **Add New**.
A new Outgoing Mobile Terminating Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The MTOR rule with the highest priority is evaluated first.
6. Set conditions for the rule.
7. Enter the rule matching ratio in the **Rule Matching Ratio** box.
8. From the **Conversion Table** list, select a 'Conversion Table'. Default value is 'None'.
9. Check the **Inc. TP-MR in MT-ForwardSM** parameter to include the TP-MR field in the outgoing MT-ForwardSM messages (By default, this field is unchecked).
10. From the **Action** list, select a routing action for the rule.
11. Set the parameters for the routing action, if required.
12. In the **Action Threshold** box, set the maximum number of messages per second that are allowed before the rule takes effect (this parameter only applies when the AT rule matches).
13. From the **Outgoing Originator Address Conversion** list, select RuleSet from the list only if it is desired to apply the outgoing address conversion on the originator addresses of all MT messages that would match this rule. By default "No Change" will be selected always.
See [Creating Outgoing Address Conversion Rule Sets](#) for more details regarding outgoing address conversion.
14. Optionally select a log profile from the **Log Profile** list.
15. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
16. Click **Save**.
The MGR creates the rule and closes the tab.
17. Activate the rule.

4.4.5.1 MTO Rule Conditions

MTO rule sets are evaluated in many scenarios; therefore, the amount of message-related information that is available to the rule set evaluation varies significantly. Most conditions should be used with care. Additional conditions may be required to disambiguate among cases. The message type condition is the primary example of such an additional condition.

The MTO rule sets support conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the MT message, but is evaluated against the time at which the rule is evaluated.
SMSC Address	General	If the MT message was issued by an external SMSC, this condition is evaluated against the normalized SMSC address found at the MAP layer of the inbound MT message. If the message was issued by the RTR, this condition is evaluated against the RTR's common address or, if there is no common address, the RTR's specific global title (GT). The latter is not commonly used.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the E.164 address representing the SMSC.
	Country	This condition is evaluated against the country derived from the SMSC address by extracting the E.164 country code. Evaluation of this condition depends on the provisioned countries.
	Network	This condition is evaluated against the mobile network derived from the SMSC address by matching the E.164 number against the number ranges and/or network prefixes that are provisioned for each mobile network. Evaluation of this condition depends on the provisioned countries and mobile networks.
	List	This condition evaluates the SMSC address against a list of MSISDNs.
Originator	General	This condition is evaluated against a normalized version of the originator address of the MT message. In case of a Status Report, the condition is evaluated against the recipient of the original message that caused the generation of the status report. When the MTO rule set is evaluated for an SRI-SM request issued by an external SMSC or for the HLR's response to that request, the originator may not be available (the RP-SMEA field of the SRI-SM request is optional and typically not present). If the originator address is not present, a non-inverted condition evaluates to false and an inverted condition evaluates to true.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the originator address of the MT message, if it is categorized an MSISDN.
	Single short number, short number range, or short number prefix	This condition is evaluated against the originator address of the MT message, if it is categorized as a short number.
	Application	This condition is evaluated against the application associated with the originator address of the MT

Condition	Format	Description
		<p>message, if a locally provisioned application matches the originator address by means of the short number or an alphanumeric alias.</p> <p>Note: MT messages originating from an external SMSC may have a different meaning/application assigned to a certain short number or alphanumeric alias. Therefore, this condition should be used with care.</p>
	Country	This condition is evaluated against the country derived from the originator address by extracting the E.164 country code from the normalized MSISDN. Evaluation of this condition depends on the provisioned countries.
	List	This condition evaluates the normalized originator against a list of MSISDNs or short numbers (as determined by the list's type).
	Alphanumeric	This condition is evaluated against an alphanumeric originator address (as determined by the type of number of the originator address). Alphanumeric addresses can be no longer than 11 characters from the GSM default alphabet.
	Application category	<p>The Application Category configured under the Originator condition is considered matched when at least one of the configured bit matches with the originating application.</p> <p>In case of MTOR rules, for incoming application originated message (e.g. AO-MT path), while evaluating the Originator condition, the source application is considered as the originating application.</p>
Originator - SMSC Addr. Match		<p>This condition is evaluated by comparing the Originator address and SMSC Address on the basis of their country and network parameters. The respective country is derived by extracting the E.164 country code from the Originator and the SMSC address and matching the same against the provisioned countries. Similarly, the respective network is derived by matching the Originator and the SMSC address against the provisioned mobile network number ranges/prefixes. In case no provisioned country or network number range/prefix is matched, then the corresponding country or network is considered as "unknown".</p> <p>The comparison of the Originator and the SMSC address is based on the following criteria, which are configurable on the MGR:</p>

Condition	Format	Description
		<ul style="list-style-type: none"> • 0 - Originator Country equals SMSC • 1 - Originator Country strictly equals SMSC • 2 - Originator Network equals SMSC • 3 - Originator Network strictly equals SMSC <p>The 'strictly equals' criterion requires an exact match of the two values being compared, and it is a special case of the 'equals' criterion which can be satisfied even if one (or both) of the values being compared is (are) 'unknown'. Note that only one matching criterion can be configured at a time. In case none of the criteria is configured, the non-inverted condition always evaluates to FALSE and the inverted condition always evaluates to TRUE.</p> <p>The Originator address used for evaluating this condition is the same as the address used for evaluating the 'Originator' condition. The SMSC address is taken from the MAP layer service centre address (SM-RP-OA) in the case of an incoming MT message, and for other types of messages it is the same as the address used for evaluating the 'SMSC Address' condition.</p> <p>Note:</p> <p>This condition is not supported for outgoing MT Status Reports, SRI-SM Requests and SRI-SM Responses. If configured, the condition will always evaluate to false while matching a MTO rule against any of the above message types.</p>
Dest. MSC or SGSN	General	<p>This condition is evaluated against the terminating MSC or SGSN of the MT message. This information is not available when:</p> <ul style="list-style-type: none"> • The MTO rule set is evaluated for an SRI-SM request (in such a case, a non-inverted condition evaluates to false and an inverted condition evaluates to true) • The MTOX rule set is evaluated for the response to an SRI-SM request • The MTOR rule set is evaluated for the response to an SRI-SM request issued by the RTR <p>When the MTOR rule set is evaluated for the response to an SRI-SM request issued by an external SMSC and the MSC and SGSN address are both available, the rule set is evaluated twice: once for the MSC and once for the SGSN, as selected by the semi-static attribute <code>preferredmtdestination</code>. The RTR uses the matching rule with the higher priority.</p>

Condition	Format	Description
		Note: If the Network configuration is available according to MSC and/or SGSN (i.e. received in the HLR query), the Preferred MT Destination in the Network configuration overrides the semi static attribute <code>preferredmtdestination</code> for the rules evaluation.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the E.164 address representing the terminating MSC or SGSN.
	Country	This condition is evaluated against the country derived from the MSC or SGSN address by extracting the E.164 country code. Evaluation of this condition depends on the provisioned countries.
	Network	This condition is evaluated against the mobile network derived from the MSC or SGSN address by matching the E.164 number against the number ranges and/or number prefixes that are provisioned for each mobile network. Evaluation of this condition depends on the provisioned countries and mobile networks.
	List	This condition evaluates the MSC or SGSN address against a list of MSISDNs.
	Single point code or point code range	When the MTO rule set is evaluated against an MT message issued by an external SMSC, the MSC/SGSN address is only available in the SCCP called party address (CDPA). If PC/SSN routing is used, rather than global title (GT) routing, the MSC/SGSN address may only be available in the form of a point code (PC). This condition is evaluated against that PC. If the PC is not available, a non-inverted condition evaluated to false and an inverted condition evaluates to true.
Recipient	General	This condition is evaluated against the MT message's recipient address. The recipient MSISDN is not part of an MT message; therefore, if the MT message was issued by an external SMSC and not Home Routed, the recipient MSISDN is not available to this condition. The recipient IMSI is not available when: <ul style="list-style-type: none"> • The MTO rule set is evaluated for an SRI-SM request • The MTOX rule set is evaluated for the response to an SRI-SM request issued by the RTR
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the recipient MSISDN. When not available, the non-inverted condition evaluates to false, and the inverted condition evaluates to true.

Condition	Format	Description
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the recipient IMSI.
	Country	This condition is evaluated against the country for which the recipient's IMSI has been issued. Evaluation of this condition depends on the provisioned countries.
	Network	This condition is evaluated against the mobile network for which the recipient IMSI has been issued. Evaluation of this condition depends on the provisioned countries and mobile networks.
	List	This condition evaluates the recipient MSISDN or IMSI against a list of MSISDNs or IMSIs.
SCCP Calling Party Address	General	This condition is evaluated against the Calling Party Address received at the SCCP layer of the MT message. This information is applicable only for MT-FSM requests originated from external SMSCs. For all other types of MT messages, a non-inverted condition evaluates to false and an inverted condition evaluates to true.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the E.164 address representing Calling Party at the SCCP layer.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is received at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
	PC or PC Range	<p>This condition evaluates the PC included in Calling Party address received at the SCCP layer of the MT message against a Point Code or a Point Code Range.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. 2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
SCCP Called Party Address	General	This condition is evaluated against the Called Party Address received at the SCCP layer of the MT message. This information is applicable only for MT-FSM requests originated from external SMSCs. For all other types of MT messages, a non-inverted condition evaluates to false and an inverted condition evaluates to true.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the E.164 address representing the Called Party at the SCCP layer.
	Country	<p>This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries.</p> <p>Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.</p>
	Network	<p>This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes.</p> <p>Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.</p>
	List	This condition evaluates the Called Party address received at the SCCP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
	PC or PC Range	<p>This condition evaluates the PC included in Called Party address received at the SCCP layer of the MT message against a Point Code or a Point Code Range.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. 2. If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
User Data		This condition is evaluated against the user data of an MT message. If the message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request (or its response) issued by an external SMSC, no user data is available.
User Data Hdr		This condition is evaluated against the list of user data header information element identifiers present in the MT message. If the message is a Status Report, if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), or if the MT message does not contain a user data header, no user data header is available.
Reply Path		This condition is evaluated against the MT message's TP-RP flag. If the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), no reply path information is available.
Status Report		This condition is evaluated against the MT message's TP-SRI flag. If the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), no status report indication information is available.
PID		This condition is evaluated against the Deliver-SM's TP-PID parameter. If the MT message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), the condition evaluates as if the TP-PID parameter were set to 0.
DCS		This condition is evaluated against the Deliver-SM's TP-DCS parameter. If the MT message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), the condition evaluates as if the TP-DCS parameter were set to 0.

Condition	Format	Description
Originator TON		This condition is evaluated against the type of number (TON) parameter of the originator. Refer to the description of the originator condition for information about this parameter's availability.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the originator. Refer to the description of the originator condition for information about this parameter's availability.
Ext Att		This condition is evaluated against the external attributes as set and reset by the EC application consulted during the evaluation of EC rules.
XS Message		<p>This condition is evaluated against the XS message type of an MT message. Only Deliver-SMs can have an XS message type other than "no XS message". Valid XS message types are:</p> <ul style="list-style-type: none"> • Forwarded message • Message copied to a subscriber • Message copied to an application (not relevant to MTO rule sets) • Auto-reply message • Copy to Email (not relevant to MTO rule sets) • Forward to Email (not relevant to MTO rule sets) <p>This condition is not supported in the MTIC and MTIX rule sets.</p>
Message Type		<p>This condition is evaluated against the type of message. Valid values are:</p> <ul style="list-style-type: none"> • Deliver-SM (normal message) • Status Report • SRI-SM Request • SRI-SM Response
Originator SSI		This condition is evaluated against the SSI information of the originator. It enables you to specify which services the originator must or must not have. If the MTO rule set is evaluated while the originator MSISDN is not available (such as for SRI-SM requests issued by an external SMSC with the RP-SMEA field not present, and the subsequent responses), no originator SSI is available. If SSI is not used, this condition should not be specified.
Recipient SSI		This condition is evaluated against the SSI information of the recipient. It enables you to specify which services the recipient must or must not have. If the MTO rule set

Condition	Format	Description
		is evaluated while the recipient MSISDN is not available (such as for unsolicited MT messages issued by an external SMSC), no recipient SSI is available. If SSI is not used, this condition should not be specified.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC, which issued the SRI-SM request or MT message. If the RTR issued the message, it is considered trusted.
Message Concatenated Match		This condition is evaluated against the Deliver-SM's UDH in the IEI parameter. If the MT message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), the condition evaluates as if the UDH in IEI parameter were set to 0 or 8.

4.4.5.2 MTOR Routing Action

The primary effect of the evaluation of the MTOR rule set is that the RTR determines if a message should be passed or blocked, which is implemented through the matching MTOR rule's routing action. The possible actions are:

Action	Effect
Pass	When the MTOR rule set is evaluated for an SRI-SM request, this action causes the RTR to send the SRI-SM request to the HLR, so that the HLR will send its response back to the RTR. When the MTOR rule set is evaluated for the response to an SRI-SM request issued by an external SMSC, this action means that SRI-SM response processing will continue by the inbound SRI-SM processing logic's evaluation of the SRI-SM Response rule set. When the MTOR rule set is evaluated for an MT message, this action means that the MT message shall be sent to the MSC/SGSN, so that the MSC/SGSN will send its response back to the RTR.
Block with temporary error	This action means that the requestor of the outbound SRI-SM or MT message will consider the requested outbound service to have failed with an error classified as temporary.
Block with permanent error	This action means that the requestor of the outbound SRI-SM or MT message will consider the requested outbound service to have failed with an error classified as permanent.
Block with no response	This action means that if the SRI-SM request or MT message was issued by an external SMSC, the RTR will discard the inbound message and return no response. For MT delivery attempts requested by the RTR, this action produces the same behavior as the "block with temporary error" action.
Block with acknowledgment	When the MTOR rule set is evaluated for an MT message, this action causes the RTR to not send the MT message to the MSC/SGSN, but to indicate successful delivery to the requestor of the outbound MT service. When the

Action	Effect
	MTOR rule set is evaluated for a SRI-SM request or response, this action produces the same behavior as the "pass" action.
Release	<p>When the MTOR rule set is evaluated for a SRI-SM request issued by an external SMSC, this action causes the RTR to relay the SRI-SM request to the HLR so that the HLR will send its response directly to the external SMSC (not to the RTR). When the MTOR rule set is evaluated for the response to an SRI-SM request issued by an external SMSC, this action means that the RTR skips evaluation of the SRI-SM Response rules of the inbound SRI-SM processing, and subsequent MT messages are therefore not get Home-Routed. In all other cases, this action has the same effect as the "pass" action.</p> <p>Note: The "release" action is deprecated. The SRI-SM Request and SRI-SM Response rule sets should be used.</p>

If no MTOR rule matches, the RTR applies routing logic that is the same as for the "pass" action.

4.4.5.3 MTOR Mobile Domain

Mobile Domain parameter indicates the Recipient mobile network domain (IMS or SS7) where message should be delivered.

Condition	Format	Description
Mobile Domain (if 'Domain Selection' license is TRUE)	No Change (default)	This indicates that message delivery is performed in domain configured in semi-static file or received from EC application.
	IMS	This indicates that message delivery is performed in IMS domain.
	IMS then SS7	This indicates that message delivery is performed in IMS domain and if failed, fallback to SS7 domain.
	SS7	This indicates that message delivery is performed in SS7 domain.

4.4.6 Creating an AO Routing Rule

Prerequisites:

- AMS queue
- Application
- Application category

- Application group
- Billing profile
- CIMD tariff class
- CIMD tariff class description
- External attribute
- Modifier
- Routing number group
- Service class
- SMSC group

To create an application-originating routing (AOR) rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **AOR**.
The Application Originating Routing Rules tab appears.
2. Click **Add New**.
A new Application Originating Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The AOR rule with the highest priority is evaluated first.
6. In the **Maximum** box, enter the maximum number of messages per second allowed for the primary destination of the rule (defaults to 65,535).
7. In the **Committed** box, enter the committed number of messages per second for the primary destination of the rule (defaults to 10,000).
The committed number of messages applies in cases of congestion.
8. Set conditions for the rule.
9. From the **Action** list, select a routing action for the rule.
10. Set the parameters for the routing action, if required.
11. Optionally select an AO modifier from the **Modifier** list.
12. Optionally select a log profile from the **Log Profile** list.
13. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
14. Click **Save**.
The MGR creates the rule and closes the tab.
15. Activate the rule.

4.4.6.1 AO Rule Conditions

The following table details the conditions that are available for AO rules.

Condition	Values	Description
Time Schedule	<ul style="list-style-type: none"> • Always • Schedule 	Condition on the evaluation time of the message: <ul style="list-style-type: none"> • Always: The condition is always true.

Condition	Values	Description
		<ul style="list-style-type: none"> Schedule: The condition is true if the current time falls within the schedule as specified by the selected routing schedule, defined in Routing ► Schedules.
Application	<ul style="list-style-type: none"> None Application 	Index of the application originating the message.
Application Group	<ul style="list-style-type: none"> None Bit string 	Index of the application group associated with the application originating the message.
Application Category	<ul style="list-style-type: none"> None Bit string 	Index of the application category associated with the application originating the message.
Service Class	<ul style="list-style-type: none"> None Bitstring 	Index of the service class associated with the application originating the message.
Protocol	<ul style="list-style-type: none"> None Bitstring <ul style="list-style-type: none"> UCP SMPP CIMD 	Protocol used by the originating application to submit the message.
Operation	<ul style="list-style-type: none"> None Bit string <ul style="list-style-type: none"> 0: UCP call input operation (01) 1: UCP multiple address call input operation (02) 2: UCP call input with supplementary services operation (03) 3: UCP MS message transfer operation (30) 4: UCP submit short message operation (51) 	Operation used by the originating application to submit the SM. The condition pertains to the following protocol specific fields: <ul style="list-style-type: none"> UCP: Command ID SMPP: Command ID CIMD: Operation Code

Condition	Values	Description
	<ul style="list-style-type: none"> • 9: UCP operation other than above • 10: SMPP SubmitSm • 12: SMPP SubmitMulti • 13: SMPP DataSm • 19: SMPP operation other than above • 20: CIMD SubmitMessage • 29: CIMD operation other than above • 30: Other operations (from another protocol than UCP, SMPP, or CIMD) 	
Originator	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List 	<p>Originator that is specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: OAdC / OTOA • SMPP: source_addr • CIMD: [Alphanumeric] Originating address
Originator TON	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	<p>Type of number (TON) specified for the originator of the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: OAdC / OTOA • SMPP: source_addr_ton • CIMD: [Alphanumeric] Originating address

Condition	Values	Description
Originator NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN Telephony • 2: Data • 3: Telex • 4: Reserved • 5: Reserved • 6: Reserved • 7: Reserved • 8: National numbering plan • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	<p>Numbering plan identification (NPI) specified for the originator of the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: OTOA • SMPP: source_addr_npi • CIMD: [Alphanumeric] Originating address
Recipient	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List • Single IMSI • IMSI range • IMSI prefix 	<p>Recipient that is specified in the SM. The condition pertains to the following protocol specific fields :</p> <ul style="list-style-type: none"> • UCP: ADC • SMPP: destination_addr • CIMD: Destination address <p>Note: When an IMSI-related condition is used but the recipient IMSI is not known at the moment of rule evaluation, the condition will evaluate to FALSE if not negated or TRUE if negated. This condition requires the recipient number to be an MSISDN and the HLR query to be performed before the rule evaluation (to obtain the recipient IMSI). The Early SRI-SM for AO/SM attribute in the MGR (Routing > Properties) controls when the HLR query is performed.</p>
Recipient TON	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number 	<p>Type of number (TON) specified for the recipient of the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: ADC • SMPP: destination_addr_ton • CIMD: Destination address

Condition	Values	Description
	<ul style="list-style-type: none"> • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	
Recipient NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN telephony • 2: Data • 3: Telex • 4: Reserved • 5: Reserved • 6: Reserved • 7: Reserved • 8: National numbering plan • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	<p>Numbering plan identification (NPI) specified for the recipient of the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: (always isdnTelephony) • SMPP: destination_addr_npi • CIMD: (always isdnTelephony)
Terminating MSC/SGSN	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • List • Country • Network 	<p>Destination MSC and/or SGSN. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before AO rule evaluation (to obtain the MSC and/or SGSN). The Early SRI-SM for AO/SM attribute in the MGR (Routing > Properties) controls when the HLR query is performed. If both the MSC and SGSN are present, the preferredmtdestination attribute determines which will be used for rules evaluation. If the HLR query fails, the condition will evaluate to "false", whether it is a negative or positive condition.</p>

Condition	Values	Description
User Data	<ul style="list-style-type: none"> • None • Full text • Text tag • Subtext (contains) • Text length 	<p>The text that is specified in the user data of the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: Amsg • SMPP: message_payload • CIMD: User data [binary] <p>Content of the message:</p> <ul style="list-style-type: none"> • Full text: Compares the entire message content with a defined string. Only evaluates positively if there is an exact match with the user data (message content). • Text tag: Compares the first part of the message content with a defined tag-string. Only evaluates positively if the message starts exactly with the defined tag-string. Useful to define a rule on keywords (e.g. *LONG# for CMG SMSCs). • Subtext (contains): Compares if the message content contains a defined tag-string. To optimise the search, a start position (default 1) and an end position (default 160) must be specified in which the string is to be found. <p>Note: All message content scanning is case-insensitive.</p>
User Data Header Indication	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	<p>User data header indication that is specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: XSER (GSM UDH information) • SMPP: esm_class (UDHI) or UDH information received in concatenation related TLVs (sar_msg_ref_num, sar_total_segments, sar_segment_seqnum) • CIMD: User data header
User Data Header	<ul style="list-style-type: none"> • None • Byte value 	<p>Value specified in one of the IEs of the user data header (UDH) of the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: XSER (GSM UDH information) • SMPP: short_message (prefix) or UDH information received in concatenation related TLVs (sar_msg_ref_num, sar_total_segments, sar_segment_seqnum) • CIMD: User data header <p>Only evaluates positively if there is an exact match with the information element identifier (00-FF,</p>

Condition	Values	Description
		hexadecimal) of the UDH. Refer to technical specification 3GPP 23.040 for more information. Most common information element identifier (IEI) values: <ul style="list-style-type: none"> • 00: Concatenated short message • 01: Special SMS message indication • 04: Application port addressing scheme, 8-bit address • 05: Application port addressing scheme, 16-bit address • 06: SMSC control parameters • 07: UDH Source Indicator
Reply Path	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0: Off • 1: On 	Reply path indication that is specified in the SM. The condition pertains to the following protocol specific fields: <ul style="list-style-type: none"> • UCP: RPI • SMPP: esm_class (RPI) • CIMD: Reply Path
Notification Address	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List • Single TCP/IP address • Single X121 address 	Notification address that is specified in the SM. The condition pertains to the following protocol specific fields: <ul style="list-style-type: none"> • UCP: NAdC
Notification Request	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	Notification request indication that is specified in the SM. The condition pertains to the following protocol specific fields: <ul style="list-style-type: none"> • UCP: Nrq • SMPP: registered_delivery • CIMD: Status report request
Notification Type	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • Delivered 	Notification type that is specified in the SM. The condition pertains to the following protocol specific fields: <ul style="list-style-type: none"> • UCP: Nrq

Condition	Values	Description
	<ul style="list-style-type: none"> • Not delivered • Buffered 	<ul style="list-style-type: none"> • SMPP: registered_delivery • CIMD: Status report request <p>The following bit string values apply:</p> <ul style="list-style-type: none"> • Delivered: Delivery Notification (DN) • Not delivered: Non-delivery notification (ND) • Buffered: Buffered message notification (BN) <p>0 default value, 1 = DN, 2 = ND, 3 = DN+ND, 4 = BN, 5 = BN+DN, 6 = BN+ND, 7 = all.</p>
Single Shot Indicator	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	<p>Single-shot indicator that is specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: XSER (single Shot Indication)
More Messages To Send	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	<p>More-messages-to-send indicator that is specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: MMS • SMPP: more_messages_to_send • CIMD: More messages to send
Priority	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: UCP no priority requested • 1: UCP priority requested • 10: SMPP no priority requested • 11: SMPP priority requested • 20: CIMD priority level 1 (most urgent) • 21: CIMD priority level 2 • 22: CIMD priority level 3 • 23: CIMD priority level 4 • 24: CIMD priority level 5 	<p>Priority level that is specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: PR • SMPP: priority_flag • CIMD: Priority

Condition	Values	Description
	<ul style="list-style-type: none"> • 25: CIMD priority level 6 • 26: CIMD priority level 7 • 27: CIMD priority level 8 • 28: CIMD priority level 9 	
Protocol Identifier (PID)	<ul style="list-style-type: none"> • None • Byte value (between 00 and FF hexadecimal) 	<p>Protocol ID (PID) specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: RPID • SMPP: protocol_id • CIMD: Protocol identifier
Data Coding Scheme (DCS)	<ul style="list-style-type: none"> • None • Byte value (between 00 and FF hexadecimal) 	<p>Data coding scheme (DCS) specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: XSER (DCS) • SMPP: data_coding • CIMD: Data coding schema <p>Note: If the value of the HUB parameter hubPropDcsCharCodingConversion and rtrdcscharcodingconversion are set to 'japan' and the data_coding value in the incoming SMPP AO message is 0x02, then this rule shall be applied on the converted data_coding 0x04.</p>
Concat. Msg. Segments	<ul style="list-style-type: none"> • None • Bit String <ul style="list-style-type: none"> • First Segment • Last Segment • Not First Nor Last 	<p>Segment sequence number of a concatenated SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: XSER (GSM UDH information) • SMPP: short_message (prefix) or UDH information received in concatenation related TLVs (sar_segment_seqnum) • CIMD: User data header
UCP Authentication Code	<ul style="list-style-type: none"> • None • Digit string 	<p>Authentication code specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: AC

Condition	Values	Description
Notification PID	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Mobile station • 1: Fax group 3 • 2: Menu over PSTN • 3: PC application over PSTN • 4: PC application over ISDN • 5: PC application over TCP/IP • 6: PC application over X25 • 7: Unknown 	<p>The Notification PID specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: NPID / Nrq <p>Note: To have the NPID matched, the UCP fields Notification Request (NRq) must be set, Notification Type (NT) should be larger than 0, and Notification Address (NAdC) should be filled in as well in the message.</p>
Last Resort Address	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List • Single TCP/IP address • Single X121 address 	<p>Last Resort Address (LRAd) specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: LRAD
Last Resort Request	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	<p>Last Resort Address Request indicator specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: LRAd <p>The following bit string values apply:</p> <ul style="list-style-type: none"> • 0 = LRAd not used • 1 = LRAd used
Last Resort PID	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Mobile station • 1: Fax group 3 • 2: Menu over PSTN 	<p>Last Resort Address PID specified SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: LPID

Condition	Values	Description
	<ul style="list-style-type: none"> • 3: PC application over PSTN • 4: PC application over ISDN • 5: PC application over TCP/IP • 6: PC application over X25 • 7: Unknown 	
CIMD Tariff Class	<ul style="list-style-type: none"> • None • Bit string 	<p>Index of the CIMD tariff class specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • CIMD: Tariff class
CIMD Service Description	<ul style="list-style-type: none"> • None • Bit string 	<p>Index of the CIMD service description specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • CIMD: Service description
Ext Att	<ul style="list-style-type: none"> • None • External attributes 	A set of 32 attributes, the value of which can be controlled by external condition (EC) applications.
Validity Period	<ul style="list-style-type: none"> • None • Relative Time 	<p>Validity period specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: VP • SMPP: validity_period • CIMD: Validity period absolute/relative
Deferred Delivery Time	<ul style="list-style-type: none"> • None • Relative Time 	<p>Deferred delivery time specified in the SM. The condition pertains to the following protocol specific fields:</p> <ul style="list-style-type: none"> • UCP: DDT • SMPP: scheduled_delivery_time • CIMD: First delivery time absolute/relative
Recipient RN Group	<ul style="list-style-type: none"> • None • SNMP index 	Routing number (RN) group to which the RN in the recipient address belongs
Originator SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual originator subscriber services (defined in SPF Services ► SPF Services). The condition test works like a logical AND operation (similar to the

Condition	Values	Description
		external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.
Recipient SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual recipient subscriber services. The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.

4.4.6.2 AO Routing Action Parameters

The following tables detail the parameters for AO routing actions.

Multiple AO routing actions:

Parameter	Description	Default
Billing For Submission	Billing profile to use for submission; applies to all AO routing actions	None
Billing For Successful Delivery	Billing profile to use when the routing action succeeds Applies to: <ul style="list-style-type: none"> • Path AO-AO (to SMSC) • Path AO-AT (to Application) • Path AO-MT (to MT) • Path AO-MT-AO (Try-and-Forward MT), when MT routing succeeds • Discard with ACK 	None
Billing For Failed Delivery	Billing profile to use when the routing action fails Applies to: <ul style="list-style-type: none"> • Path AO-AO (to SMSC) • Path AO-MT-AO (Try-and-Forward MT), when MT routing fails with a permanent error 	None
Billing For Delivery Notification	Billing profile to use for delivery notification Applies to: <ul style="list-style-type: none"> • Path AO-AO (to SMSC) • Path AO-AT (to Application) • Path AO-MT (to MT) • Path AO-MT-AO (Try-and-Forward MT) 	None

Parameter	Description	Default
	<ul style="list-style-type: none"> Discard with ACK 	
Billing For Discarded Messages	Billing profile to use for Discarded messages Applies to: <ul style="list-style-type: none"> Discard with negative acknowledgement. 	None

Path AO-AO (to SMSC):

Parameter	Description	Default
SMSC Group	SMSC group to route to	None
Modified Source Application	Application to use as the source application when forwarding an AO message as AO to an SMSC Note: <i>Outside only</i> applications cannot be used as the modified source application.	None

Path AO-AT (to application):

Parameter	Description	Default
Application	Application to route traffic to	Default to Short Number
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic)	None

Path AO-MT-AO (Try-and-Forward MT):

Parameter	Description	Default
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails	None
SMSC Group	SMSC group to route to	None
Modified Source Application	Application to use as the source application when forwarding an AO message as AO to an SMSC Note: <i>Outside only</i> applications cannot be used as the modified source application.	None

Store for delivery to MS:

Parameter	Description	Default
AMS Queue	AMS queue to use for storage	First defined AMS queue

Route to MS, fallback to storage:

Parameter	Description	Default
AMS Queue	AMS queue to use for storage	First defined AMS queue

Store for delivery to application:

Parameter	Description	Default
Application	Application to route traffic to	Default to Short Number
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic)	None
AMS Queue	AMS queue to use for storage	First defined AMS queue

Route to application, fallback to storage:

Parameter	Description	Default
Application	Application to route traffic to	Default to Short Number
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic)	None
AMS Queue	AMS queue to use for storage	First defined AMS queue

4.4.7 Creating an Incoming AT Routing Rule

Prerequisites:

- Application
- Application category
- Application group
- Billing profile
- External attribute
- Service class
- Modifier

To create an incoming application-terminating routing (ATIR) rule:

1. In the left navigation bar, select **Routing ► Routing Rules ► ATIR**.
The Incoming Application Terminating Routing Rules tab appears.
2. Click **Add New**.
A new Incoming Application Terminating Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The ATIR rule with the highest priority is evaluated first.
6. Set conditions for the rule.
7. From the **Action** list, select a routing action for the rule.
Note: In the case of AT-AT routing, the RTR evaluates ATIR rules before it evaluates ATOR rules.
8. Set the parameters for the routing action, if required.
9. Optionally select an AT modifier from the **Modifier** list.
10. Optionally select a log profile from the **Log Profile** list.
11. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
12. Click **Save**.
The MGR creates the rule and closes the tab.
13. Activate the rule.

4.4.7.1 ATI Rule Conditions

The following table details the conditions that are available for ATIR rules.

Condition	Values	Description
Time Schedule	<ul style="list-style-type: none"> • Always • Schedule 	Condition on the evaluation time of the message: <ul style="list-style-type: none"> • Always: The condition is always true. • Schedule: The condition is true if the current time falls within the schedule as specified by the selected routing schedule, defined in Routing ► Schedules.
Application	<ul style="list-style-type: none"> • None • Application 	Index of the application originating the message.
Application Group	<ul style="list-style-type: none"> • None • Bit string 	Index of the application group associated with the application originating the message.
Application Category	<ul style="list-style-type: none"> • None • Bit string 	Index of the application category associated with the application (with inside session) sending the inbound AT message.

Condition	Values	Description
Service Class	<ul style="list-style-type: none"> • None • Bit string 	Index of the service class associated with the application originating the message.
Message Type	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Normal AT message • 1: Delivery notification 	<p>Indicates which message type applies (each bit corresponds to a message type). If the bit is 1, the message type applies. If the bit is 0, the message type does not apply.</p> <p>Note: Bit 0 is the least significant (last) bit, while bit 2 is the most significant (first) bit.</p>
Protocol	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • UCP • SMPP • CIMD 	The protocol used by the originating application to submit the message.
Operation	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: CP call input operation (01) • 1: UCP multiple address call input operation (02) • 2: UCP call input with supplementary services operation (03) • 3: UCP MS message transfer operation (30) • 4: UCP submit short message operation (51) • 9: UCP operation other than above • 10: SMPP SubmitSm • 12: SMPP SubmitMulti • 13: SMPP DataSm 	The operation used by the originating application to submit the message.

Condition	Values	Description
	<ul style="list-style-type: none"> • 19: SMPP operation other than above • 20: CIMD SubmitMessage • 29: CIMD operation other than above • 30: Operation from another protocol than UCP, SMPP, or CIMD 	
Originator	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List 	The originator specified in the message.
Originator TON	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	The type of number (TON) specified in the originator address of the message.
Originator NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN telephony • 2: Data 	The numbering plan identification (NPI) specified for the recipient of the message.

Condition	Values	Description
	<ul style="list-style-type: none"> • 3: Telex • 4: Reserved • 5: Reserved • 6: Reserved • 7: Reserved • 8: National numbering plan • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	
Recipient	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List 	The recipient specified in the message.
Recipient TON	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	The type of number (TON) specified in the recipient address of the message.

Condition	Values	Description
Recipient NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN telephony • 2: Data • 3: Telex • 4: Reserved • 5: Reserved • 6: Reserved • 7: Reserved • 8: National numbering plan • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	The number plan identifier (NPI) specified in the recipient address of the message.
Priority	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: UCP no priority requested • 1: UCP priority requested • 10: SMPP no priority requested • 11: SMPP priority requested • 20: CIMD priority level 1 (most urgent) • 21: CIMD priority level 2 • 22: CIMD priority level 3 • 23: CIMD priority level 4 • 24: CIMD priority level 5 	The priority level specified in the message.

Condition	Values	Description
	<ul style="list-style-type: none"> • 25: CIMD priority level 6 • 26: CIMD priority level 7 • 27: CIMD priority level 8 • 28: CIMD priority level 9 	
PID	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	The protocol ID specified in the message.
Service Centre	<ul style="list-style-type: none"> • None • Bit string 	<p>Index of the service centre (each bit in the string corresponds to a service centre). If the bit is 1, the service centre (SC) applies. If the bit is 0, the service centre does not apply.</p> <p>Up to 250 service centres can be defined. Therefore, the bit string consists of 250 bits with the least significant (last) bit indicating whether the service centre with SNMP index 1 applies and the most significant (first) bit indicating whether the service centre with SNMP index 250 applies.</p>
SC Timestamp	<ul style="list-style-type: none"> • None • Relative time 	The SC timestamp specified in the message.
Segment Type	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: First segment of a segmented message • 1: Last segment of a segmented message • 2: Neither the first nor the last segment of a segmented message 	<p>Indicates which concatenated message segments apply (each bit corresponds to a segment of a concatenated message). If the bit is 1, the segment applies. If the bit is 0, the segment does not apply.</p> <p>Note:</p> <ul style="list-style-type: none"> • Bit 0 is the least significant (last) bit, while bit 2 is the most significant (first) bit. • Concatenation information received in SMPP SAR TLV (<i>sar_segment_seqnum</i>) is also considered while matching this condition.
Data Coding Scheme (DCS)	<ul style="list-style-type: none"> • None 	The data coding scheme (DCS) specified in the message.

Condition	Values	Description
	<ul style="list-style-type: none"> Byte value (value between 00 and FF, hexadecimal) 	
User Data	<ul style="list-style-type: none"> None Full text Text tag Subtext (contains) Text length 	<p>Content of the message:</p> <ul style="list-style-type: none"> Full text: Compares the entire message content with a defined string. Only evaluates positively if there is an exact match with the user data (message content). Text tag: Compares the first part of the message content with a defined tag-string. Only evaluates positively if the message starts exactly with the defined tag-string. Useful to define a rule on keywords (e.g. *LONG# for CMG SMSCs). Subtext (contains): Compares if the message content contains a defined tag-string. To optimise the search, a start position (default 1) and an end position (default 160) must be specified in which the string is to be found. <p>Note: All message content scanning is case-insensitive.</p>
User Data Header Indication	<ul style="list-style-type: none"> None Bit value <ul style="list-style-type: none"> 0 1 	<p>The user data header (UDH) indication specified in the message.</p> <p>Note: UDH information received in concatenation related SMPP TLVs (<i>sar_msg_ref_num</i>, <i>sar_total_segments</i>, <i>sar_segment_seqnum</i>) is also considered while matching this condition.</p>
User Data Header	<ul style="list-style-type: none"> None Byte value 	<p>Value specified in one of the IEIs of the UDH of the message. Only evaluates positively if there is an exact match with the information element identifier (00-FF, hexadecimal) of the UDH. Refer to technical specification 3GPP 23.040 for more information. Most common information element identifier (IEI) values:</p> <ul style="list-style-type: none"> 00: Concatenated short message 01: Special SMS message indication 04: Application port addressing scheme, 8-bit address 05: Application port addressing scheme, 16-bit address 06: SMSC control parameters 07: UDH Source Indicator <p>Note: UDH information received in concatenation related SMPP TLVs (<i>sar_msg_ref_num</i>,</p>

Condition	Values	Description
		sar_total_segments, sar_segment_seqnum) is also considered while matching this condition.
More Messages To Send	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	The more-messages-to-send indicator specified in the message.
Delivery Status	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0 UCP: in progress • 1 UCP: delivery failed • 2 UCP: delivery successful • 10 SMPP: no status available • 11 SMPP: in progress • 12 SMPP: validity period expired • 13 SMPP: delivery failed • 14 SMPP: delivery successful • 15 SMPP: deleted • 16 SMPP: deleted by cancel • 17 SMPP: scheduled • 18 SMPP: accepted • 19 SMPP: rejected • 20 CIMD: no status available • 21 CIMD: in progress • 22 CIMD: validity period expired • 23 CIMD: delivery failed • 24 CIMD: delivery successful • 25 CIMD: no response 	The delivery status specified in the notification.

Condition	Values	Description
	<ul style="list-style-type: none"> • 26 CIMD: last no response • 27 CIMD: cancelled • 28 CIMD: deleted • 29 CIMD: deleted by cancel 	
Delivery Timestamp	<ul style="list-style-type: none"> • None • Relative time 	The delivery timestamp specified in the notification.
Ext Att	<ul style="list-style-type: none"> • None • External attributes 	A set of 32 attributes, the value of which can be controlled by external applications.
Originator SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual originator subscriber services (defined in SPF Services ► SPF Services) . The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.
Recipient SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual recipient subscriber services. The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.

4.4.7.2 ATI Routing Action Parameters

The following tables detail the parameters for incoming AT routing actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> • Block with permanent message error • Block with permanent recipient error 	None

Route to application:

Parameter	Description	Default
Destination Application	Type of destination application: <ul style="list-style-type: none"> • Incoming Application • Based on Recipient Address • Specify Application • Application From Intermediate Cache (Icache) 	Incoming Application
Specified Destination Application	Destination application to use if the Destination Application setting is <i>Specify Application</i> .	First application on the list

Route to application, fallback to store:

Parameter	Description	Default
AMS Queue	AMS queue to use for storage	First defined AMS queue
Destination Application	Type of destination application: <ul style="list-style-type: none"> • Incoming Application • Based on Recipient Address • Specify Application • Application From Intermediate Cache (Icache) 	Incoming Application
Specified Destination Application	Destination application to use if the Destination Application setting is <i>Specify Application</i> .	First application on the list

Store for delivery to application:

Parameter	Description	Default
AMS Queue	AMS queue to use for storage	First defined AMS queue
Destination Application	Type of destination application: <ul style="list-style-type: none"> • Incoming Application • Based on Recipient Address • Specify Application • Application From Intermediate Cache (Icache) 	Incoming Application
Specified Destination Application	Destination application to use if the Destination Application setting is <i>Specify Application</i> .	First application on the list

Route to SMSC as AO:

Parameter	Description	Default
SMSC Group	SMSC group to which to route the AO message	None
Destination Application	Type of destination application: <ul style="list-style-type: none"> • Incoming Application • Based on Recipient Address • Specify Application • Application From Intermediate Cache (Icache) 	Incoming Application
Specified Destination Application	Destination application to use if the Destination Application setting is <code>Specify Application</code> .	First application on the list

Route to SMSC as AO, fallback to storage:

Parameter	Description	Default
SMSC Group	SMSC group to which to route the AO message	None
AMS Queue	AMS queue to use for storage	First defined AMS queue
Destination Application	Type of destination application: <ul style="list-style-type: none"> • Incoming Application • Based on Recipient Address • Specify Application • Application From Intermediate Cache (Icache) 	Incoming Application
Specified Destination Application	Destination application to use if the Destination Application setting is <code>Specify Application</code> .	First application on the list

Store for forwarding to SMSC as AO:

Parameter	Description	Default
SMSC Group	SMSC group to which to route the AO message	None
AMS Queue	AMS queue to use for storage	First defined AMS queue
Destination Application	Type of destination application: <ul style="list-style-type: none"> • Incoming Application • Based on Recipient Address • Specify Application • Application From Intermediate Cache (Icache) 	Incoming Application
Specified Destination Application	Destination application to use if the Destination Application setting is <code>Specify Application</code> .	First application on the list

4.4.8 Creating an Outgoing AT Routing Rule

Prerequisites:

- Application
- Application category
- Application group
- Billing profile
- External attribute
- Service class

To create an outgoing application-terminating routing (ATOR) rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **ATOR**.
The Outgoing Application Terminating Routing Rules tab appears.
2. Click **Add New**.
A new Outgoing Application Terminating Routing Rules tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 0 (lowest) and 99 (highest); the default is 50. The ATOR rule with the highest priority is evaluated first.
6. Set conditions for the rule.
7. In the **Action Threshold** box, set the maximum number of messages per second that are allowed before the rule takes effect (this parameter only applies when the ATOR rule matches).
8. From the **Outgoing Originator Address Conversion** list, select RuleSet from the list only if it is desired to apply the outgoing address conversion on the originator addresses of all AT messages that would match this rule. By default "No Change" will be selected always. See [Creating Outgoing Address Conversion Rule Sets](#) for more details regarding outgoing address conversion.
9. From the **Outgoing Recipient Address Conversion** list, select RuleSet from the list only if it is desired to apply the outgoing address conversion on the recipient addresses of all AT messages that would match this rule. By default "No Change" will be selected always. See [Creating Outgoing Address Conversion Rule Sets](#) for more details regarding outgoing address conversion.
10. From the **Action** list, select a routing action for the rule.
11. Set the parameters for the routing action, if required.
12. Optionally select a log profile from the **Log Profile** list.
13. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
14. Click **Save**.
The MGR creates the rule and closes the tab.
15. Activate the rule.

4.4.8.1 ATO Rule Conditions

The following table details the conditions that are available for ATOR rules.

Condition	Values	Description
Time Schedule	<ul style="list-style-type: none"> • Always • Schedule 	<p>Condition on the evaluation time of the message:</p> <ul style="list-style-type: none"> • Always: The condition is always true. • Schedule: The condition is true if the current time falls within the schedule as specified by the selected routing schedule, defined in Routing ► Schedules.
Application	<ul style="list-style-type: none"> • None • Application 	Index of the application originating the message.
Application Group	<ul style="list-style-type: none"> • None • Bit string 	Index of the application group associated with the application originating the message.
Application Category	<ul style="list-style-type: none"> • None • Bit string 	Index of the application category associated with the application (with outside session) receiving the outbound AT message.
Service Class	<ul style="list-style-type: none"> • None • Bitstring 	Index of the service class associated with the application originating the message.
Protocol	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • UCP • SMPP • CIMD 	The protocol used by the originating application to submit the message.
Operation	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: CP call input operation (01) • 1: UCP multiple address call input operation (02) • 2: UCP call input with supplementary services operation (03) • 3: UCP MS message transfer operation (30) 	<p>The operation used by the originating application to submit the message.</p> <p>Note: For AT/AT-AT routing paths the ATOC rules cannot be used with the Operation condition (they can only be used on AGW systems).</p>

Condition	Values	Description
	<ul style="list-style-type: none"> • 4: UCP submit short message operation (51) • 9: UCP operation other than above • 10: SMPP SubmitSm • 12: SMPP SubmitMulti • 13: SMPP DataSm • 19: SMPP operation other than above • 20: CIMD SubmitMessage • 29: CIMD operation other than above • 30: Operation from another protocol than UCP, SMPP, or CIMD 	
Protocol Identifier (PID)	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	The protocol ID specified in the message.
More Messages To Send	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	The more-messages-to-send indicator specified in the message.
Originator	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List 	The originator specified in the message.

Condition	Values	Description
Originator TON	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	The type of number (TON) specified in the originator address of the message.
Originator NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN Telephony • 2: Data • 3: Telex • 4: Reserved • 5: Reserved • 6: Reserved • 7: Reserved • 8: National numbering plan • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	The numbering plan identification (NPI) specified for the recipient of the message.
Originator IMSI	<ul style="list-style-type: none"> • None • Single IMSI • IMSI range • County 	The IMSI specified for the originator of the message.

Condition	Values	Description
	<ul style="list-style-type: none"> • Network • List 	
Recipient	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • Single short number • Short number range • Short number prefix • Application • List 	The recipient specified in the message.
Recipient TON	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: International number • 2: National number • 3: Network specific number • 4: Subscriber number • 5: Alphanumeric • 6: Abbreviated number • 7: Reserved 	The type of number (TON) specified in the recipient address of the message.
Recipient NPI	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: Unknown • 1: ISDN Telephony • 2: Data • 3: Telex • 4: Reserved • 5: Reserved • 6: Reserved • 7: Reserved • 8: National numbering plan 	The number plan identifier (NPI) specified in the recipient address of the message.

Condition	Values	Description
	<ul style="list-style-type: none"> • 9: Private numbering plan • 10: ERMES numbering plan • 11: Reserved • 12: Reserved • 13: Reserved • 14: Reserved • 15: Reserved 	
Orig. MSC/SGSN	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • List 	The MSC or SGSN serving the originator specified in the message.
SMSC Address	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix • Country • Network • List 	The SMSC specified in the message.
User Data	<ul style="list-style-type: none"> • None • Full text • Text tag • Subtext (contains) • Text length 	<p>Content of the message:</p> <ul style="list-style-type: none"> • Full text: Compares the entire message content with a defined string. Only evaluates positively if there is an exact match with the user data (message content). • Text tag: Compares the first part of the message content with a defined tag-string. Only evaluates positively if the message starts exactly with the defined tag-string. Useful to define a rule on keywords (e.g. *LONG# for CMG SMSCs). • Subtext (contains): Compares if the message content contains a defined tag-string. To optimise the search, a start position (default 1) and an end position (default 160) must be specified in which the string is to be found. <p>Note: All message content scanning is case-insensitive.</p>

Condition	Values	Description
User Data Header Indication	<ul style="list-style-type: none"> • None • Bit value <ul style="list-style-type: none"> • 0 • 1 	<p>The user data header (UDH) indication specified in the message.</p> <p>Note: UDH information received in concatenation related SMPP TLVs (<i>sar_msg_ref_num</i>, <i>sar_total_segments</i>, <i>sar_segment_seqnum</i>) is also considered while matching this condition.</p>
User Data Header	<ul style="list-style-type: none"> • None • Byte value 	<p>Value specified in one of the IEs of the UDH of the message. Only evaluates positively if there is an exact match with the information element identifier (00-FF, hexadecimal) of the UDH. Refer to technical specification 3GPP 23.040 for more information. Most common information element identifier (IEI) values:</p> <ul style="list-style-type: none"> • 00: Concatenated short message • 01: Special SMS message indication • 04: Application port addressing scheme, 8-bit address • 05: Application port addressing scheme, 16-bit address • 06: SMSC control parameters • 07: UDH Source Indicator <p>Note: UDH information received in concatenation related SMPP TLVs (<i>sar_msg_ref_num</i>, <i>sar_total_segments</i>, <i>sar_segment_seqnum</i>) is also considered while matching this condition.</p>
Priority	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0: UCP no priority requested • 1: UCP priority requested • 10: SMPP no priority requested • 11: SMPP priority requested • 20: CIMD priority level 1 (most urgent) • 21: CIMD priority level 2 • 22: CIMD priority level 3 	<p>The priority level specified in the message.</p>

Condition	Values	Description
	<ul style="list-style-type: none"> • 23: CIMD priority level 4 • 24: CIMD priority level 5 • 25: CIMD priority level 6 • 26: CIMD priority level 7 • 27: CIMD priority level 8 • 28: CIMD priority level 9 	
Message Type	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0 : Normal AT Message • 1 : Delivery Notification 	Condition pertaining to the message type applicable for this message.
Data Coding Scheme (DCS)	<ul style="list-style-type: none"> • None • Byte value (value between 00 and FF, hexadecimal) 	The data coding scheme (DCS) specified in the message.
Concat. Msg. Segments	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • First segment • Last segment • Not first nor last 	The segment sequence number of a concatenated message. Note: Concatenation information received in SMPP TLVs (<i>sar_segment_seqnum</i>) is also considered while matching this condition.
SC Timestamp	<ul style="list-style-type: none"> • None • Relative time 	The service centre (SC) timestamp specified in the message.
Delivery Status	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • 0 UCP: in progress • 1 UCP: delivery failed 	The delivery status specified in the notification. Note: This condition is only applicable for AT-AT scenarios and not applicable for RTR generated notifications.

Condition	Values	Description
	<ul style="list-style-type: none"> • 2 UCP: delivery successful • 10 SMPP: no status available • 11 SMPP: in progress • 12 SMPP: validity period expired • 13 SMPP: delivery failed • 14 SMPP: delivery successful • 15 SMPP: deleted • 16 SMPP: deleted by cancel • 17 SMPP: scheduled • 18 SMPP: accepted • 19 SMPP: rejected • 20 CIMD: no status available • 21 CIMD: in progress • 22 CIMD: validity period expired • 23 CIMD: delivery failed • 24 CIMD: delivery successful • 25 CIMD: no response • 26 CIMD: last no response • 27 CIMD: cancelled • 28 CIMD: deleted • 29 CIMD: deleted by cancel 	
Delivery Timestamp	<ul style="list-style-type: none"> • None • Relative time 	The delivery timestamp specified in the notification.
Ext Att	<ul style="list-style-type: none"> • None • External attributes 	A set of 32 attributes, the value of which can be controlled by external applications.

Condition	Values	Description
XS Message	<ul style="list-style-type: none"> • None • Bit string <ul style="list-style-type: none"> • Not an XS Message • Copy to Application Message • Auto Reply Message • Copy to Email • Forward to Email 	The eXternal Service (XS) message type applicable for this SM.
Originator SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual originator subscriber services (defined in SPF Services ► SPF Services). The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.
Recipient SSI	<ul style="list-style-type: none"> • None • Subscriber Services 	Perform a positive or negative test on one or more individual recipient subscriber services. The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.

4.4.8.2 ATO Routing Action Parameters

The following tables detail the parameters for outgoing AT routing actions.

All outgoing AT routing actions:

Parameter	Description	Default
Billing For Submission	Billing profile to use for submission	None
Billing For Failed Delivery	Billing profile to use when the routing action fails	None

Pass:

Parameter	Description	Default
Billing For Successful Delivery	Billing profile to use when the routing action succeeds	None
Billing For Delivery Notification	Billing profile to use for delivery notification	None

All outgoing AT block actions:

Parameter	Description	Default
Billing for Blocked Delivery	Billing profile to use when the routing rule blocks delivery	None

4.4.9 Creating an IGM Routing Rule

To create an internally generated message routing (IGMR) rule:

1. In the left navigation bar, select **Routing** ► **Routing Rules** ► **IGMR**.

The Internally Generated Message Routing Rules tab appears.

2. Click **Add New**.

A new Internally Generated Message Routing Rules tab appears.

3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.

The priority must be between 0 (lowest) and 99 (highest); the default is 50. Each rule must have a different priority. The rule with the highest priority is evaluated first.

6. Set conditions for the rule.
7. In the **Action** box, select a routing action for the rule.
8. Set the parameters for the routing action, if required.
9. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
10. Click **Save**.

The MGR creates the rule and closes the tab.

11. Activate the rule.

4.4.9.1 IGM Rule Conditions

The IGM rule sets share the following set of supported rule conditions:

Condition	Format	Description
Time Schedule		This condition does not depend on any parameter of the IGM, it evaluates against the current time (local to the RTR instance) at the moment that the rule set is evaluated.
Originator	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized originator address, if it is categorized as MSISDN ⁶ .
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from

⁶ While only ARP messages pass through these rules, both the IGM's originator and recipient are expected to always be categorized as MSISDNs.

Condition	Format	Description
		the normalized MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes. Successful association of the MSISDN with a provisioned mobile network can only happen if mobile number portability is not supported for that network, and if the network and its number range(s)/prefix(es) have been provisioned.
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs, enabling logical OR operation.
Originator SSI		This condition is evaluated against the originator's SSI. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified.
Recipient	General	If an early SRI-SM query was executed for the IGM, both the recipient's MSISDN and IMSI may be available.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized recipient address, if it is categorized as MSISDN ⁶ .
	Country	If the recipient's IMSI has been retrieved, this condition is evaluated against the country, as derived from extracting the mobile country code (MCC) from the IMSI. Otherwise, the condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN. Successful extraction of the country depends on the provisioned countries.
	Network	If the recipient's IMSI has been retrieved, this condition is evaluated against the mobile network, as derived from extracting the mobile network code (MNC) from the IMSI. Otherwise, the condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes. Successful extraction of the mobile network depends on the provisioned mobile networks.
	List	This condition evaluates the normalized MSISDN or IMSI against a list of MSISDNs or IMSIs, enabling logical OR operation.

Condition	Format	Description
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the recipient IMSI, if that IMSI has been retrieved prior to the evaluation of the rule set.
Recipient SSI		This condition is evaluated against the recipient's SSI. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
User Data		This condition is evaluated against the user data of the IGM.
External Attributes		This condition is evaluated against the external attributes as set by the EC application(s) consulted during the evaluation of the IGMX rule set. Due to the nature of the EC rule set evaluation, this condition is only supported in the IGMR and IGMC rule sets.
XS Message		This condition is evaluated against the XS message type of the IGM. As currently, IGM processing only applies to Auto Reply (ARP) messages, this condition should not be used.
Recipient RN Group		This condition is evaluated against the recipient's Routing Number (RN) group. A routing number can be retrieved by issuing an early SRI-SM query, and routing numbers can only ever be extracted when they were provisioned.
Terminating MSC/SGSN	General	The terminating MSC or SGSN address is only available during rule evaluation after a successful early SRI-SM query. If that query returned both an MSC and an SGSN address the condition is evaluate against the address selected by the semi-static configuration setting <code>preferredmtdestination</code> only.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the MSC or SGSN E.164 number.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the MS or SGSN address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the E.164 address against the provisioned mobile network number ranges and/or network prefixes. Successful association of the MSC or SGSN address with a provisioned mobile network can only happen if the network and its number range(s)/prefix(es) have been provisioned.

Condition	Format	Description
	List	This condition evaluates the MSC or SGSN address against a list of E.164 numbers, enabling logical OR operation.

4.4.9.2 IGMR Routing Action

The possible routing actions are:

Action	Effect
Discard	Discard the IGM, and do the post-processing as if the message was successfully delivered.
Reject	Discard the IGM, and do the post-processing as if the delivery of the message failed and the message got dropped.
Route to MS	Try to deliver the IGM to a Mobile Station (MS), no fallback upon failure.
Route to MS, Fallback to Storage	Try to deliver the IGM to an MS, or try to store the IGM in the specified AMS queue upon temporary failure of the first MT delivery attempt.
Store for Delivery to MS	Try to store the IGM in the specified AMS queue, such that the AMS takes care of requesting the delivery of the IGM to an MS. Such IGMR rules only match if, at the time of rule evaluation, at least one AMS is available, which indicates the capability for storing messages (as opposed to Icache functionality only).
Route to Application	<p>Try to deliver the IGM as AT to an application. The destination application is determined by the Application Selection field:</p> <ul style="list-style-type: none"> • By Rule: The IGMR needs to specify the destination application. • By Load Balancing Group: The IGMR needs to specify the load balancing group to be used when determining the destination application. <p>Such IGMR rules only match if, at the time of the rule evaluation, the destination application is available, i.e. there are active outside sessions for the destination application(s).</p>
Route To Application, Fallback to Storage	Try to deliver the IGM as AT to an application, or try to store the IGM in the specified AMS queue upon temporary failure of the first AT delivery attempt. The destination application is determined in the same way as it is for the Route to Application action. Such IGMR rules only match if, at the time of the rule evaluation, either the destination application or the AMS is available.
Store for Delivery to Application	Try to store the IGM in the specified AMS queue, such that the AMS takes care of requesting the delivery of the IGM to an application. The destination application is determined in the same way as it is for the Route to Application action. Such IGMR rules only match if, at the time of rule evaluation, at least one AMS is available.
Route to SMSC as AO	Try to forward the IGM as an AO message to an external SMSC. The IGMR needs to specify both the application to use when forwarding the AO

Action	Effect
	message, and the SMSC group to which the IGM is supposed to be forwarded. Such IGMR rules only match if, at the time of rule evaluation, at least one of the SMSCs in the SMSC group is available to receive AO messages from the designated application.
Route to SMSC as AO, Fallback to Storage	Try to forward the IGM as an AO message to an external SMSC, or try to store the IGM in the specified AMS queue upon temporary failure of the first AO forwarding attempt. The IGMR needs to specify both the application to use when forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded. Such IGMR rules only match if, at the time of rule evaluation, at least one of the SMSCs in the SMSC group is available to receive AO messages from the designated application, or if at least one AMS is available.
Store for Forwarding to SMSC as AO	Try to store the IGM in the specified AMS queue, such that the AMS takes care of requesting the forwarding of the IGM as AO to an external SMSC. The IGMR needs to specify both the application to use when forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded. Such IGMR rules only match if, at the time of rule evaluation, at least one AMS is available.
Route to MS, Fallback to SMSC as AO	Try to deliver the IGM to an MS, or try to forward the IGM as an AO message to an external SMSC upon temporary failure of the first MT delivery attempt. The IGMR needs to specify both the application to use when forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded.

If no IGMR rule matches, the IGM processing continues as if an IGMR with Routing Action "Reject" had matched.

Note: When the selected routing action leads to the an MT or AT delivery attempt, the MTOX or ATOX rule set only gets evaluated for IGMs if the semi-static configuration attribute `outboundextcondrulesenabledforigsm` is set to *true*.

4.4.10 MO Rule Conditions for SIP Originated Message

MO Routing rules support SIP Headers conditions which can be used to determine Routing Action based on SIP Header values received in incoming SIP messages.

If set as "SIP Header", sub-conditions will be matched against SIP header received in incoming SIP Originated message. Four sub-conditions can be provisioned.

Note: SIP Header to be used in Rule Evaluation must be provisioned in SIP Header Screen under IPSPM-GW tab. For example, if user wants to apply condition on SIP header "P-Access-Network-Info"& "P-Visited-Network-Id" then, it should be configured Under the IPSPM-GW tab.

Routing		IPSMGW/sipHeader		Routing/aoRtgRule	
Routing		SIP Headers			
Firewall		ID	Name	Last Updated	
SMS Applications		1	P-Access-Network-Info	2017-02-13 10:11:24	
Environment		3	P-Visited-Network-Id	2017-02-14 10:52:40	
Storage					
IPSMGW					
SIP Headers					
Advanced Filters					

Four SIP Header conditions can be provisioned in MO Rules as in the following image:

Message Segments [cond]:	None		
SIP Header [cond]:	SIP Header		
SIP Header Assignments			
ID	Name	Condition	Value
1	P-Access-Network-Info	Contains	3GPP-E-UTRAN-FDD;utran
2	P-Visited-Network-Id	Does Not Contain	Hello.mnc002.mcc262.3gpp
3	P-Visited-Network-Id	Equals	ims.mnc002.mcc262.3gpp
4	P-Access-Network-Info	Not Equal	3GPP-E-UTRAN-FDD;3gpp
Action:		Discard with acknowledgement	
Billing for Submission:		None	

Each SIP Header condition consists of three parts:

1. Name:

Index to the SIP Header Table. It indicates the SIP Header on which this condition must be applied.

2. Condition type:

This parameter indicates the Condition Type: contains, does not contain, equals, not equal. Default value is none. Below table describe for the condition type.

Condition type	Description
contains	If the condition type is Contains , then the condition will match only if the configured Value string is contained in the corresponding SIP Header of the incoming message.
doesNotContain	If the condition type is Does not Contain , then the condition will match only if the configured Value string is not contained in the corresponding SIP Header of the incoming message.
equals	If the condition type is Equals , then the condition will match only if the configured Value string is exactly contained in the corresponding SIP Header of the incoming message.
notEqual	If the condition type is Not Equal , then the condition will match only if the configured Value string is not exactly contained in the corresponding SIP Header of the incoming message.

3. Value:

This parameter indicates the SIP header value to be searched in corresponding SIP Header in the incoming message. The value can be 255 characters long.

Note: If non-basic ASCII characters are configured in the SIP Header condition, the SNMP commands like "tp_walk" on a terminal may not display the characters properly. This does not mean the configuration is wrong. Please check the SNMP trace to confirm the configuration. The terminal display of the characters depends on the Operating System, Locale setting and language support of the machine where the terminal runs.

4.4.10.1 Processing Logic

On receiving a SIP Originated Message, the IIW parses the message and captures the SIP Header provisioned in the SIP Header table. The IIW forwards the captured headers to the RTR using the internal interface. The RTR further uses the headers in rule evaluation.

Some important points to observe:

1. If the SIP Header provisioned in the condition was not received in the incoming SIP message, then the condition fails and the rule is not matched.
2. Only first 255 bytes of SIP header are captured. The rest are ignored and will not be part of the rule evaluation.
3. The header can be a multi-header in comma separated format or multiple instances of the same header. In both cases the header will be shared in comma separated format.
4. For a SIP multi-header string, the search will be performed on the complete string (including the comma as well) and not just on the last header.
5. Up to 10 SIP headers can be provisioned.
6. Up to 4 SIP header sub-conditions are allowed.
7. Evaluation is performed on the sub-conditions one by one and the combined result is the logical AND of all the sub-conditions.
8. If negation is specified for a SIP condition, then the combined result of all SIP sub-conditions will be reverted.
9. Search will be performed case-insensitive.
10. Leading spaces in the SIP header name are not recommended due to the default behavior in IIW which will truncate the leading spaces (if any) present in a SIP Originated Message.
11. When an incoming SIPO message with more than 255 characters is received by the IIW, the IIW truncates the SIP header and captures only first 255 characters. In case if the 255th character is a space (" "), the IIW & RTR consider it as a character, which further impacts the rule matching as in MGR GUI only 254 characters with condition type as "equal" & SIP header length in the capture is 255 character, then rule will not match.
12. When the IIW receives incoming SIP message with short form of the header name and the SIP header provisioned in the condition with original header name in MGR GUI then condition fails and rule will not be matched.

The following are examples of valid To header fields.

The compact form of the To header field is t.

```
t: sip:+12125551212@server.phone2net.com
```

If the SIP header is configured as To, the condition fails and the rules will not match.

The rule evaluation logic based on the **Condition type**, assuming A, B, C are strings without comma:

Header Value	Condition Value	Condition: contains	Condition: does not contains	Condition: equals	Condition: not equal
A	A	Match	Fail	Match	Fail
AB (A is a substring of AB)	A	Match	Fail	Fail	Match
A;B	A	Match	Fail	Fail	Match
A	A;B	Fail	Match	Fail	Match
A;B	A;B	Match	Fail	Match	Fail
B;A	A;B	Fail	Match	Fail	Match
A;B;C	A;B	Match	Fail	Fail	Match

4.4.10.2 Examples of MO Rule Conditions for SIP Originated Message

Example 1:

If the operator wants to discard a SIP message, using the headers `P-Access-Network-Info` and `P-Visited-Network-Id` with condition types "contains" and "equal", respectively, where:

- The `P-Access-Network-Info` header contains the value "3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=262096ea10014104"
- The `P-Visited-Network-Id` header contains the value "ims.mnc002.mcc262.3gppnetwork.org"

and SIP Header conditions are configured as given in the below example. Here,

```
P-Access-Network-Info: Contains = 3GPP-E-UTRAN-FDD; utran
P-Visited-Network-Info: Equals = ims.mnc002.mcc262.3gppnetwork.org
```

Note: The **Value** box in the GUI displays a limited amount of text, as shown in this example.

If the content of **Value** exists as a substring in the `P-Access-Network-Info` header and a complete string in the `P-Visited-Network-Info` header, then the condition matches and the MO rule will be applied as per the routing action.

Message Segments [cond]: = None

SIP Header [cond]: = SIP Header

SIP Header Assignments			
ID	Name	Condition	Value
1	P-Access-Network-Info	Contains	3GPP-E-UTRAN-FDD;utran
2	P-Visited-Network-Id	Equals	ims.mnc002.mcc262.3gpp
3	None	None	
4	None	None	

Action: ▾ Discard with acknowledgement

Billing for Submission: ▾ None

Example 2:

If the operator wants to route the SIP message using headers P-Access-Network-Info and P-Visited-Network-Id, with condition types "does not contain" and "not equal", respectively, where :

- The P-Access-Network-Info header contains the value "3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=262096ea10014104"
- The P-Visited-Network-Id header contains the value "ims.mnc002.123mcc262.3gppnetwork.org"

and SIP Header conditions are configured as given in the below example. Here,

P-Access-Network-Info: Does Not Contain = 3GPP-E-UTRAN-FDD; utran
 P-Visited-Network-Info: Not Equal = ims.mnc002.mcc262.3gppnetwork.org

Note: The **Value** box in the GUI displays a limited amount of text, as shown in this example.

If the sub-string search for the P-Access-Network-Info header and complete string search for the P-Visited-Network-Info header, as per the configured **Value** (example), is not successful, the condition will be successful and the MO rule will be applied as per the routing action.

Message Segments [cond]: = None

SIP Header [cond]: = SIP Header

SIP Header Assignments			
ID	Name	Condition	Value
1	P-Access-Network-Info	Does Not Contain	3GPP-E-UTRAN-FDD;utran
2	P-Visited-Network-Id	Not Equal	ims.mnc002.mcc262.3gpp
3	None	None	
4	None	None	

Action: ▾ Route to MS

Always Respond With Ack: ▾

Modifier: ▾ None

Billing for Submission: ▾ None

Billing for Successful Delivery: ▾ None

Note: The SIP header conditions are applicable in the MOR/MOX/MOC rule.

4.5 Creating External Condition Rules

Use external condition (EC) rules to process incoming and outgoing messages and forward them to applications that connect to the RTR through the External Condition Interface (ECI). The types of external condition rules are:

- Mobile-originating external condition rules (MOX)
- Incoming mobile-terminating external condition rules (MTIX)
- Outgoing mobile-terminating external condition rules (MTOX)
- Application-originating external condition rules (AOX)
- Incoming application-terminating external condition rules (ATIX)
- Outgoing application-terminating external condition rules (ATOX)
- Internally generated message external condition rules (IGMX)

Note: The MGR automatically assigns an index to each rule when it is created. When you use the `tp_walk` command-line tool to view rule-related counters, the index indicates which rule applies. For example, `moExtCondRuleTotalAppliedCounter.3` provides the number of times that the MO EC rule with index 3 was applied.

4.5.1 Creating an MO External Condition Rule

Prerequisites:

- Device
- External attribute
- External condition application
- Routing number group

The conditions for a mobile-originating external condition routing rule (MOX) are the same as the conditions for a mobile-originating routing rule (MOR).

To create a mobile-originating external condition routing rule (MOX):

1. In the left navigation bar, select **Routing** ► **EC Rules** ► **MOX**.
The Mobile Originating External Conditions tab appears.
2. Click **Add New**.
A new Mobile Originating External Conditions tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 100 (lowest) and 199 (highest); the default is 150.
6. Set conditions for the rule.
7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.
8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.

The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.

9. From the **Failure Action** list, select the action to take when the external condition evaluates to false.
10. Optionally select a log profile from the **Log Profile** list (or select **Default** to use the default log profile).
11. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
12. Click **Save**.
The MGR creates the rule and closes the tab.
13. Activate the rule.

4.5.1.1 MOX Failure Action Parameters

The following tables detail the parameters for MO external condition failure actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> • Discard with negative acknowledgement. • Discard without response. 	None
Return Message	Return Message template to use for this discarded messages Applies to: <ul style="list-style-type: none"> • Discard with negative acknowledgement. • Discard without response. 	None

4.5.2 Creating an Incoming MT External Condition Rule

Prerequisites:

- External condition application

The conditions for an incoming mobile-terminating external condition routing rule (MTIX) are the same as the conditions for an incoming mobile-terminating routing rule (MTIR).

To create an outgoing mobile-terminating external condition routing rule (MTIX):

1. In the left navigation bar, select **Routing** > **EC Rules** > **MTIX**.
The Incoming Mobile Terminating External Conditions tab appears.
2. Click **Add New**.
A new Incoming Mobile Terminating External Conditions tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).

4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.
The priority must be between 100 (lowest) and 199 (highest); the default is 150.
6. Set conditions for the rule.
7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.
8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.
The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.
9. From the **Failure Action** list, select the action to take when the external condition evaluates to false.
10. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
11. Click **Save**.
The MGR creates the rule and closes the tab.
12. Activate the rule.

4.5.2.1 MTIX Rule Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding MTIX rule's external condition), then the processing of the sorted list of matching MTIX rules stops and the failure action of the MTIX rule is applied.

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching MTIX rules, or assume that the message "passed" the MTIX rule evaluation if there are no more matching rules in the list.
Discard With Temporary Error	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with temporary error" had matched.
Discard With Permanent Error	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with permanent error" had matched.
Discard With No Response	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with no response" had matched.
Discard With Ack	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with ACK" had matched.

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following routing action:

1. Discard with permanent error
2. Discard with no response

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Apart from the above stated condition, if the semi-static parameter `rtcreatemtcdrforerrorscenarios` is configured as true, CDRs will also be generated using the billing profile (if configured) for Discarded Messages when the configured billing profile is of 3G CDR format and the message is discarded due to the application of any of the following routing actions:

1. Discard with permanent error
2. Discard with no response
3. Discard with temporary error

4.5.2.2 MTIX Failure Action Parameters

The following tables detail the parameters for incoming MT external condition failure actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> • Discard with permanent error • Discard without response 	None
Billing for Blocked Messages	Billing Profile to use for block message records. Applies to: <ul style="list-style-type: none"> • Discard with temporary error 	None

4.5.2.3 Message Status on CCI Event Log Search for MTIX Rule Failure Action

The message status on CCI for each of the failure action is as below:

Discard with Ack	Deleted
Discard with No Response	Pending
Discard with Permanent Error	Rejected
For Successful Delivery	Delivered

4.5.3 Creating an Outgoing MT External Condition Rule

Prerequisites:

- External attribute
- External condition application

The conditions for an outgoing mobile-terminating external condition routing rule (MTOX) are the same as the conditions for an outgoing mobile-terminating routing rule (MTOR).

To create an outgoing mobile-terminating external condition routing rule (MTOX):

1. In the left navigation bar, select **Routing** ► **EC Rules** ► **MTOX**.
The Outgoing Mobile Terminating External Conditions tab appears.
2. Click **Add New**.
A new Outgoing Mobile Terminating External Conditions tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.
The priority must be between 100 (lowest) and 199 (highest); the default is 150.
6. Set conditions for the rule.
7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.
8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.
The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.
9. From the **Failure Action** list, select the action to take when the external condition evaluates to false.
10. Optionally select a log profile from the **Log Profile** list.
11. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
12. Click **Save**.
The MGR creates the rule and closes the tab.
13. Activate the rule.

4.5.3.1 MTOX Failure Action

If the ECI evaluation produces, after the optional inversion of the corresponding MTOX rule's external condition, a result of FALSE, then, the processing of the sorted list of matching MTOX rules [see the generic description of the evaluation of X rules in the introduction section] stops, and the Failure Action, associated with that MTOX rule gets applied. If the Failure Action is set to "None", then the result of the external evaluation is ignored. Whenever the purpose of the EC application is other than to block certain messages, this Failure Action should be used. All other Failure Actions behave like their MTOX counterparts (see above).

If the ECI evaluated produces a result of false (after the optional inversion of the corresponding MTOX rule's external condition), then the processing of the sorted list of matching MTOX rules stops and the failure action of the MTOX rule is applied.

If the failure action is set to "none", then the result of the external evaluation is ignored. If the purpose of the EC application is anything other than blocking certain messages, this failure action should be used. All other failure actions behave like their MTOX counterparts (see [MTOX Routing Action](#)).

4.5.3.2 MTOX Failure Action Parameters

The following tables detail the parameters for outgoing MT external condition failure actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> Block with permanent error Block with no response 	None
Billing for Blocked Messages	Billing Profile to use for block message records. Applies to: <ul style="list-style-type: none"> Discard with temporary error 	None

4.5.3.3 Message Status on CCI Event Log Search for MTOX Rule Failure Action

The message status on CCI for each of the failure action is as below:

Discard with Ack	Deleted
Discard with No Response	Pending
Discard with Permanent Error	Rejected
For Successful Delivery	Delivered

4.5.4 Creating an AO External Condition Rule

Prerequisites:

- Application
- Application category
- Application group
- CIMD tariff class
- CIMD tariff class description
- External attribute
- External condition application
- Routing number group
- Service class

The conditions for an application-originating external condition routing rule (AOX) are the same as the conditions for an application-originating routing rule (AOR).

To create an application-originating external condition routing rule (AOX):

1. In the left navigation bar, select **Routing** ► **EC Rules** ► **AOX**.
The Application Originating External Conditions tab appears.
2. Click **Add New**.
A new Application Originating External Conditions tab appears.

3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 100 (lowest) and 199 (highest); the default is 150.
6. Set conditions for the rule.
7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.
8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.
The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.
9. From the **Failure Action** list, select the action to take when the external condition evaluates to false.
10. Optionally select a log profile from the **Log Profile** list (or select **Default** to use the default log profile).
11. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
12. Click **Save**.
The MGR creates the rule and closes the tab.
13. Activate the rule.

4.5.4.1 AOX Failure Action Parameters

The following tables detail the parameters for AO external condition failure actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> • Discard with negative acknowledgement. 	None

4.5.5 Creating an Incoming AT External Condition Rule

Prerequisites:

- Application
- Application category
- Application group
- External attribute
- External condition application
- Service class

The conditions for an incoming application-terminating external condition routing rule (ATIX) are the same as the conditions for an incoming application-terminating routing rule (ATIR)

To create an incoming application-terminating external condition routing rule (ATIX):

1. In the left navigation bar, select **Routing** ► **EC Rules** ► **ATIX**.
The Incoming Application Terminating External Conditions tab appears.
2. Click **Add New**.
A new Incoming Application Terminating External Conditions tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 100 (lowest) and 199 (highest); the default is 150.
6. Set conditions for the rule.
7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.
8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.
The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.
9. From the **Failure Action** list, select the action to take when the external condition evaluates to false.
10. Optionally select a log profile from the **Log Profile** list (or select **Default** to use the default log profile).
11. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
12. Click **Save**.
The MGR creates the rule and closes the tab.
13. Activate the rule.

4.5.5.1 ATIX Failure Action Parameters

The following tables detail the parameters for incoming AT external condition failure actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> • Block with permanent error. 	None

4.5.6 Creating an Outgoing AT External Condition Rule

Prerequisites:

- Application
- Application category
- Application group
- External attribute
- External condition application
- Service class

The conditions for an outgoing application-terminating external condition routing rule (ATOX) are the same as the conditions for an outgoing application-terminating routing rule (ATOR).

To create an outgoing application-terminating external condition routing rule (ATOX):

1. In the left navigation bar, select **Routing** ► **EC Rules** ► **ATOX**.
The Outgoing Application Terminating External Conditions tab appears.
2. Click **Add New**.
A new Outgoing Application Terminating External Conditions tab appears.
3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Set the rule's priority in the **Priority** box.
The priority must be between 100 (lowest) and 199 (highest); the default is 150.
6. Set conditions for the rule.
7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.
8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.
The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.
9. From the **Failure Action** list, select the action to take when the external condition evaluates to false.
10. Optionally select a log profile from the **Log Profile** list (or select **Default** to use the default log profile).
11. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.
12. Click **Save**.
The MGR creates the rule and closes the tab.
13. Activate the rule.

4.5.6.1 ATOX Failure Action Parameters

The following tables detail the parameters for outgoing AT external condition failure actions.

Parameter	Description	Default
Billing for Discarded Messages	Billing Profile to use for discard/block message records. Applies to: <ul style="list-style-type: none"> • Block with permanent error. 	None

4.5.7 Creating an IGM External Condition Rule

Prerequisites:

- External condition application

The conditions for an internally generated message external condition routing rule (IGMX) are the same as the conditions for an internally generated message routing rule (IGMR).

To create an internally generated message external condition routing rule (IGMX):

1. In the left navigation bar, select **Routing** ► **EC Rules** ► **IGMX**.

The Internally Generated Message External Conditions tab appears.

2. Click **Add New**.

A new Internally Generated Message External Conditions tab appears.

3. Enter a unique name for the rule in the **Name** box (up to 31 characters).
4. Optionally enter a description of the rule in the **Description** box.
5. Enter the rule's priority in the **Priority** box.

The priority must be between 100 (lowest) and 199 (highest); the default is 150. Each IGMX rule must have a different priority.

6. Set conditions for the rule.

The conditions for IGMX rules are the same as the conditions for IGMR rules.

7. Select the external condition (EC) application that must validate the rule from the **EC Application** list.

8. Optionally, select the **External Attribute Settings** to configure the set of 32 Boolean attributes.

The configured values will be set in the `externalAttribute` field of the ECI evaluation request before sending the same to the EC application.

9. From the **Failure Action** list, select how to treat internally generated messages (IGM) when the external condition evaluates to false:

- None
- Reject (consider the routing result to be failure)
- Discard (consider the routing result to be successful delivery)

10. In the **Device Assignments** section, select the RTR device(s) to which this rule applies.

11. Click **Save**.

The MGR creates the rule and closes the tab.

12. Activate the rule.

4.5.7.1 IGMX Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding IGMX rule's external condition), then the processing of the sorted list of matching IGMX rules stops and the failure action of the IGMX rule is applied.

Possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching IGMX rules, or assume that the message "passed" the IGMX rule evaluation if there are no more matching rules in the list.

Action	Effect
Reject	Leave the IGMX rule evaluation and proceed with the post-processing for the IGM, indicating that the message was not delivered, i.e. dropped.
Discard	Leave the IGMX rule evaluation and proceed with the post-processing for the IGM, indicating that the message was "delivered successfully".

4.6 Creating Counting Rules

Counting rules track the number of messages that meet user-defined criteria. Counting rules are used as inputs to logging profiles.

The types of counting rules correspond to the types of routing rules:

- Mobile-originating counting rules (MOC)
- Incoming mobile-terminating counting rules (MTIC)
- Outgoing mobile-terminating counting rules (MTOC)
- Application-originating counting rules (AOC)
- Incoming application-terminating counting rules (ATIC)
- Outgoing application-terminating counting rules (ATOC)
- Internally generated message counting rules (IGMC)

Note: MTIC and IGMC rules currently do not have a Log Profile option.

4.7 Defining External Condition Applications

External condition (EC) applications connect to the RTR through a proprietary interface, the External Condition Interface (ECI).

4.7.1 Defining EC Application Attributes

EC application attributes are result flags that an EC application can return to the RTR for use in routing.

To define an EC application attribute:

1. In the left navigation bar, select **Routing** ► **EC Applications** ► **Attributes**.

The External Attributes tab appears.

2. Click **Add New**.

A new External Attributes tab appears.

3. Enter a unique name for the attribute in the **Name** box (up to 31 characters).
4. Optionally enter a description of the attribute in the **Description** box.
5. Enter the bit position of the attribute (between 1 and 32) in the **Position** box.

Each attribute must have a unique position.

6. Click **Save**.

The MGR saves the attribute and closes the tab.

4.7.2 Creating EC Applications

To create an EC application:

1. In the left navigation bar, select **Routing** ► **EC Applications** ► **Applications**.

The External Condition Applications tab appears.

2. Click **Add New**.

A new External Condition Applications tab appears.

3. Enter a unique name for the EC application in the **Name** box (up to 31 characters).
4. Optionally enter a description of the EC application in the **Description** box.
5. In the **User Identity** box, enter the user ID that the EC application should use when connecting to the devices.
6. In the **ECI Password** box, enter the password that the EC application should use when connecting to the devices.
7. In the **Client IP White List** box, enter a list of allowed IP addresses of accepted ECI clients for this EC application. If no IP addresses are provisioned, all addresses are allowed and round robin ECI distribution applies (by default, the list is empty).

Note: Steps 7 through 10 are required if key-based ECI load distribution is desired.

Note: To save the IP address list in the database, the EC application configuration must be saved as in step 26. The client IP whitelist must be saved first before the load distribution keys can be configured in step 8, 9, and 10.

8. Check the **Distribution Key Originator** if the originator address should be used as key parameter to calculate the key-based load distribution (default is unchecked). The key can only be selected if at least one IP address is provisioned and saved in the **Client IP White List**.
9. Check the **Distribution Key Recipient** if the recipient address should be used as key parameter to calculate the key-based load distribution (default is unchecked). The key can only be selected if at least one IP address is provisioned and saved in the **Client IP White List**.
10. Check the **Distribution Key Calling Party** if the calling party SCCP address should be used as key parameter to calculate the key-based load distribution (default is unchecked). The calling party SCCP address can contain any combination of the originator Point Code (PC) or the originator Global Title (GT). The key can only be selected if at least one IP address is provisioned and saved in the **Client IP White List**.
11. If the EC application should be allowed to modify fields in the message, select **Modification Allowed** (by default, the EC application is not allowed to modify fields).
12. In the **Max Inactivity Time** box, enter the maximum number of seconds the link to the EC application can be idle before the Router disconnects it (defaults to 60 seconds).
13. In the **Max Response Time** box, enter the maximum number of seconds the Router will wait on an EC application to respond (defaults to 5 seconds).

If set to 0, the Router will not wait on a response.

14. In the **Max Sessions** box, enter the maximum number of sessions allowed between the EC application and the Router (defaults to 128).
15. In the **Throughput** box, enter the maximum number of messages per second allowed for an EC application (defaults to 0).
If set to 0, throughput will be unlimited.
16. Select how the originator should be specified in ECI requests from the **Originator Format** list:
 - Transparent
 - National
 - International
 - System-wide setting (default)
17. Select how the originator should be specified in ECI requests from the **Recipient Format** list:
 - Transparent
 - National
 - International
 - System-wide setting (default)
18. Select how the originator should be specified in ECI requests from the **MSC Format** list:
 - Transparent
 - National
 - International
 - System-wide setting (default)
19. Select how the originator should be specified in ECI requests from the **SMSC Format** list:
 - Transparent
 - National
 - International
 - System-wide setting (default)
20. If, when the RTR cannot connect to the EC application to evaluate a message, the `evaluationResult` field in the `evaluationResponse` message should be set to not connected, select **Not Connected [default]**.
21. If, when the EC application's evaluation of a message times out, the `evaluationResult` field in the `evaluationResponse` message should be set to timeout, select **Timeout [default]**.
22. If, when the EC application's evaluation of a message returns an invalid response, the `evaluationResult` field in the `evaluationResponse` message should be set to invalid response, select **Invalid Response [default]**.
23. If, when the EC application disconnects from the RTR while evaluating a message, the `evaluationResult` field in the `evaluationResponse` message should be set to disconnect, select **Disconnect [default]**.
24. If, when an EC application cannot evaluate a message because the application exceeded its throughput, the `evaluationResult` field in the `evaluationResponse` message should be set to throughput exceeded, select **Throughput Exceeded [default]**.
25. Select the ECI message field(s) that should be included in the request to the EC application.
Refer to [Include ECI Message Fields](#) for an overview and a short description of the fields.

26. Click **Save**.

The MGR creates the EC application and closes the tab.

27. Activate the EC application, as described in [Activate](#).

4.7.2.1 Include ECI Message Fields

Field	Description
Inc. Originator Address:	Indicator specifying whether the field 'originatorAddress' should be included in the ECI evaluationRequest or not. By default, the field is included.
Inc. Originator Imsi:	Indicator specifying whether the field 'originatorImsi' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Originating Application:	Indicator specifying whether the field 'originatingApplication' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Terminating Application:	Indicator specifying whether the field 'terminatingApplication' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Recipient Address:	Indicator specifying whether the field 'recipientAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Recipient Imsi:	Indicator specifying whether the field 'recipientImsi' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Original Submit Time:	Indicator specifying whether the field 'originalSubmitTime' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Unique Submit Time:	Indicator specifying whether the field 'uniqueSubmitTime' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Length Of Message:	Indicator specifying whether the field 'lengthOfMessage' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Priority Indicator:	Indicator specifying whether the field 'priorityIndicator' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. User Data Header Indicator:	Indicator specifying whether the field 'userDataHeaderIndicator' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. More Messages To Send Indicator:	Indicator specifying whether the field 'moreMessagesToSendIndicator' should be included in the ECI evaluationRequest or not. By default, the field is not included.

Field	Description
Inc. Single Shot Indicator:	Indicator specifying whether the field 'singleShotIndicator' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Reply Path Indicator:	Indicator specifying whether the field 'replyPathIndicator' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Notification Request:	Indicator specifying whether the field 'notificationRequest' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Validity Period:	Indicator specifying whether the field 'validityPeriod' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Defer Period:	Indicator specifying whether the field 'deferPerid' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Called Party Address:	Indicator specifying whether the field 'calledPartyAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Destination Point Code:	Indicator specifying whether the field 'destinationPointCode' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Calling Party Address:	Indicator specifying whether the field 'callingPartyAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Originating Point Code:	Indicator specifying whether the field 'originatingPointCode' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Protocol Id:	Indicator specifying whether the field 'protocolId' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Consolidation:	Indicator specifying whether the field 'consolidation' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Billing Identifier:	Indicator specifying whether the field 'billingIdentifier' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. CM Reference Number:	Indicator specifying whether the field 'cmReferenceNumber' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. CM Current Segment:	Indicator specifying whether the field 'cmCurrentSegment' should be included in the ECI evaluationRequest or not. By default, the field is not included.

Field	Description
Inc. CM Total Segments:	Indicator specifying whether the field 'cmTotalSegments' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Tariff Class:	Indicator specifying whether the field 'tariffClass' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Service Description:	Indicator specifying whether the field 'serviceDescription' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Data Coding Scheme:	Indicator specifying whether the field 'dataCodingScheme' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. User Data:	Indicator specifying whether the field 'userData' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. User Data Header:	Indicator specifying whether the field 'userDataHeader' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Delivery Status:	Indicator specifying whether the field 'deliveryStatus' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Notification Address:	Indicator specifying whether the field 'notificationAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Notification PID:	Indicator specifying whether the field 'notificationPid' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Notification Type:	Indicator specifying whether the field 'notificationType' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Delivery Time:	Indicator specifying whether the field 'deliveryTime' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. SMSC Address:	Indicator specifying whether the field 'smscAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. MSC Address:	Indicator specifying whether the field 'mscAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. SGSN Address:	Indicator specifying whether the field 'sgsnAddress' should be included in the ECI evaluationRequest or not. By default, the field is not included.

Field	Description
Inc. TCAP Transaction Id:	Indicator specifying whether the field 'tcapTransactionId' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. LMSI:	Indicator specifying whether the field 'lmsi' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. MW Status:	Indicator specifying whether the field 'mwStatus' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. HLR Error:	Indicator specifying whether the field 'hlrError' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Selected Ext. Condition Rule:	Indicator specifying whether the field 'selectedExternalConditionRule' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Alphanumeric Originator:	Indicator specifying whether the field 'alphanumericOriginator' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Alphanumeric Recipient:	Indicator specifying whether the field 'alphanumericRecipient' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Status Report Info:	Indicator specifying whether the field 'statusReportInfo' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Smpp Message Id:	Indicator specifying whether the field 'smppMessageInfo' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Charge Indication:	Indicator specifying whether the field 'chargeIndication' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Originating App. Charging Units:	Indicator specifying whether the field 'applicationOriginatorChargingUnits' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Recipient App. Charging Units:	Indicator specifying whether the field 'applicationRecipientChargingUnits' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Application Port:	Indicator specifying whether the field 'applicationPort' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Billing Info:	Indicator specifying whether the field 'billingInfo' should be included in the ECI evaluationRequest or not. By default, the field is not included.

Field	Description
Inc. Application Protocol:	Indicator specifying whether the field 'applicationProtocol' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. External Attributes:	Indicator specifying whether the field 'externalAttributes' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Recipient RN:	Indicator specifying whether the field 'recipientRoutingNumber' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Content Rating:	Indicator specifying whether the field 'contentRating' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. XS Service Indicator:	Indicator specifying whether the field 'xsServiceIndicator' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Originator SSI Services:	Indicator specifying whether the field 'originatorSsiServices' should be included in the ECI evaluationRequest or not. By default, the field is not included. The 'originatorSsiServices' field contains a list of originator services <i>active</i> for a subscriber. Refer to the RTR Operator Manual for additional information.
Inc. Masked Originator SSI Service Ids:	Indicator specifying whether the field 'maskedOriginatorSsiServiceIds' should be included in the ECI evaluationRequest or not. By default, the field is not included. The 'maskedOriginatorSsiServiceIds' field contains a list of originator service IDs that are <i>requested</i> to be applied for a subscriber. Refer to the RTR Operator Manual for additional information.
Inc. Recipient SSI Services:	Indicator specifying whether the field 'recipientSsiServices' should be included in the ECI evaluationRequest or not. By default, the field is not included. The 'recipientSsiServices' field contains a list of recipient services <i>active</i> for a subscriber. Refer to the RTR Operator Manual for additional information.
Inc. Masked Recipient SSI Service Ids:	Indicator specifying whether the field 'maskedRecipientSsiServiceIds' should be included in the ECI evaluationRequest or not. By default, the field is not included. The 'maskedRecipientSsiServiceIds' field contains a list of recipient service IDs that are <i>requested</i> to be applied for a subscriber. Refer to the RTR Operator Manual for additional information.

Field	Description
Inc. Unique Event ID:	Indicator specifying whether the field 'smUniqueEventId' should be included in the ECI evaluationRequest or not. By default, the field is not included.
Inc. Requestor SSI Service Name:	Indicator specifying whether the field 'smRequestorSsiServiceName' should be included in the ECI evaluationRequest or not. By default, the field is not included. The 'smRequestorSsiServiceName' field can be used by the PBC to distinguish between the Copy to Phone (CPY) and Copy to Application (CTA) services. Refer to the PBC Operator Manual for additional information.
Inc. Services:	Indicator specifying whether the field 'services' should be included in the ECI evaluationRequest or not. By default, the field is not included. The 'services' field contains a list of service types. Currently only used by the Signature (SIG) service.

4.7.3 Defining EC Messages

To define an external condition message (ECM):

1. In the left navigation bar, select **Routing ► EC Applications ► Messages**.
The External Condition Messages tab appears.
2. Click **Add New**.
A new External Condition Messages tab appears.
3. Enter a unique name for the external condition message in the **Message Name** box.
4. From the **Match On** list, select whether the condition field and result code fields should be checked:
 - Specific Field and Code (default)
 - All Results (have a lower matching precedence)
5. If you selected **Specific Field and Code**, select the **Condition Field**:
 - Message Key (default)
 - Diameter Status
6. If you selected **Specific Field and Code**, enter the result code in the **Result Code** box.
7. From the **Specific EC Application** list, select the EC application that can trigger the generation of a message (select **None** if any application can trigger it).
8. From the **External Condition Result** list, select the ECI evaluation result:
 - Any (default)
 - True Only
 - False Only

9. From the **Enabled For** list, select the type(s) of original message for which a message can be generated:
 - MO Message
 - AO Message

By default, no message type is selected.

10. In the **Message Template** box, enter the template for the message to generate.
A maximum length of 480 bytes or 160 Unicode characters is supported. Template variables are:
 - \$(SCTS) — Service centre timestamp, indicating when the Router accepted the message
 - \$(DESTINATION) — The message's destination address
 - \$(SOURCE) — The message's originator address
 - \$(CODE) — Numeric value of the code input parameter

Sample message template:

```
Your message to $(DESTINATION) was not sent, because your handset might be infected by a virus. Please report code $(CODE) to our Customer Care Centre.
```

11. In the **Message Originator** box, enter the originator address to use for the generated message (if blank, the Router uses its common global title).
The originator can be numeric (up to 20 digits), or alphanumeric (up to 11 GSM default alphabet characters).
 12. From the **Message Recipient** list, select the recipient of the generated message:
 - Original Originator (default)
 - Original Recipient
 - Charged Party
 13. If the MT status report or AT notification should be suppressed when a message has been generated, select the **Suppress Status Report** option (not selected by default).
 14. Click **Save**.
The MGR creates the EC message and closes the tab.
 15. Activate the EC message.
- Note:** Provisioned ECM entries with a smaller index have a higher priority.

4.8 Creating Modifiers

Use modifiers to change fields in a message before it is routed to its destination. Modifiers are used as inputs to routing rules:

- Mobile-originating (MO) modifiers can be applied in MO routing rules (MOR)
- Incoming mobile-terminating (MTI) modifiers can be applied in incoming MT routing (MTIR) rules
- Outgoing mobile-terminating (MTO) modifiers can be applied in outgoing MT routing (MTOR) rules
- Application-originating (AO) modifiers can be applied in AO routing rules (AOR)
- Application-terminating (AT) modifiers can be applied in incoming AT routing rules (ATIR)

4.8.1 Modifier Priority

Message fields can be modified by both routing rule modifiers and external condition (EC) applications. If both modify the same field, the EC application value takes priority.

4.8.2 Creating MO Modifiers

To create a mobile-originating (MO) modifier:

1. In the left navigation bar, select **Routing** ► **Modifiers** ► **MO**.
The MO Modifiers tab appears.
2. Click **Add New**.
A new MO Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to delay/postpone the first delivery of the MO Message, enter a value in the **Delivery Delay** box. The default value is 0, meaning the modifier does not apply any delay. The value for this field is in seconds and the maximum allowed value is 8035200.
6. If you want to modify the message originator, enter an E.164 number in the **Originator** box.
The E.164 number must be:
 - A full number in international format, without international prefix, or
 - A short number
7. If you want to modify the message recipient, enter an E.164 number in the **Recipient** box.
The E.164 number must be:
 - A full number in international format, without international prefix, or
 - A short number
8. If you want to modify the IMSI in the message, enter a value in the **IMSI** box.
9. If you want to remove characters from the beginning of the user data (content) of the message, enter a number in the **User Data chars to strip** box (defaults to 0).
If the user data contains less characters than this number, the user data becomes empty. This functionality is useful for stripping keywords from a message (such as *LONG#). Only the standard GSM character set is supported.
10. If you want to modify the reply path bit, enter a value between -1 and 1 in the **Reply Path** box.
A value of -1 means that the bit should not be modified (this is the default).
11. If you want to modify the status report request bit, enter a value between -1 and 1 in the **Status Report request** box.
A value of -1 means that the bit should not be modified (this is the default).
12. If you want to modify the protocol ID (PID), enter a value between 00 and FF in the **Protocol ID (PID)** box.
A value of -1 means that the PID should not be modified (this is the default).

13. If you want to modify the data coding scheme (DCS), enter a value between 00 and FF in the **Data Coding Scheme (DCS)** box.

A value of -1 means that the DCS should not be modified (this is the default).

Note: It is not recommended to use the MO Modifier if the DCS conversion feature set to japan (i.e. 'hubdcscharcodingconversion' and 'rtrdcscharcodingconversion' set to 'japan'). However, if one uses the MO Modifier and the DCS conversion feature with japan together, the behavior (i.e. user data conversion and character set conversion) is not as per the expectation.

14. If you want to modify the SMSC address at the MAP layer (SM-RP-OA) of incoming MO message, enter an E.164 number (in international format, without international prefix) in the **SMSC Address** box.

The RTR applies the SMSC modifier after applying the routing and external condition rules. Therefore, the RTR will compare an 'SMSC Address' condition in the rules to the SCA field's original value in the incoming message, not the modified value from the modifier. The SMSC modifier affects the MAP layer's SMS-RP-OA field.

15. Click **Save**.

The MGR creates the MO modifier and closes the tab.

16. Activate the modifier.

4.8.3 Creating MTI Modifiers

To create an incoming mobile-terminating (MTI) modifier:

1. In the left navigation bar, select **Routing > Modifiers > MTI**.
The MTI Modifiers tab appears.
2. Click **Add New**.
A new MTI Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. In the Defer Period box, enter the number of seconds to defer the delivery of an MT message.
The modification is applied to the inbound message after MTIR rule evaluation, and only has an effect if the routing action is "store for delivery to MS" or "route to SMSC as AO".
6. Click **Save**.
The MGR creates the modifier and closes the tab.
7. Activate the modifier.

4.8.4 Creating MTO Modifiers

To create an outgoing mobile-terminating (MTO) modifier:

1. In the left navigation bar, select **Routing > Modifiers > MTO**.
The MTO Modifiers tab appears.
2. Click **Add New**.
A new MTO Modifiers tab appears.

3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to modify the time zone, select a new time zone from the **Timezone** list.

This modifier applies to the:

- TP-SCTS (service center timestamp) field of the SMS-DELIVER PDU
- TP-SCTS (service center timestamp) field of the STATUS-REPORT PDU
- TP-DT (discharge time) field of the STATUS-REPORT PDU

The limitations on this modifier are:

- It can only be used on the MO-MT-MO, MO-MT-AT, AO-MT, and MT-MT routing paths
 - It cannot be used on MtForwardSm operations that are issued by an SMSC that the RTR/FWL considers to be suspect
6. If you want to modify the reply path bit, enter a value between -1 and 1 in the **Reply Path** box. A value of -1 means that the bit should not be modified (this is the default).
 7. If you want to modify the SMSC address, enter an E.164 number (in international format, without international prefix) in the **SMSC Address** box.
The RTR applies the SMSC modifier after applying the routing and external condition rules. Therefore, the RTR will compare an SMSC condition in the rules to the SMSC field's original value. The SMSC modifier affects the MAP layer's SMS-RP-OA field.
 8. If you want to modify the message originator format, select a format from the **Originator Format** list:
 - **Transparent**—Do not modify the originator address (default)
 - **National**—Change the originator address to national format
 - **International**—Encode the originator address as international

This modifier overrides the format specified in the `mtoriginatorformatfordomestictraffic` and `mtoriginatorformatformtmtdomestictraffic` parameters in the semi-static configuration file. These parameters take effect only when the modifier is set to **Transparent**.
 9. If you want to modify the originator TON, select the value from the **Originator TON** drop-down list.

Note: For newly created MTO Modifiers, any time the **Originator Format** is changed, the **Originator TON** value will be reset to the default value of the selected **Originator Format** in the MGR GUI.

Example: If the **Originator Format** is **National** and the user changes it to **International**, the **Originator TON** will automatically be reset to 1 (default value for the **International** format).

Default values for the Originator TON

Originator Format	Originator TON
Transparent	-1
International	1
National	0

10. If you want to modify the originator NPI, select the value from the **Originator NPI** drop-down list.

Note: For newly created MTO Modifiers, any time the **Originator Format** is changed, the **Originator NPI** value will be reset to the default value of the selected **Originator Format** in the MGR GUI.

Example: If the **Originator Format** is **National** and the user changes it to **International**, the **Originator NPI** will automatically be reset to 1 (default value for the **International** format).

Default values for the Originator NPI

Originator Format	Originator NPI
Transparent	-1
International	1
National	1

11. If you want to modify the message's SMSC address during SendRoutingInfoForSM (SRI-SM) operations, enter an E.164 number (in international format, without international prefix) in the **SMSC Address for SRI SM Ops** box.
This modifier overrides the `smscaddressforhlroperations` parameter in the semi-static configuration file.
12. If you want to modify the message's SMSC address during ReportSMDeliveryStatus operations, enter an E.164 number (in international format, without international prefix) in the **SMSC Address for Report SM Ops** box.
This modifier overrides the `smscaddressforhlroperations` parameter in the semi-static configuration file.
13. If you want to remove digits from the beginning of the message's SCCP called party address (CdPA) during the SendRoutingInfoForSM operation, enter a number of digits in the **Strip SCCP CdPA of SRISM** box.
14. If you want to add digits to the beginning of the message's SCCP called party address (CdPA) during the SendRoutingInfoForSM operation, enter the digits in the **Prefix SCCP CdPA of SRISM** box.

Note:

1. If the strip and prefix functionalities are used together, stripping occurs before prefixing.
 2. The maximum configurable length of the **Prefix SCCP CdPA of SRISM** is 15 digits. The number of configured prefix digits used to modify the SCCP called party address is decided such that the modified SCCP called party address after adding the prefix to the SCCP called party address is not more than 20 digits. For example, if the configured **Prefix SCCP CdPA of SRISM** is of 10 digits and received SCCP called party address is of 12 digits then only first 8 digits of the configured prefix value will only be used to modify the SCCP called party address.
15. If you want to replace the message's SCCP called party address (CdPA) with a different global title (GT) during the SendRoutingInfoForSM operation, enter the GT in the **Replace SCCP CdPA of SRISM** box.

Note:

- The replace functionality is mutually exclusive with the strip and prefix functionalities. The strip and prefix functionalities can be used together, but neither should be used with the replace functionality.

- This parameter also supports special character 'z' which will be replaced with three-digit Country Code of the Recipient MSISDN. The maximum length of this parameter is 15 octets.
16. If you want to modify the message's SCCP called party address (CDPA) during ReportSMDeliveryStatus operation with the modifiers that were applied during the SendRoutingInfoForSM operation, set the **Apply SCCP CdPA Modifier for Report SM operation** parameter.

SMSC Address for Report SM Ops.:	<input type="text"/>
Strip SCCP CdPA of SRISM:	<input type="text" value="0"/>
Prefix SCCP CdPA of SRISM:	<input type="text"/>
Replace SCCP CdPA of SRISM:	<input type="text"/>
Apply SCCP CdPA Modifier for Report SM operation:	<input type="checkbox"/>
Last Updated:	Auto Generated

Figure 18: MGR GUI screenshot of Apply SCCP CdPA Modifier for Report SM operation checkbox in MTO Modifier properties

Note: This field can be enabled in the MGR GUI when at least one of the following fields contains a valid value:

- **Strip SCCP CdPA of SRISM**
- **Prefix SCCP CdPA of SRISM**
- **Replace SCCP CdPA of SRISM**

17. Click **Save**.

The MGR creates the modifier and closes the tab.

18. Activate the modifier.

Note:

1. The MTO modifier is not applied to intercepted MT traffic (unsolicited TCAP CONTINUE messages) from non-trusted external SMSC. One such scenario for intercepted MT traffic from non-trusted SMSC is when the recipient of the intercepted MT traffic belongs to a different operator. In such scenario the RTR will forward the message to MCS/SGSN without any modification.

The originating external SMSC of an inbound MT message is categorized as trusted if:

- The SMSC address at the SCCP layer (and at the MAP layer, if present) matches the list of trusted SMSCs in the semi-static configuration attribute `firewalltrustedsmsclist`, or
 - If the MT message was received with an originating point code (OPC) that is different from the provisioned STP's.
2. The MT modifiers are not applied on the message's SCCP called party address (CDPA) during early SRISM operation triggered for incoming AO message. But if the parameter **Apply SCCP CdPA Modifier for Report SM operation** is set, then message's SCCP called party address (CDPA) during ReportSMDeliveryStatus operation will be modified as per the applied MTO modifier configuration.
 3. In case early SRISM operation is enabled for incoming AO message, then, on activating a MTO modifier with the configuration to modify the CdPA address of the SRISM request, the RTR will log a warning message in the syslog. The same will be true if early SRISM is enabled for

the incoming AO message when at least one active MTO modifier rule exists on the RTR with the configuration to modify the CdPA address of the SRISM request.

4. With Japanese MNP enabled on the RTR, the MT modifiers are not applied on the message's SCCP called party address (CDPA) when the message delivery is triggered through AMS. In this case the message's SCCP called party address (CDPA) during ReportSMDeliveryStatus operation will be modified as described in section 18.10.5 of RTR Operator Manual.

4.8.5 Creating AO Modifiers

To create an application-originating (AO) modifier:

1. In the left navigation bar, select **Routing > Modifiers > AO**.
The AO Modifiers tab appears.
2. Click **Add New**.
A new AO Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to modify the message's validity period, enter a value in the **Validity Period** box:
 - -1—Do not modify (default)
 - 0—Remove the validity period field (if present)
 - Any other value (up to 16,000,000)—Number of seconds in the future

Note: The AMS treatment of the **Validity Period** takes precedence for messages that pass through the AMS in the course of their routing. Specifically, the AMS will reset a zero, missing, or too-large **Validity Period** to the default value specified in the AMS configuration.

6. If you want to modify the delivery delay, enter a value in the **Delivery Delay** box:
 - -1—Do not modify (default)
 - 0—Remove the delivery delay field (if present)
 - Any other value—Number of seconds in the future

This value affects the:

- `deferred-delivery-time` field for UCP
- `schedule-delivery-time` field for SMPP
- `first-delivery-time` field for CIMD

Note: AO-MT messages that have a delivery delay that is a positive value are normally dropped. Set this property to 0 to remove the field and allow these messages to be routed rather than dropped.

7. If you want to modify the `replace-if-present` bit for SMPP messages, enter a value between -1 and 1 in the **Replace If Present** box.
A value of -1 means that the bit should not be modified (this is the default).
8. If you want to modify the delivery notification request bit, enter a value between -1 and 1 in the **Delivery Notification** box.
A value of -1 means that the bit should not be modified (this is the default).

9. If you want to modify the non-delivery notification request bit, enter a value between -1 and 1 in the **Non Delivery Notification** box.
A value of -1 means that the bit should not be modified (this is the default).
10. If you want to modify the buffered notification request bit, enter a value between -1 and 1 in the **Buffered Notification** box.
A value of -1 means that the bit should not be modified (this is the default).
The delivery notification request bit, non-delivery notification request bit, and buffered notification request bit modifiers are similar to the semi-static configuration attributes `override_delivery_notification_request_for_aoa_messages`, `override_non_delivery_notification_request_for_aoa_messages`, and `override_buffered_notification_request_for_aoa_messages`, respectively. For each bit, you may set the parameter to a non-default value in the MGR or in the semi-static configuration file, but not in both. Changing both items to a non-default value will result in unexpected behaviour. For example, if `Delivery Notification` is set to 1, `override_delivery_notification_request_for_aoa_messages` must be set to -1 (its default).
11. If you want to modify the notification address for UCP messages, enter a value in the **Notification Address** box (up to 38 characters in length).
If the specified value is IGNORE (default), the RTR will not modify the notification address. If no value is specified, the RTR will remove the notification address field.
12. If you want to modify the protocol ID, enter a value between -1 and 255 in the **Protocol Id** box.
A value of -1 means that the protocol ID should not be modified (this is the default).
13. If you want to modify the notification protocol ID for UCP messages, select a value from the **Notification Protocol Id** list:
 - No change (default)
 - None
 - Mobile station
 - Fax group 3
 - X400
 - Menu over PSTN
 - PC application over PSTN
 - PC application over X25
 - PC application over ISDN
 - PC application over TCP/IP
14. If you want to modify the priority flag, select a value from the **Priority** list:
 - No change (default)
 - Background
 - Bulk
 - Low
 - Normal
 - Interactive
 - Medium
 - Urgent
 - High

- Emergency

Note: UCP messages have Boolean priority values representing priority and non-priority delivery. These values correspond to modifier settings Emergency and Normal, respectively. Using other modifier settings on UCP messages may cause inconsistent priority values to appear in CDRs and log files.

15. If you want to modify the message's single-shot indicator bit, enter a value between -1 and 1 in in the **Single Shot Indicator** box:

This field affects the single-shot indicator bit in the FCDR's ASER field in submit and deliver CDRs. A value of -1 means that the bit should not be modified (this is the default).

16. Click **Save**.

The MGR creates the AO modifier and closes the tab.

17. Activate the modifier.

Note: You can change the properties of an active AO modifier; deactivating it is not required.

4.8.6 Creating AT Modifiers

Application-terminating (AT) modifiers can be used with incoming AT routing (ATIR) rules.

To create an AT modifier:

1. In the left navigation bar, select **Routing** ► **Modifiers** ► **AT**.

The AT Modifiers tab appears.

2. Click **Add New**.

A new AT Modifiers tab appears.

3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).

4. Optionally enter a description of the modifier in the **Description** box.

5. If you want to modify the priority flag, select a value from the **Priority** list:

- No change (default)
- Background
- Bulk
- Low
- Normal
- Interactive
- Medium
- Urgent
- High
- Emergency

6. Click **Save**.

The MGR creates the AT modifier and closes the tab.

7. Activate the modifier.

Note: You can change the properties of an active AT modifier; deactivating it is not required.

4.8.7 Priority Values for AO and AT Modifiers

The values that are available for the AO and AT message priority modifiers correspond to:

Priority	SMPP	UCP	CIMD
Background	4	0	9
Bulk	0	0	8
Low	0	0	7
Normal	1	0	6
Interactive	1	1	5
Medium	2	1	4
Urgent	2	1	3
High	3	1	2
Emergency	3	1	1

4.9 Creating Lists

Use lists to group multiple configuration items into a single list that can be used as input to routing and counting rules. Lists simplify configuration; if a list is used in a routing or counting rule and any item in the list matches the rule conditions, the rule evaluates to true.

Lists can contain overlapping entries, and you can modify a list without disabling the list or the associated rule.

4.9.1 Types of Lists

You can define the following types of lists:

List Type	Entry Format	Entry Format Example
MSISDN	<ul style="list-style-type: none"> • Single MSISDN • MSISDN range • MSISDN prefix 	<ul style="list-style-type: none"> • 31689543777 • 31689543700-31689543799 • 3168*
IMSI	<ul style="list-style-type: none"> • Single IMSI • IMSI range • IMSI prefix 	<ul style="list-style-type: none"> • 262013564857956 • 262013564850000-262013564859999 • 26201*
Point code	<ul style="list-style-type: none"> • Single point code • Point code range 	<ul style="list-style-type: none"> • 126 • 120-129

List Type	Entry Format	Entry Format Example
Short number	<ul style="list-style-type: none"> • Single short number • Short number range • Short number prefix 	<ul style="list-style-type: none"> • 5454 • 5000-5999 • 54*
Alphanumeric	<ul style="list-style-type: none"> • Single Alphanumeric address with a maximum of 11 characters GSM from the 3GPP specifications 23.038 	<ul style="list-style-type: none"> • Newnet, Newnet12345
IPAddress Port	IPv6 Address	fd5b:bd9d:c3e0:100::135
	IPv6 Address with Port	[fd5b:bd9d:c3e0:100::135]:5060
	IPv6 Address with Port in alphanumeric format	[fd5b:bd9d:c3e0:100::135]:SIP
	IPv4 Address	172.16.133.55
	IPv4 Address with Port	172.16.133.55:5050
	IPv4 Address with Port in alphanumeric format	172.16.133.55:SIP
	Hostname	hostname
	Hostname with Port	hostname:5050
	Hostname with Port in alphanumeric format	hostname:SIP

Note: Before you create list entries, ensure that you determine the format in which MSISDNs are sent to the RTR, especially with regard to leading zeroes. For example, an MSISDN that is formatted as 31205557788 will not match list entry 0031205557788.

If an alphanumeric port is configured in IPAddress-Port list, then same must be configured in /etc/services files on all traffic element nodes.

If a decimal or alphanumeric port is configured along with an IPv6 address, then the address must be enclosed within square brackets, otherwise there would be a configuration error.

4.9.2 Creating a List

To create a list:

1. In the left navigation bar, select **Routing ► Lists**.
The Lists tab appears.
2. Click **Add New**.
3. Enter a unique name for the list in the **Name** box (up to 31 characters).
4. Optionally enter a description of the list in the **Description** box.

5. Select a type from the **List Type** list:
 - MSISDN
 - IMSI
 - Point code
 - Short number
 - Alphanumeric address
6. In the **List Entries** box, enter the list entries with each entry on a separate line.
Refer to *Types of Lists* for information about the accepted formats for entries in each type of list.
7. Click **Save**.
The MGR saves the list and closes the tab.

4.9.3 Referencing a List

You can reference a list in the following fields in routing and counting rules:

- Originator
- Recipient
- SMSC
- MSC/SGSN

To reference a list:

1. Select **List** from the list next to one of the fields identified above.

A list of defined lists appears.

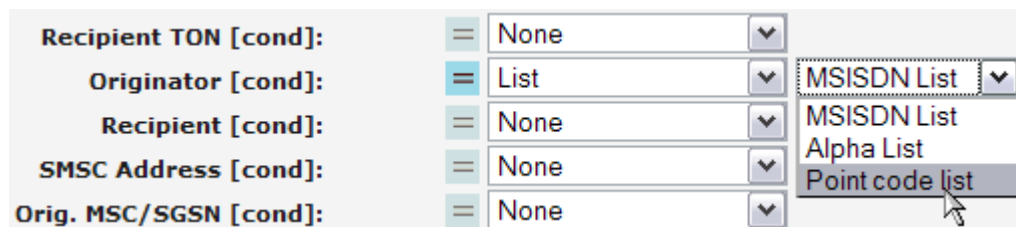


Figure 19: Example of configured lists

2. Select a list.

4.9.4 Creating an ABL List

You can create an ABL List and reference it when configuring an advanced filter with the Blacklist Party as "Originating GT" or "Originating Network".

To create an ABL list:

1. In the left navigation bar, select **Routing ► Lists**.
The Lists tab appears.
2. Click **Add New**.
3. Enter a unique name for the list in the **Name** box (up to 31 characters).

4. Optionally enter a description of the list in the **Description** box.
5. Select **MSISDN** from the **List Type** list.
6. Select the **ABL List** checkbox.

Note: this checkbox is available only for **MSISDN** list type.

Lists

Index:	Auto Generated
Name: ✓	ABL_GT_List
Description:	List of GTs to be blacklisted
List Type: ▾	MSISDN ▾
ABL List: ▶	<input checked="" type="checkbox"/>
List Entries:	<div style="border: 1px solid black; height: 50px;"></div>
Last Updated:	Auto Generated

7. Click **Save**.
The MGR saves the list and closes the tab.

4.9.5 Referencing an ABL List

To reference an ABL list:

Select one of the ABL lists from the **List** field of Advanced Filters.

Note: The **List** field will be shown only when **Blacklist Party** is Originating GT or Originating Network.

Advanced Filters

Index:	Auto Generated
Name: ✓	ABL_GT
Description:	
Priority:	50
Action:	Return True ▼
Blacklist Party: ▼	Originating GT ▼
List: ▶	ABL_GT_List ▼
Blacklist Action: ▶	ABL_GT_List
	ABL_Network_List
Append:	
Last Updated:	Auto Generated

Filter Conditions

4.10 Creating Auto Black List Entries

4.10.1 Types of Blacklisting

Blacklisting Type	Entry Format	Entry Format Example
Originating GT	<ul style="list-style-type: none"> Single MSISDN 	<ul style="list-style-type: none"> 31689543777
Originating Network	<ul style="list-style-type: none"> Single MSISDN MSISDN range MSISDN prefix 	<ul style="list-style-type: none"> 31689543777 31689543700-31689543799 3168*

4.10.2 Creating a Blacklisting Entry

There are 2 ways to create a blacklisting entry:

- Automatic Blacklisting by FAF Provisioning (for more information, refer to the FAF Operator Manual)
- Creating blacklisting entry manually

Note: The command `tp_set` should not be used to modify an existing blacklisting entry and ABL List.

To create an entry to be blacklisted:

1. In the left navigation bar, select **Routing** ► **Others** ► **Auto Black Lists**.
The **Auto Black Lists** tab appears.
2. Click **Add New**.
3. Select the ABL list from the **Related List** field. The new entry will be added to the selected list automatically.
4. Select a type from the **Blacklist Type** list:
 - Originating GT
 - Originating Network
5. If **Blacklist Type** is selected as *Originating GT*, enter the entry value in the **Blacklisted Party** box.
If **Blacklist Type** is selected as *Originating Network*, select a network from the **Related Network** list.
Refer to [Types of Blacklisting](#) for information about the accepted formats for entries.
6. Select the blacklist blocking duration type in the **Duration Type** field.
 - **Permanent**: SMSC GT or Network range will be blocked permanently.
 - **Relative Time-based**: SMSC GT or Network range will be blocked for the duration specified in **Duration** field.
 - **Absolute Time-based**: SMSC GT or Network is to be blacklisted until a specific date time.

Note: If the **Blacklist Action** is **Permanent Blocking**, then continue at step 8.
7. In the **Duration** field, if the **Duration Type** is set to **Relative Time-based**, specify the time for which the subscriber will be blacklisted. The duration should be less than 99 days (the maximum allowed duration is 98 Days 23 Hours 59 Minutes). The minimum duration is 1 Minute. If the **Duration Type** is set to **Absolute Time-based**, specify the last date time for which the subscriber or network should be blacklisted.

Note: For **Absolute Time-based** the option "00" should be used as seconds.
8. Click **Save**.
The MGR saves the list and closes the tab.

4.11 Defining Routing Numbers

A routing number (RN) is a hexadecimal address prefix of up to eight digits. You can define groups of routing numbers for the RTR to compare to the recipient MSISDN, IMSI, or both. You can also define default groups for MSISDNs and IMSIs that do not match a number in an existing group.

Refer to the RTR Operator Manual for more information about how the RTR uses the routing number functionality.

4.11.1 Creating Routing Number Groups

To create a routing number (RN) group:

1. In the left navigation bar, select **Routing > Routing Numbers > RN Groups**.
The Routing Number Group tab appears.
2. Click **Add New**.
A new Routing Number Group tab appears.
3. Enter a unique name for the group in the **Name** box (up to 31 characters).
4. Click **Save**.
The MGR saves the group and closes the tab.

4.11.1.1 Add a Routing Number

To add a number to a routing number (RN) group:

1. In the left navigation bar, select **Routing > Routing Numbers > RN Groups**.
The Routing Number Group tab appears.
2. Click the desired group.
The group opens in a new tab.
3. Click **Add**.
A new Routing Number tab appears.
4. Select the RN group from the **Routing Number Group** list (defaults to the group that you previously selected).
5. Enter the routing number in the **Number** box.
6. If you want the RTR to remove the RN from numbers with a certain TON only, select the TON from the **TON** list.
If you leave the default setting of "all", the RTR will remove the RN from all numbers that match this RN group.
7. If you want the RTR to remove the RN from numbers with a certain NPI only, select the NPI from the **NPI** list.
If you leave the default setting of "all", the RTR will remove the RN from all numbers that match this RN group.

4.11.2 Setting Routing Number Properties

Prerequisites:

- Routing number group

To set routing number properties:

1. In the left navigation bar, select **Routing > Routing Numbers > RN Properties**.
The Routing Number Properties tab appears.
2. Set the following properties:
 - **Enable Matching for Recipient MSISDN**—Select this option if the RTR should attempt to match the MSISDN digits to the routing numbers in the routing number group (disabled by default).
 - **Enable Matching for Recipient IMSI**—Select this option if the RTR should attempt to match the IMSI digits to the routing numbers in the routing number group (disabled by default).

- **Default Group for Recipient MSISDN**—Select the routing number group that should be used if a recipient MSISDN does not match a number in any of the routing number groups (set to “none” by default).
 - **Default Group for Recipient IMSI**—Select the routing number group that should be used if a recipient IMSI does not match a number in any of the routing number groups (set to “none” by default).
3. Click **Save**.

The MGR saves the changes and closes the tab.

4.12 Creating Application Load Balancing Groups

The RTR supports application load balancing groups, which are groups of (ESME) applications among which AT traffic should be load-balanced. The use of a load balancing group is triggered by a matching MO or AO routing rule with an AT-related action (routeToApplication, routeToApplicationFallbackToStorage, or StoreForDeliveryToApplication). If such a rule refers to a load-balancing group, the SM will be sent to one of the applications in that group.

Each application in a load balancing group can be associated with a priority and a weight, governing the load distribution algorithm. An application can be part of multiple load balancing groups.

The decision of which application will receive the AT message is made at AT-delivery time. As such, the SM is not stored to be delivered to a specific application, and the fact that any of the load balancing group's applications connects to the Mobile Messaging system will not trigger the delivery of the SM as AT to that application.

When configured in an MO or AO routing rule, the load-balancing group takes precedence over other mechanisms that would determine the destination application.

Prerequisites:

- Application

To create an application load balancing group:

1. In the left navigation bar, select **Routing ► Load Balancing**.

The Load Balancing Group tab appears.
2. Click **Add New**.

A new Load Balancing Group tab appears.
3. Enter a unique name for the group in the **Name** box (up to 31 characters).
4. Optionally enter a description of the group in the **Description** box.
5. In the **Members** section, select the applications to include in the group.
6. For each application that you select, enter a priority between 0 and 100 in the **Priority** box (default is 50).
7. For each application that you select, enter a weight in the **Weight** box.

For example, an application with a weight of 2 will receive twice as many messages as an application with a weight of 1.

8. Click **Save**.

The MGR creates the application load balancing group and closes the tab.

4.13 Creating Address Conversion Rules

To perform advanced number normalization you can create rules for the conversion of GSM addresses. For addresses that do not need to be converted, no rule is required.

The addresses that result from a conversion are used by the rule processor to match conditions in the routing and counting rules. When no address conversion rules are defined, the RTR uses a scheme for address conversion that is solely based on the NPI/TON supplied with the GSM address.

Refer to the RTR Operator Manual for more information.

4.13.1 Configuring Area Code Properties

To configure fixed-length area code properties for GSM address conversion rules:

1. In the left navigation bar, select **Routing ► Address Conversion ► Properties**.

The Area Code Properties tab appears.

2. In the **Fixed Area Code Length** field enter the number of digits for area code as used in the country in which this Mobile Messaging system operates. Default is 0.

In some countries, the area code has a variable length. If this is the case, the **Fixed Area Code Length** field must be set to 0 and the variable-length area codes should be provisioned in the area code table via **Routing ► Address Conversion ► Area Codes**.

Note: The **Fixed Area Code Length** field cannot be set to a non-zero value when area codes have been provisioned in the area code table.

3. Click **Save**.

The MGR sets the number of digits for the area code and closes the tab.

4.13.2 Configuring Area Codes

To configure area codes in the area code table:

1. In the left navigation bar, select **Routing ► Address Conversion ► Area Codes**.

The Area Codes tab appears.

2. **If you want to ...** **Then ...**

Add an area code

1. Click **Add New**.

A new Area Codes tab appears.

2. In the **Description** field, optionally enter a description for the area code (up to 1024 characters).

If you want to ...	Then ...
	<ol style="list-style-type: none"> 3. In the Area Code field enter the area code to add to the area code table. The area code has a range of 1 up to 6 digits. 4. Click Save. <p>The MGR creates the area code and closes the tab.</p>
Modify an area code	<ol style="list-style-type: none"> 1. In the area code table, click on the area code that you want to modify. The area code opens in a new Area Codes tab. 2. In the Description field, optionally enter a description for the area code (up to 1024 characters). 3. In the Area Code field enter the required area code. The area code has a range of 1 up to 6 digits. 4. Click Save. <p>The MGR saves the area code and closes the tab.</p>
Delete an area code	For instructions on removing an area code, refer to Delete .

4.13.3 Creating GSM Address Conversion Rules

To create a GSM address conversion rule:

1. In the left navigation bar, select **Routing ► Address Conversion ► Conversion Rules**.
The GSM Address Conversion Rules tab appears.
2. Click **Add New**.
A new GSM Address Conversion Rules tab appears
3. Enter a unique description for this conversion rule in the **Description** field (up to 1024 characters).
4. In the **Input TON** field, select the value for Type of Number (TON) that should match with the TON of an address-to-be-converted in order for the GSM address conversion rule to apply.

Possible values are:

- Any
- Unknown (default)
- International
- National
- Network Actual
- Subscriber
- Abbreviated
- Reserved

For details (standard values) refer to 3GPP TS 23.040.

5. In the **Input NPI** field, select the value for Numbering Plan Identification (NPI) that should match with the NPI of an address-to-be-converted in order for the GSM address conversion rule to apply.

Possible values are:

- Any
- Unknown (default)
- ISDN Telephony
- Data
- Telex
- National
- Private
- Ermes

All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.

6. In the **Input Address Prefix** field, enter an input pattern for the prefixing digits of the GSM address.

The pattern is a string (up to 38 characters) and may contain only digits and, optionally, one or more **N** wildcard character(s) and, optionally, one **A** wildcard character, where:

- **A** matches the longest area code defined in the area code table provisioned in **Routing ► Address Conversion ► Area Codes**.

Note: The longest area code match takes priority for multiple applicable matches.

- **N** matches a single digit.

7. In the **Input Minimum Address Length** field, enter the minimum value for length (0 up to 38) of an address-to-be-converted in order for the GSM address conversion rule to apply.

8. In the **Input Maximum Address Length** field, enter the maximum value for length (0 up to 38) of an address-to-be-converted in order for the GSM address conversion rule to apply.

9. In the **Output Address Prefix** field, enter the GSM address output pattern.

This field specifies the output replacement pattern (up to 38⁷ characters) for the prefixing digits of the GSM address. The pattern may contain only digits and, optionally, one or more **N** character(s) and, optionally, one **A** and/or **@** character.

- **A** is replaced by the area code matched by the respective **A** in the input pattern **Input Address Prefix**.
- **N** is replaced by the digit matched by the respective **N** in the input pattern **Input Address Prefix**.
- **@** is replaced by the area code as present in the originator of the message.

Example:

For an input pattern of 12**NAN**33 and an output pattern of 003**A0NN**2, the address 12799633 will be replaced with 003990762, assuming that area code 99 is specified in the area code list provisioned in **Routing ► Address Conversion ► Area Codes**.

Refer to the RTR Operator Manual for more examples.

10. In the **Output Type** field, select how an address should be treated by the rule processor.

Possible values are:

- **determinedByLength** (default), implies that the address type is determined based on the address length. If the length exceeds the threshold that has been configured for the

⁷ If the Output Address Prefix is X characters longer than the Input Address Prefix then the upper limit for Input Minimum Address Length and Input Maximum Address Length is 38 - X

`maxlengthforshortnumber` parameter in the common configuration file, the rule processor will treat the address as an MSISDN. Otherwise, it will be treated as a short number.

- `msisdn`, indicates that the rule processor should treat the address as an MSISDN
- `shortNumber`, indicates that the rule processor should treat the address as a short number.

11. Click **Save**.

The MGR creates the address conversion rule and closes the tab.

4.13.4 Creating Outgoing Address Conversion Rule Sets

Note: **Outgoing Address Conversion Rules** are obsolete from release 16.0. They have been replaced by **Outgoing Address Conversion Rules** under **Outgoing Address Conversion Rule Sets**.

To create an outgoing address conversion rule set:

1. In the left navigation bar, select **Routing** ► **Address Conversion** ► **Out. Rule Sets**.

The Outgoing Address Conversion Rule Sets tab appears.

2. Click **Add New**.

A new Outgoing Address Conversion Rule Set tab appears

3. Enter a Name for this Outgoing Conversion Rule Set in the **Name** field.

4. Click **Save**.

The MGR creates the address conversion rule set and closes the tab.

4.13.4.1 Creating Outgoing Address Conversion Rules

To create an outgoing address conversion rule:

1. Click on the rule set from the list of outgoing address conversion rule sets, under which the user wants to create the new rule.

Outgoing Address Conversion Rule tab appears.

2. Click **Add New**.

3. Enter a name for this outgoing conversion rule in the **Name** field. The **Name** field is optional.

4. Enter a unique description for this conversion rule in the **Description** field (up to 1024 characters).

5. In the **Input TON** field, select the value for the Type of Number (TON) that should match with the TON of an address-to-be-converted in order for the outgoing address conversion rule to apply.

Possible values are:

- Any (wildcard)
- Unknown (default)
- International
- National
- Network Actual
- Subscriber
- Abbreviated
- Reserved

For details (standard values) refer to 3GPP TS 23.040.

6. In the **Input NPI** field, select the value for Numbering Plan Identification (NPI) that should match with the NPI of an address-to-be-converted in order for the outgoing address conversion rule to apply.

Possible values are:

- Any (wildcard)
- Unknown (default)
- ISDN Telephony
- Data
- Telex
- National
- Private
- Ermes

All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.

7. In the **Input Address Prefix** field, enter an input pattern for the prefixing digits of the outgoing address .

The pattern is a string (up to 38 characters) and may contain only digits and, optionally, one or more **N** wildcard character(s) and, optionally, one **A** wildcard character, where:

- **A** matches the longest area code defined in the area code table provisioned in **Routing ► Address Conversion ► Area Codes**.

Note: The longest area code match takes priority for multiple applicable matches.

- **N** matches a single digit.

8. In the **Input Minimum Address Length** field, enter the minimum value for length (0 up to 38) of an address-to-be-converted in order for the outgoing address conversion rule to apply.
9. In the **Input Maximum Address Length** field, enter the maximum value for length (0 up to 38) of an address-to-be-converted in order for the outgoing address conversion rule to apply.
10. In the **Output TON** field, select the value for the Type of Number (TON) that should match with the TON of an address-to-be-converted in order for the outgoing address conversion rule to apply.

Possible values are:

- Default
- Unknown
- International
- National
- Network Actual
- Subscriber
- Alphanumeric
- Abbreviated
- Reserved

For details refer to 3GPP TS 23.040.

11. In the **Output NPI** field, select the value for Numbering Plan Identification (NPI) that should match with the NPI of an address-to-be-converted in order for the outgoing address conversion rule to apply.

Possible values are:

- Default
- Unknown
- ISDN Telephony
- Data
- Telex
- National
- Private
- Ermes

All other values are reserved. For details refer to 3GPP TS 23.040.

12. In the **Output Address Prefix** field, enter the outgoing address output pattern.

This field specifies the output replacement pattern (up to 38⁸ characters) for the prefixing digits of the outgoing address. The pattern may contain only digits and, optionally, one or more N character(s) and, optionally, one A and/or @ character and/or one C character.

- A is replaced by the area code matched by the respective A in the input pattern **Input Address Prefix**.
- N is replaced by the digit matched by the respective N in the input pattern **Input Address Prefix**.
- C is replaced by the Carrier Specific Prefix; if configured in semi-static file.
- @ is replaced by the area code as present in the originator of the message.

Example:

For an input pattern of 12NAN33 and an output pattern of 003CA0NN2, if Carrier Specific Prefix is configured as "41", the address 12799633 will be replaced with 00341990762, assuming that the area code 99 is specified in the area code list provisioned in **Routing ► Address Conversion ► Area Codes**.

Refer to the RTR Operator Manual for more examples.

13. The value of the **Output Address** will specify the exact value of the address to be used in the outgoing message. The **Output Address** field will allow the input as alphanumeric value.

Also the **Output Address Prefix** and **Output Address** will be mutually exclusive fields, i.e. only one of them can be configured at a given point of time.

14. Click **Save**.

The MGR creates the address conversion rule and closes the tab.

⁸ If the Output Address Prefix is X characters longer than the Input Address Prefix then the upper limit for Input Minimum Address Length and Input Maximum Address Length is 38 - X

4.14 Configuring Routing Schedules

Routing schedules can be configured and used when defining a **Time Schedule [cond]** condition in the routing, external condition, or counting rules. The time interval fields are interpreted relative to the RTR's local time. A maximum of 3000 routing schedules can be defined.

To configure a routing schedule:

1. In the left navigation bar, select **Routing ► Schedules**.
The Schedules tab appears.
2. In the **Name** field, enter a name for the schedule.
3. In the **Description** field, optionally enter a short description for the schedule.
4. In the **Year** field, enter the years when the time interval is valid. The range of valid values is 2000 - 2104. The default value is a single asterisk (*).
Refer to [Valid Values](#) for the valid time interval values for this field.
5. In the **Month** field, enter the months of the year when the time interval is valid. The range of valid values is 1 - 12. The default value is a single asterisk (*).
Refer to [Valid Values](#) for the valid time interval values for this field.
6. In the **Day Of Month** field, enter the days of the month when the time interval is valid. The range of valid values is 1 - 31. The default value is a single asterisk (*).
Refer to [Valid Values](#) for the valid time interval values for this field.
Note: It is possible to configure invalid dates (for example, February 31), but the MGR will not give an error or warning for these. Invalid dates are ignored in the RTR.
7. In the **Day Of Week** field, enter the days of the week when the time interval is valid. The range of valid values is 1 - 7, where 1 represents Sunday. The default value is a single asterisk (*).
Refer to [Valid Values](#) for the valid time interval values for this field.
8. In the **Hour** field, enter the hours when the time interval is valid. Specifies hours after midnight. The range of valid numbers is 0 - 23. The default value is a single asterisk (*).
Refer to [Valid Values](#) for the valid time interval values for this field.
9. In the **Minute** field, enter the minutes when the time interval is valid. Specifies minutes after a full hour. The range of valid numbers is 0 - 59. The default value is a single asterisk (*).
Refer to [Valid Values](#) for the valid time interval values for this field.
10. In the **Duration** field, enter a duration in minutes. The duration starts after the most recent period specified by the other time interval fields (**Year**, **Month**, **Day Of Month**, **Day Of Week**, **Hour**, **Minute**). It must be specified as a single number in the range of 0 - 527040 minutes. The default value is 0 minutes.
11. Click **Save**.
The MGR saves the settings and closes the tab.
12. Activate the schedule.
Note: It is allowed to modify time schedule attributes while the schedule is active.

Valid Values

The valid time interval values for the **Year, Month, Day Of Month, Day Of Week, Hour, Minute** fields can be either:

- a single asterisk (*), representing the entire range of valid numbers.
- a single number from the range of valid numbers.
- a list of numbers from the range of valid numbers, separated by a comma (,).
- a range of numbers, separated by a dash (-). Both start and end number are included in the range of numbers. The start number must not be higher than the end number.

4.15 Configuring Routing Properties

To configure routing properties:

1. In the left navigation bar, select **Routing ► Properties**.

The Properties tab appears.

2. In the **Enable Portable Application For MO** check box specify if the Portable Application feature is enabled for incoming MO/SMs. By default, this check box is cleared (disabled).
3. In the **Enable Portable Application For MT** check box specify if the Portable Application feature is enabled for incoming MT/SMs. By default, this check box is cleared (disabled).
4. In the **Early SRI-SM for MO/SM Whitelist** field select a list with conditions that should be matched with the recipient MSISDN of an inbound MO message. If a list is specified, and the corresponding list is provisioned, the setting of **Early SRI-SM for MO/SM** is ignored.

If there is a match, the RTR will issue an HLR query before evaluating the MOX rules. If a list is not specified (default) or does not match with a provisioned condition list, the **Early SRI-SM for MO/SM** parameter is used to control the behaviour of the RTR, independent of the MO message's recipient address.

5. In the **Early SRI-SM for MO/SM** check box specify if an HLR query for the recipient is done before or after the evaluation of the MOX rules. By default, this check box is cleared (disabled).

When disabled, the HLR query for recipient is done after the evaluation of MOX rules. When enabled, the HLR query for recipient precedes the evaluation of MOX rules.

6. In the **Early SRI-SM for AO/SM Whitelist** field select a list with conditions that should be matched with the recipient MSISDN of an inbound AO message. If a list is specified, and the corresponding list is provisioned, the setting of **Early SRI-SM for AO/SM** is ignored.

If there is a match, the RTR will issue an HLR query before evaluating the AOX rules. If a list is not specified (default) or does not match with a provisioned condition list, the **Early SRI-SM for AO/SM** parameter is used to control the behaviour of the RTR, independent of the AO message's recipient address.

7. In the **Early SRI-SM for AO/SM** check box specify if an HLR query for the recipient is done before the evaluation of the AOX rules. By default, this check box is cleared (disabled).

When disabled, the HLR query for the recipient is done depending on the routing path applied to the AO message. An HLR query is only attempted if the recipient number has been recognized as an MSISDN.

8. In the **Early SRI-SM for IGM/SM Whitelist** field select a list with conditions that should be matched with the recipient MSISDN of an Internally Generated SM (IGM). If a list is specified, and the corresponding list is provisioned, the setting of **Early SRI-SM for IGM/SM** is ignored.

If there is a match, the RTR will issue an HLR query before evaluating the IGMX rules. If a list not specified (default) or does not match with a provisioned condition list, the **Early SRI-SM for IGM/SM** parameter is used to control the behaviour of the RTR, independent of the IGM's recipient address.

9. In the **Early SRI-SM for IGM/SM** check box specify if an HLR query for the recipient shall be done before the evaluation of the IGMX rules. By default, this check box is cleared (disabled).

When disabled, the HLR query for the recipient may be done later during the IGM processing, depending on the selected routing path. An HLR query is only attempted if the recipient number has been recognized as an MSISDN.

10. In the **Email Gateway Application** field select the SMS Application corresponding to EMG, in order to provision the Copy to Email and Forward to Email SPF Services.

11. Click **Save**.

The MGR saves the settings and closes the tab.

4.16 Configuring Unicode Conversion Table

The old "MT Character Map" table is replaced by "Unicode Conv." table. This feature obsoletes the backward compatibility of old MT Character Conversion Table.

Follow the below steps to configure a Unicode Conversion table:

1. In the left navigation bar, select **Routing > Others > Unicode Conv.**
The **Unicode Conv** tab appears.
2. Select a **Conversion Table** from 20 default conversion tables.
The selected Conversion Table tab appears.
3. Enter a unique name for the **Conversion Table** in the **Name** box (up to 31 characters).
4. Optionally, enter a description of the **Conversion Table** in the **Description** box.
5. Click **Save**.

The MGR updates the Conversion Table and closes the tab.

Note: User cannot add a new Conversion Table or delete any existing Conversion Table.

4.16.1 Configure Translation Characters

The following policies are applicable for the configuration of Translation Characters:

- Input code point cannot be blank in any Translation Character entry. Please refer section [Configure Single Translation Character](#) for more details.

- Output code point can be blank in any Translation Character entry to remove input code points (i.e *Variation Selectors* or any Unicode Code Point). Please refer section [Configure Single Translation Character](#) for more details.
- Input code point cannot be same as Output code point in any Translation Character entry.
- The same Input code point cannot be mapped with two Output code points.
- Input and Output code point values cannot be greater than 0x10FFFF in any Translation Character entry.
- Input and Output code point values cannot be smaller than 1 in any Translation Character entry.
- Maximum 32000 Translation Character entries can be configured for a single Conversion Table.
- UTF16 surrogate pairs cannot be used directly as Input or Output code point value (varies in the range 0xD800-- 0xDFFF). They should be used as Input and Output after conversion to Hexadecimal Unicode Scalar values.

4.16.1.1 Configure Single Translation Character

Follow the below steps to configure a Single Translation Character:

1. In the left navigation bar, select **Routing > Others > Unicode Conv.**
The **Unicode Character Conversion** tab appears.
2. Select a **Conversion Table**.
The selected **Conversion Table** tab appears.
3. Under Translation Characters, click **Add New**.
A **Conversion Table** tab appears.
4. In **Input** box, enter the input code point with 1 or 2 Unicode code points (first box is mandatory). Only hex values are allowed for this field. The value can optionally be preceded by '0x'.
5. In **Output** box, enter the output code point with 1 or 2 Unicode code points or an empty string to remove input code points. Empty string and hex values are allowed for this field. The value can optionally be preceded by '0x'. Output code point 1 cannot be blank while output code point 2 is filled.
6. Click **Save**.
The MGR closes the Unicode Character Conversion tab and adds the entry in Translation Characters Table.

4.16.1.2 Configure Multiple Translation Characters

Follow the below steps to configure Multiple Translation Characters:

1. In the left navigation bar, select **Routing > Others > Unicode Conv.**
The **Unicode Character Conversion** tab appears.
2. Select a **Conversion Table**.
The selected **Conversion Table** tab appears.
3. Under **Translation Characters**, click **Configure List** if the table has no entry or click **Reconfigure List** if the table has entries.
A new **Conversion Translation** tab appears for file upload.
4. Create an input file in csv format for configuring multiple translation characters. For more information, please refer to section [Creating Input File for Translation Characters](#) .

5. Click the **Choose File** button and select the file created in the previous step.
6. Click **Upload**.
After successful upload, the MGR closes the tab and adds the entry in Translation Characters Table.

4.16.1.3 Creating Input File for Translation Characters

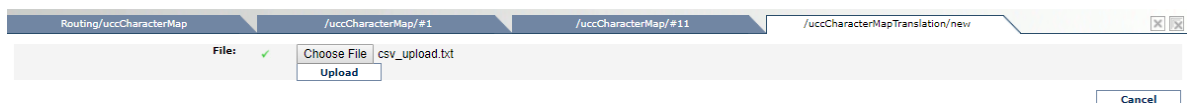
While creating an input file for translation characters, the following restrictions should be taken into consideration:

1. The data in the input file must be in csv format i.e. comma-separated. However, the filename extension does not necessarily have to be ".csv"; any valid filename with or without an extension is supported.
2. The input file is allowed to contain up to 32000 lines and each line contains only one translation character mapping. Each line should have a minimum of 4 columns, with an optional 5th column for description, i.e.
 - 4 columns (first two input code points, last two output code points)
 - 5 columns (first two input code points, next two output code points, last description)
3. First two characters are always the input code point 1 and input code point 2.
4. Optionally, the value of Input or output code points can be preceded by '0x'. However, the value is always considered in hexadecimal format, irrespective of whether it is preceded by '0x'.

The MGR performs the following validation checks on each translation character mapping in the input file:

- Input and output code points:
 - Must be separated by ','
 - Input code point 1 cannot be blank.
 - Output code point 1 cannot be blank while output code point 2 is filled.
 - Must be in hexadecimal format, optionally preceded by '0x'.
 - Cannot be greater than '0x10FFFF' or smaller than '0x1' .
- Output code point 1 and Output code point 2 can be set as blank at the same time, in any Translation Character entry, to remove input code points (i.e *Variation Selectors* or any Unicode Code Points).
- Output code point cannot be the same as Input code point. However, the MGR does not consider the presence of such values as an error in the input file.
- Duplicate input code points cannot be configured in a single conversion table.
- UTF16 surrogate pairs cannot be used directly as Input or Output code point value (varies in the range 0xD800 -- 0xDFFF). They should be used as Input and Output after conversion to Hexadecimal Unicode Scalar values.

If validation fails for a translation entry, MGR will generate an error and user will need to upload the file again after correction.



Sample of valid csv file:

```
A1, ,B11,B12,description1
A21,0xA22,B21,
A31, ,B31, ,description 3
0xA41,A42,0xB41,0xB42
0xFE0F, , ,variation selector
```

4.17 Configuring Mobile Number Portability

Follow the below steps to configure a Mobile Number Portability (MNP) entry:

1. In the left navigation bar, select **Routing** ► **Number Portability**.
The **Number Portability** tab appears.
2. Click **Add New**.
A new **Number Portability** tab appears on the screen.
3. Optionally enter a description of the MNP entry in the **Description** box.
4. In the **Received CdPA Prefix** field, enter a string of up to five hexadecimal digits as the prefix to the SCCP Called Party Address (CdPA) of an incoming SRI-SM Request. By default this field is blank.
5. In the **IMSI** field, enter a string of exactly 15 digits, or a string of 1-14 digits followed by a wildcard (*) character at the end, or a single wildcard (*) character as the recipient IMSI or IMSI prefix. This field is mandatory.
The combination of the **Received CdPA Prefix** and **IMSI** fields in an active MNP entry must be unique. If the **Received CdPA Prefix** field is an empty string (blank) then the same IMSI can be configured for a different MNP entry only if that other entry contains a non-empty CdPA prefix.
6. In the **Action** field, select an action from the drop-down list to be performed by the RTR (By default, MNP action is Accept). For more detailed description on MNP Action, refer to [MNP Action](#).
7. In the **MNP Network Info** field, select a destination network from the drop-down list. The field is applicable when **Action** is set as Forward.
8. In the **Forward Prefix** field, enter a string of up to five hexadecimal digits as a prefix to the SCCP CdPA while forwarding a SRI-SM Request.
Note: The **Forward Prefix** field cannot be left blank when **Action** field is set as 'Forward'.
9. Click **Save**.
The MGR creates the MNP entry and closes the tab.
10. Activate the MNP entry.

4.17.1 MNP Action

The following table describes the supported MNP actions:

MNP Action	Description
Accept	Indicates that the recipient of the message is not a ported subscriber, i.e. the recipient either belongs to the HPLMN or is an international number. In this case

MNP Action	Description
	no further processing related to number portability is required, hence RTR should continue with its normal functionality in order to deliver the message.
Forward	Indicates that the recipient of the message is a ported subscriber. In this case it is required to send a second SRI-SM Request or forward the received SRI-SM Request towards another operator's network, in order to determine the actual destination network for the delivery of the message.
Discard	Indicates that the message should be discarded with a permanent error.

4.18 Configuring Message Template

To create a message template:

1. In the left navigation bar, select **Routing > Others > Message Template**.
The **Message Template** tab appears.
2. Click **Add New**.
A new **Message Template** tab appears on the screen.
3. Enter a unique name for the message template in the **Name** box (up to 31 characters).
4. In the **Translated Originator TON** field, select the value for Type of Number (TON) that should be used for this messages template.

Possible values are:

- Alphanumeric (default)
- Unknown
- International
- National
- Network specific
- Subscriber
- Abbreviated
- Reserved

For details, refer to 3GPP TS 23.040.

5. In the **Translated Originator NPI** field, select the value for Numbering Plan Identification (NPI) that should be used for this message template.

Possible values are:

- Unknown (default)
- ISDN Telephony
- Data
- Telex
- Service Centre specific plan1
- Service Centre specific plan2
- National
- Private

- Ermes
- Reserved

For details, refer to 3GPP TS 23.040.

6. In the **Translated Originator** field, enter an address that should be used by this template as translated originator address for the generated message. The originator can be numeric (up to 20 digits) or alphanumeric (up to 11 GSM default alphabet characters). Information is the default value used by the RTR.
7. In the **Untranslated Originator TON** field, select the value for Type of Number (TON) that should be used for this messages template.

Possible values are:

- Alphanumeric
- Unknown
- International
- National
- Network Specific (default)
- Subscriber
- Abbreviated
- Reserved

For details, refer to 3GPP TS 23.040.

8. In the **Untranslated Originator NPI** field, select the value for Numbering Plan Identification (NPI) that should be used for this message template.

Possible values are:

- Unknown
- ISDN Telephony
- Data
- Telex
- Service Centre specific plan1
- Service Centre specific plan2
- National
- Private (default)
- Ermes
- Reserved

For details, refer to 3GPP TS 23.040.

9. In the **Untranslated Originator** field, enter an address that should be used by this template as untranslated originator address for the generated message.

The originator can be numeric (up to 20 digits) or alphanumeric (up to 11 GSM default alphabet characters). The default value used by the RTR for the untranslated Originator address is 8085.

10. In the **Return Message Template** field, enter the pattern to be used for the return message to be generated.


The pattern supports a maximum length of 480 bytes or 160 Unicode characters if the configured characters are all 3 bytes. By default this pattern is an empty string. The pattern supports the following variables:

- \$(USER_DATA): User Data of the original message
- \$(RCP): Address of the recipient address
- \$(SCTS_2): Service Centre Timestamp formatted according to smsPropDateFormatOfMtReturnMessage.

For details, refer to the "dateformatofmtreturnmessage" parameter, under the Semi-Static Configuration section (tpconfig Entity) of the RTR Operator Manual.

11. Click Save.

The MGR creates the message template and closes the tab.

Message Template Expert View 

Index:	5
Name:	<input type="text" value="MT5"/>
Translated Originator TON:	<input type="text" value="Alphanumeric"/> ▼
Translated Originator NPI:	<input type="text" value="Unknown"/> ▼
Translated Originator:	<input type="text" value="Information"/>
Untranslated Originator TON:	<input type="text" value="Network specific number"/> ▼
Untranslated Originator NPI:	<input type="text" value="Private numbering plan"/> ▼
Untranslated Originator:	<input type="text" value="8085"/>
Return Message Template:	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>
Last Updated:	2017-03-28 08:17:39

Chapter 5

Firewall

Topics:

- *Introduction.....198*
- *Configuring MO Firewall Properties.....198*
- *Configuring MT Firewall Properties.....198*

5.1 Introduction

The Firewall (FWL) is integrated with the RTR and screens and filters incoming messages by applying patented detection techniques.

5.2 Configuring MO Firewall Properties

Prerequisite:

- List

Note: To configure Firewall (FWL) properties, your assigned privileges must include the RTR.

To configure FWL properties for MO routing:

1. In the left navigation bar, select **Firewall > MO > Properties**.
The Firewall Properties tab appears.
2. From the **Fwd. Empty TC-Begin with CdPA** list, select a list that contains addresses that the RTR will match against the SCCP Called Party Address (CdPA) of all empty TCAP BEGIN messages received for MO messages.
The RTR uses this list to determine where to route MO-MO traffic when the destination SMSC is not provisioned in the Mobile Messaging network (an "unknown" SMSC).
3. From the **Fwd. Empty TC-Begin List Type** list, select whether the list is a blacklist or whitelist.
If the CdPA matches an entry in a whitelist or does not match an entry in a blacklist, the RTR will transparently forward the BEGIN message to the external SMSC.
4. Click **Save**.
The MGR saves the properties and closes the tab.

For more information about MO routing to unknown SMSCs, refer to the RTR Operator Manual.

5.3 Configuring MT Firewall Properties

To configure FWL properties, your assigned privileges must include the RTR.

To configure FWL properties for MT routing:

1. In the left navigation bar, select **Firewall > MT > Properties**.
The Firewall Properties tab appears.
2. In the **IMSI Prefixes That Skip Spoofing Detection** box, enter up to 20 IMSI prefixes (separated by commas) for which the FWL will bypass the MT spoofing check for incoming MtForwardSm operations.

The ranges specified must not overlap with the IMSI scrambling ranges that are configured in **Routing > Routing Rules > SRISM Response rules**.

3. From the **MAP Phase Translation** list, indicate the support of MAP Phase Translation for Home Routed scenarios. The default value is "Translation based on App Context Not Supported Error".
4. From the **SRISM GPRS Support Indicator** list, indicate the GPRS support indicator when SRISM is targeted for Home Country and Japanese MNP is ON. The default value is "Default".
5. From the **Trusted SMSC SCCP CgPA List**, select a list that contains addresses that the RTR will match against the SCCP CgPA GT address present in an incoming SendRoutingInfoForSm to bypass the MT spoofing check. If matched, both incoming SRISM and corresponding MTFSM will be treated as 'trusted' and all MT spoofing checks will be bypassed for both messages. The default value is "No List".
6. From the **ReportSmDeliveryStatus GPRS Support Indicator** list, indicate the GPRS support indicator when incoming ReportSmDeliveryStatus Request message from SMSC targeted to an HLR. The default value is "Default".
7. Click **Save**.

The MGR saves the properties and closes the tab.

Sample IMSI Prefix Configuration

An **IMSI Prefixes That Skip Spoofing Detection** value of:

2341655, 234161234

Indicate all IMSIs in the ranges:

- 23416550000000 through 23416559999999, and
- 234161234000000 through 234161234999999

Chapter 6

SMS Applications

Topics:

- *Introduction.....202*
- *Creating SMS Application Groups.....202*
- *Provision an SMS Application.....202*
- *Creating SMS Application Categories.....231*
- *Creating Originator Lists.....232*
- *Creating Portable Applications.....232*
- *Creating CIMD Tariff Classes.....233*
- *Creating CIMD Tariff Class Descriptions.....233*
- *Creating CLI Address Lists.....234*
- *Configuring Character Set Conversion.....235*
- *Configuring Error Mapping Tables.....236*

6.1 Introduction

When your system includes a HUB, you can route SMS traffic from any SMS application to RTRs, SMS gateways, or SMSCs over a variety of application protocols.

6.2 Creating SMS Application Groups

Use SMS application groups to achieve greater control over message throughput to groups of applications. You must create at least one application group.

To create an SMS application group:

1. In the left navigation bar, select **SMS Applications ► Groups**.
The Application Groups tab appears.
2. Click **Add New**.
A new Application Groups tab appears.
3. Enter a unique name for the application group in the **Name** box (up to 31 characters).
4. Optionally enter a description of the application group in the **Description** box.
5. In the **ThroughputAo** box, enter the maximum number of messages per second allowed from the applications in the group (defaults to 65,535).
6. In the **ThroughputAt** box, enter the maximum number of messages per second allowed to the applications in the group (defaults to 65,535).
7. Click **Save**.
The MGR creates the application group and closes the tab.
8. Activate the application group.

6.3 Provision an SMS Application

Prerequisites:

- Application category
- Application group
- Character conversion set

To configure an SMS application:

1. In the left navigation bar, select **SMS Applications ► Applications**.
The SMS Application tab appears.
2. Click **Add New**.
A new SMS Application tab appears.

3. Enter a unique name for the application in the **Name** box (up to 31 characters).
4. Optionally enter a description of the application in the **Description** box.
5. In the **Short Number** box, enter the short number that the application should use to authenticate itself with the RTR.

Note: The limitation on the number of digits of a short number is set with the `tp_install_mgr` command-line tool during the installation phase. The current setting can be verified via **Settings** ► **Global Settings**.

6. In the **Alphanumeric Alias** box, optionally enter up to 10 alphanumeric aliases (separated by semicolons) that the RTR can use to match the application address in case of an AO message that uses an alphanumeric as the originator address.

The alias cannot be a short number. Each alias must be unique across all SMS applications.

7. Optionally select one or more categories from the **Category** list.
8. Select an application group from the **Application Group** list.
9. Select a logging level from the **Log Level** list:

- Error
- Warning (default)
- Info
- Off (disables event logging)

When a generic event occurs, it is logged if its level is equal to or higher than the level selected here.

10. Select the interface type from the **Interface Type** list:

- Universal Computer Protocol (UCP)
- Computer Interface to Message Distribution (CIMD)
- Short message peer-to-peer protocol (SMPP)

11. Select the session model for the application:

- Inside only - All SCs
- Outside only
- Replicate - All SCs
- Distribute - All SCs
- Inside only - SC list
- Replicate - SC list
- Distribute - SC list
- Use service class model (default)

Note: For the MO-AO and MO-MT-AO routing paths, you cannot select **Use service class model**. You must select the session model directly in the application configuration. For these routing paths, the valid session models are **Inside only - All SCs** and **Inside only - SC List**.

12. Set the session model parameters, which vary for each session model.
13. Set the interface-specific parameters.
14. In the **CDR Consolidation Field** box, optionally enter a value of up to 15 characters to use in the `ConsolidationField` in CDRs.

If this field is left blank, the HUB will use the short number.

Note: For CIMD applications, only digits can be used.

15. In the **CCDR Group Id** field box, optionally enter a value in the range 1 (default) - 65535 to use in the following fields of the Comverse CDRs generated for messages originated from or destined to this application:
 - source_ei <group> field
 - group id value included in source_ei <id> field
 - ei:group field
 - group id value included in ei:id field
16. Select one or more service classes from the **Service Class Table** list.
17. In the **FCDR Recipient Address PID** box, enter a value between -1 and 127 to use in the following CDR fields:
 - PID field of FCDR's CallDetailRecord (recipAddress)
 - PID field of FCDR's NotificationRecord (orglRecipAddress)
18. In the **FCDR Originator Address PID** box, enter a value between -1 and 127 to use in the following CDR fields:
 - PID field of FCDR's CallDetailRecord (origAddress and notifAddress)
 - PID field of FCDR's NotificationRecord (orglOrigAddress and orglNotifAddress)

Note: For both FCDR PID fields, a value of -1 mimics legacy behavior (PID value will be 57 for UCP, 59 for SMPP, and 55 for CIMD).
19. To include application-specific charging units for messages sent by this application, select **Use Originator Charging Units**.
20. Enter a number of charging units between 0 and 65,535 in the **Originator Charging Units** box.
21. To include application-specific charging units for messages sent to this application, select **Use Recipient Charging Units**.
22. Enter a number of charging units between 0 and 65,535 in the **Recipient Charging Units** box.

Note: Charging units do not indicate which party should be charged (originator or recipient). They are simply additional parameters that the billing server can take into account when computing the amount to charge.
23. From the **Format MSC** list, select how the MSC should be formatted in an AO or AT message that results from an MO message.
24. From the **Outbound SMPP Destination TON** list, select how the RTR will overwrite the TON in the recipient address for the outbound SMPP messages. This parameter is not applicable for an alphanumeric address. By default, this parameter is set to noChange (-1).
25. From the **Outbound SMPP Destination NPI** list, select how the RTR will overwrite the NPI in the recipient address for the outbound SMPP messages. This parameter is not applicable for an alphanumeric address. By default, this parameter is set to noChange (-1).
26. From the **Format Originator** list, select how the originator should be formatted in an AO or AT message that results from an MO message.
27. From the **Format Recipient** list, select how the recipient should be formatted in an AO or AT message that results from an MO message.

28. From the **Format SMSC** list, select how the SMSC should be formatted in an AO or AT message that results from an MO message.
29. From the **Notification Handling** list, select how the HUB should handle application notifications:
- **Same session preferred** (default)—The notification will be sent over the source session unless it is no longer available or if a specific different notification address is requested. In case of AO-AO routing, this setting only works if the service center to which the AO message gets forwarded also applies functionality to route subsequent notification messages back using the same session.
 - **Same session only**—The notification will be sent over the source session. If the session is no longer available, the notification is discarded. Requests with a specific notification address are forced over the source session.
 - **Dialout preferred**—Notifications with a specific notification address will always be sent using the given address, even if the application has the same dialout address. If no notification address is requested or if the address is not supported, the HUB uses the "same session preferred" behavior.
 - **Dialout only**—Notifications with a specific notification address will always be sent using the given address, even if the application has the same dialout address. If dialout is not allowed or is not possible, the notification is rejected.
 - **Same host only**—If the source session is still available, the notification behavior is the same as Same session preferred. If the source session is not available and the source IP address is available in the send notification request, the HUB will send the notification only on application sessions that originate from the same IP address as defined in the source IP address.
- If dial-out is allowed and requested, the HUB first attempts to use the same session that submitted the message. If that session is not available, the HUB attempts to use a dial-out outside session to the defined notification address. If a session does not exist, then the session selection handling function attempts to start one.
30. From the **Long Message Handling** list, select how the HUB should handle AO messages that exceed the length allowed for an MT message:
- Send as concatenated (default)
 - Send using long last tags
 - Reject
 - Send to SMSC
31. If the HUB should take HLR flags into account to optimize AO-MT delivery attempts, select **Optimised MT Delivery** (cleared by default).
32. If SRI-SM request should be sent with priority, select **Sri-SM Priority** from the dropdown list (High by default).
- Sri-SM Priority** controls the setting of priority field in the SRI-SM Request for messages originated from the application, prior to MT delivery attempt of the message. If this parameter set to 'High' or 'Low', the value of the sm-RP-PRI in the SRI-SM Request will be set to 'TRUE' (1) or 'FALSE' (0) respectively. In case of 'Use message priority', the value of sm-RP-PRI will be set as per the value of the Priority field in individual messages, if it is present; in case no Priority field is present in a particular AO message, the value of sm-RP-PRI in the SRI-SM will be set to 'FALSE'.
33. If AT traffic should be enabled, select **AT Enabled** (selected by default).

This flag indicates whether or not an inbound AT traffic (received from external SMSC) is enabled for this Application. Value of this flag does not influence outbound AT traffic (i.e. disabling this flag will not cause the RTR to block MO-AT, AO-AT or MT-AT traffic towards this Application).

34. If AO traffic should be enabled, select **AO Enabled** (selected by default).

This flag indicates whether or not an inbound AO traffic is enabled for this Application. Value of this flag does not influence the outbound AO traffic towards external SMSCs.

35. If the RTR should perform a first delivery attempt and then, if the attempt fails, fallback to the SMSC, select **AO-MT-AO Enabled** (cleared by default).

36. If the application should be allowed to perform single-shot delivery attempts, select **AO-MT Enabled** (cleared by default).

This flag indicates whether or not this Application can send messages to mobile subscribers (as MT/SM), when the RTR plays the role of an SMSC (i.e. routing paths AO-MT, AO-MT-ST or AO-ST-MT).

37. If the application will use character conversion, select a character conversion set from the **Character Conversion Set** list (defaults to no conversion).

38. In the **Throughput AO Maximum** box, enter the maximum number of messages per second allowed from the application to the NewNet Mobile Messaging system (defaults to 65,535).

39. In the **Throughput AO Committed** box, enter the committed number of messages per second from the application to the NewNet Mobile Messaging system (defaults to 65,535).

40. In the **Throughput AT Maximum** box, enter the maximum number of messages per second allowed from the NewNet Mobile Messaging system to the application (defaults to 65,535).

41. In the **Throughput AT Committed** box, enter the committed number of messages per second from the NewNet Mobile Messaging system to the application (defaults to 65,535).

42. If the HUB should delay AO messages from this application for a period of time before continuing to process them, enter the number of seconds to delay messages in the **AO Delay Time** box.

The maximum number of messages that can be delayed in the HUB at one time for all configured applications is controlled by the `hubmaxqueuedmessages` parameter in the semi-static configuration file.

Note: Setting an AO delay time does not change the way the HUB handles window size. The HUB continues to discard all requests that are received outside the window size for a session.

43. If AT recipient statistics should be collected for the application, select **Enable AT Recipient Statistics** (cleared by default).

44. If the message originator should be replaced:

a) Select **Enable Originator Replacement**.

b) In the **Originator Replacement Address** box, enter the MSISDN, short number, or alphanumeric address that should replace the originator address.

Refer to the RTR Operator Manual for more information about originator replacement.

45. From the **Virtual SMSC type** list, select the Virtual SMSC (VSMSC) type of an application. This type relates to the FCDR format.

Valid values are:

- `public` (default)
- `private`—The VSMSC address of this application (see **Virtual SMSC Address**) is required to be unique among all private VSMSC addresses, assisting in the correct routing of MO-AT traffic.

The value of this parameter influences the `vsmScType` field of FCDRs for AO and AT messages (refer to the RTR Billing Manual for additional information).

When the RTR tries to MT-deliver an AO message from an application that has a VSMSC address provisioned (irrespective of the VSMSC type), the SMSC address at the MAP layer of the `MtForwardSm` will be set to that address, unless it is overruled by an explicit MTO modifier.

This parameter can only be modified while the application is inactive.

46. In the **Virtual SMSC Address** box, enter the VSMSC address associated with this application. The address must be specified in E.164 format, i.e. as internationally significant numbers, starting with the country code. By default, no address (empty string) is specified.

When specified, this value can be used for routing MO traffic for this VSMSC address to this application (as AT/SM), and for delivering AO messages from this application (as MT/SM) using the VSMSC address as the SMSC address. The value of this parameter influences the `vsmScId` field of FCDRs for AO and AT messages (refer to the RTR Billing Manual for additional information).

This parameter can only be modified while the application is inactive.

47. Select **Multi SIM HLR Redirection Bypass** if AO-MT messages originated by this application should use the value of `tpconfig` attribute `smScAddressForMultiSimHlrRedirectionBypass` in all `SendRoutingInfoForSm` and `ReportSmDeliveryStatus` communications between the RTR and HLR (cleared by default).

This value is also used for AO-MT messages that are stored in the AMS during their processing. If no value is defined for `smScAddressForMultiSimHlrRedirectionBypass`, then selecting **Multi SIM HLR Redirection Bypass** has no effect on the message flow.

48. Click **Save**.

The MGR creates the SMS application and closes the tab.

49. Activate the application.

6.3.1 Session Models


The following table details the session models that are available.

Session Model	Description	Options
Inside only	Inbound SMS application sessions are not allowed; the HUB acts as a bridge between the Router (RTR) and service centres	<ul style="list-style-type: none"> All service centres List of service centre(s)
Outside only	Applies to applications for which no other sessions will be set up (applies particularly to AMS)	None
Replicate	One outside session results in many inside sessions (for example, MO-AT traffic or a voting application)	<ul style="list-style-type: none"> All service centres List of service centre(s)
Distribute	One outside message results in one inside session (for example, AO-MT traffic or a bulk SMS application)	<ul style="list-style-type: none"> All service centres


Session Model	Description	Options
		<ul style="list-style-type: none"> List of service centre(s)
Use service class model	Use the session model specified for the service class associated with the outside listener that the application is connected to	None

6.3.2 UCP Applications

The following table details the parameters available for UCP applications.

Parameter	Description	Applicable Session Model	Default
Service Centers	Service centers to which the application will send messages	<ul style="list-style-type: none"> Inside Only - SC list Replicate - SC list Distribute - SC list 	None
Priority	Priority of each selected service centre	<ul style="list-style-type: none"> Inside Only - SC list Replicate - SC list Distribute - SC list 	50
Weight	Weight of traffic sent to the service centre (for example, a service centre with a weight of 2 will receive twice as many messages as a service centre with a weight of 1)	<ul style="list-style-type: none"> Inside Only - SC list Replicate - SC list Distribute - SC list 	1
Outside Authentication Method	Authentication method for the application to use: <ul style="list-style-type: none"> Password authentication CLI authentication One or the other (not both) When password and CLI authentication are both selected, they must both match for the application to be authenticated.	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Outside UCP Password	Password that the application should use when password authentication has been selected as the outside authentication method; click  to generate a password	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list 	None

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> Use service class model 	
Outside CLI Type	Type of CLI authentication that the application should use when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	IP Address
Outside CLI IP Address	IP address to use for CLI authentication when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	12.0.0.1
Outside CLI IP Mask	IP mask to use for matching the IP when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255.255.255.255
Outside CLI TCP Port	Port to use for CLI authentication when CLI authentication has been selected as the outside authentication method (0 indicates that any port will be accepted)	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	0
Outside CLI Type	Type of CLI source address to use: <ul style="list-style-type: none"> Address CLI List 	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs 	Address

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	
CLI List	List of addresses to use for CLI authentication when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Inside Authentication Method	Authentication method for the service centre to use	<ul style="list-style-type: none"> Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Inside UCP Password	Password for the application to use for sessions toward the service centres; click  to generate a password	<ul style="list-style-type: none"> Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Inside UCP Window Size	Window size to use on links between the HUB and the service centre	<ul style="list-style-type: none"> Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	100
Number of SMSC Only Sessions	Number of sessions to set up toward each SMSC	<ul style="list-style-type: none"> Inside only - All SCs Inside only - SC list 	1

Parameter	Description	Applicable Session Model	Default
Allow Notification	Controls whether delivery notifications are allowed for AO-MT messages; if the application requests notification and it is not allowed, the HUB rejects the message	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Selected
Send Short Ack	Controls whether to send acknowledgment to the Application for an outside session request as soon as the HUB receives the first positive acknowledgment from an SMSC(IP) and successfully sets up one inside session. This is applicable only in case of Replicate and Distribute Session Model, or in the case of Use Service Class Model provided the application is associated with a service class configured with either Replicate or Distribute Session Model.	<ul style="list-style-type: none"> • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Not selected
Notification Address Mode	The mode to use for handling notification addresses in outbound AO messages: <ul style="list-style-type: none"> • Transparent—Pass the notification address transparently to the Service Center. • Clear—Erase the notification address, effectively requesting the notification to be returned by the Service Center over the same session as used for issuing the outbound AO message. 	<ul style="list-style-type: none"> • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Transparent
Ams Queue For Dialout Notifications	Specifies the AMS queue to use for dialout notifications. If None is selected, the dialout notifications are sent to the globally configured queue.	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None

Parameter	Description	Applicable Session Model	Default
TCP Keep-Alive	<p>Activates the TCP keep-alive functionality on connections from this application:</p> <ul style="list-style-type: none"> For outside sessions that are successfully authenticated after TCP keep-alive is activated As soon as the connection is started for inside sessions and outside dial-out sessions 	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	False
Outside Max Inactivity Time	Maximum number of seconds that a link to an application can be inactive before the HUB disconnects it	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	60
Outside Max Response Time	<p>Maximum number of seconds that the HUB waits for a response from an application before considering it to be timed out.</p> <p>The Outside Max Response Time, should relate to the (RTR's)hubmaxresponsetime attribute (default of 15 seconds) as follows:</p> $T < \text{hubmaxresponsetime} / (1 + (\max(\text{round_down}(W/4), 10) / W))$ <p>Where T is the application's Outside Max Response Time, and W is the application's applicable outside window.</p>	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	5
Max Outside UCP Sessions	Maximum number of links between the HUB and the application	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255
Outside UCP Window Size	Window size to use on links between the HUB and the application	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs 	100

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> • Distribute - SC list • Use service class model 	
Respond After Delivery	Controls whether the RTR generates a response after delivery of a message to an MS	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Cleared
Outside Dialout Type	Type of dialout connection to use if a dialout request is received on the dialout listen port or in the case of permanent dialout	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Outside Dialout TCP Port	TCP port to use for a dialout connection; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	
Outside Dialout Inactivity Time	Maximum number of seconds that an outside dialout link to an application is idle before the HUB disconnects it; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	60
Outside Dialout IP Address	IP address to use for a dialout connection only applies if outside dialout type is IP; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list 	127.0.0.1

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> • Distribute - All SCs • Distribute - SC list • Use service class model 	
Outside Dialout Max Sessions	Maximum number of dialout sessions between the application and the HUB; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	0
Outside Dialout UCP Window Size	Window size used on links between the application and the HUB; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	1
UCP Forward Error Map	Forward error mapping table to use for this application	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Default UCP forward error map
UCP Reverse Error Map	Reverse error mapping table to use for this application	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Default UCP reverse error map


Note: Application passwords are encoded in the MySQL database.


6.3.3 SMPP Applications

The following table details the parameters available for SMPP applications.

Parameter	Description	Applicable Session Model	Default
Service Centres	Service centre(s) to which the application will send messages	<ul style="list-style-type: none"> • Inside Only - SC list • Replicate - SC list • Distribute - SC list 	None
Priority	Priority of each selected service centre	<ul style="list-style-type: none"> • Inside Only - SC list • Replicate - SC list • Distribute - SC list 	50
Weight	Weight of traffic sent to the service centre (for example, a service centre with a weight of 2 will receive twice as many messages as a service centre with a weight of 1)	<ul style="list-style-type: none"> • Inside Only - SC list • Replicate - SC list • Distribute - SC list 	1
Outside SMPP Address Range	Range of MSISDNs that can potentially be routed to the application	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Outside Type of Number (TON)	TON of the SMS application address	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Unknown
Outside Numbering Plan Id (NPI)	NPI of the SMS application address	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Max Outside RC Links	Maximum number of simultaneous SMPP receiver links that the application can establish toward the HUB	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list 	255

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> Distribute - All SCs Distribute - SC list Use service class model 	
Max Outside TM Links	Maximum number of simultaneous SMPP transmitter links that the application can establish toward the HUB	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255
Max Outside TC Links	Maximum number of simultaneous SMPP transceiver links that the application can establish toward the HUB	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255
Outside SMPP Transmit Window Size	<p>Transmitting window size used on the links between TextPass and the Application on bind type BIND_RECEIVE/BIND_TRANSRECEIVER and used for sending AT messages to application. Only applicable if TextPass and the Application interface through SMPP.</p> <p>The valid range for this parameter is 1-1024.</p>	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255
Outside SMPP Receive Window Size	<p>Receiving window size used on the links between TextPass and the application on bind type BIND_TRANSMIT/BIND_TRANSRECEIVER and used for receiving AO messages from application. Only applicable if TextPass and the Application interface through SMPP.</p> <p>The valid range for this parameter is 1-1024.</p>	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255
Outside Authentication Method	<p>Authentication method for the application to use:</p> <ul style="list-style-type: none"> Password authentication CLI authentication 	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list 	None

Parameter	Description	Applicable Session Model	Default
	<ul style="list-style-type: none"> One or the other (not both) <p>When password and CLI authentication are both selected, they must both match for the application to be authenticated.</p>	<ul style="list-style-type: none"> Distribute - All SCs Distribute - SC list Use service class model 	
Outside SMPP Password	<p>Password that the application should use when password authentication has been selected as the outside authentication method; click  to generate a password</p>	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Outside CLI Type	Type of CLI authentication that the application should use when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	IP Address
Outside CLI IP Address	IP address to use for CLI authentication when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	12.0.0.1
Outside CLI IP Mask	IP mask to use for matching the IP when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255.255.255.255
Outside CLI Type	<p>Type of CLI source address to use:</p> <ul style="list-style-type: none"> Address CLI List 	<ul style="list-style-type: none"> Outside only Inside only - All SCs Inside only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Address

Parameter	Description	Applicable Session Model	Default
CLI List	List of addresses to use for CLI authentication when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	
Outside CLI TCP Port	Port to use for CLI authentication when CLI authentication has been selected as the outside authentication method (0 indicates that any port will be accepted)	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	0
Inside Authentication Method	Authentication method for the service centre to use	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Inside SMPP Password	Password for the application to use for sessions toward the service centres; click  to generate a password	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list • Use service class model 	None
Inside SMPP Window Size	Window size to use on links between the HUB and the service centre. The valid range for this parameter is 1-1024.	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list • Use service class model 	255
Number of SMSC Only Sessions	Number of sessions to set up toward each SMSC	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list • Use service class model 	1
Inside SMPP Version	Defines the SMPP bind behaviour: <ul style="list-style-type: none"> • SMPP v3.3: Receiver and transmitter sessions will be set up 	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list • Use service class model 	SMPP v3.4

Parameter	Description	Applicable Session Model	Default
	<ul style="list-style-type: none"> SMPP v3.4: Receiver, transmitter, and transceiver sessions will be set up SMPP v5.0: Receiver, transmitter, and transceiver sessions will be set up 		
Inside SMPP Bind Type	Defines the SMPP v3.4 bind type: <ul style="list-style-type: none"> Transceiver Separate Transceiver 	<ul style="list-style-type: none"> Inside Only - All SCs Inside Only - SC list Use service class model 	Transceiver
Allow Notification	Controls whether delivery notifications are allowed for AO-MT messages; if the application requests notification and it is not allowed, the HUB rejects the message	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Selected
Send Short Ack	Controls whether to send acknowledgment to the Application for an outside session request as soon as the HUB receives the first positive acknowledgment from an SMSC(IP) and successfully sets up one inside session. This is applicable only in case of Replicate and Distribute Session Model, or in the case of Use Service Class Model provided the application is associated with a service class configured with either Replicate or Distribute Session Model.	<ul style="list-style-type: none"> Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Not selected
Notification Address Mode	The mode to use for the notification address: <ul style="list-style-type: none"> Transparent—Pass the notification address Clear—Force the address to session-only notification Common IP—Use common IP address of the HUB, including application inside dialout listen port Own IP—Use own IP address of the HUB, including application inside dialout listen port 	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Transparent

Parameter	Description	Applicable Session Model	Default
TCP Keep-Alive	<p>Activates the TCP keep-alive functionality on connections from this application:</p> <ul style="list-style-type: none"> For outside sessions that are successfully authenticated after TCP keep-alive is activated As soon as the connection is started for inside sessions and outside dial-out sessions 	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	False
Outside Max Inactivity Time	Maximum number of seconds that a link to an application can be inactive before the HUB disconnects it	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	60
Outside Max Response Time	<p>Maximum number of seconds that the HUB waits for a response from an application before considering it to be timed out.</p> <p>The Outside Max Response Time, should relate to the (RTR's)hubmaxresponsetime attribute (default of 15 seconds) as follows:</p> $T < \text{hubmaxresponsetime} / (1 + (\max(\text{round_down}(W/4), 10) / W))$ <p>Where T is the application's Outside Max Response Time, and W is the application's applicable outside window.</p>	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	5
Respond After Delivery	Controls whether the RTR generates a response after delivery of a message to an MS	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Cleared
Outside Dialout Type	Type of dialout connection to use if a dialout request is received on the dialout listen port or in the case of permanent dialout	<ul style="list-style-type: none"> Outside only Inside Only - All SCs Inside Only - SC list Replicate - All SCs, 	None

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	
Outside Dialout TCP Port	TCP port to use for a dialout connection; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs, • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Outside Dialout Inactivity Time	Maximum number of seconds that an outside dialout link to an application is idle before the RTR disconnects it; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	60
Outside Dialout IP Address	IP address to use for a dialout connection only applies if outside dialout type is IP; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	127.0.0.1
Outside Dialout Max Sessions	Maximum number of dialout sessions between the application and the HUB; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	0

Parameter	Description	Applicable Session Model	Default
Outside Dialout SMPP Window Size	Window size used on links between the application and the HUB; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	1
Outside Dialout SMPP Password	Password of the application used for outside dialout sessions toward the dialout applications; only applies if dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	
SMPP System ID	System ID of the application	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	1
SMPP System Type	System type of the application	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	1
Outside SMPP Originator Addr. Tag	TLV tag value that reflects a short code of the source that is used for billing	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list 	0

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> • Distribute - All SCs • Distribute - SC list • Use service class model 	
Generate GSM Status Report	Controls if the RTR will generate GSM status reports	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Cleared
Outside Life Check Interval	Controls if the HUB will send life check messages to an application to verify connectivity (when SMPP is implemented with the enquire_link PDU); maximum is 3600 seconds ⁹	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	0
SMPP Forward Error Map	Forward error mapping table to use for this application	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Default SMPP forward error map
SMPP Reverse Error Map	Reverse error mapping table to use for this application	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list 	Default SMPP forward error map

⁹ If you set the **Outside Life Check Interval** to a value that is greater than the difference between the application's **Outside Max Inactivity Time** and its **Outside Max Response Time**, the HUB will use that difference as the life check interval. If the difference is zero or a negative value, the HUB will use the outside maximum inactivity time as the life check interval.


Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> Use service class model 	
SMPP Service Type	<p>Service Type of the SMPP application.</p> <p>It is used in outgoing Deliver SM or Data SM towards this application.</p> <p>Also used to validate the service type received in incoming Submit_SM or Data_SM based on semi-static parameter "hubdiscardonsmppservicetypemismatch".</p>	<ul style="list-style-type: none"> Outside only Inside Only - All SCs Inside Only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Empty string
SMPP Bind Response System Id	System ID set in Bind Responses sent towards the Application	<ul style="list-style-type: none"> Outside only Inside Only - All SCs Inside Only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	TextPass

Note: Application passwords are encoded in the MySQL database.


6.3.4 CIMD Applications

The following table details the parameters available for CIMD applications.

Parameter	Description	Applicable Session Model	Default
Service Centres	Service centre(s) to which the application will send messages	<ul style="list-style-type: none"> Inside Only - SC list Replicate - SC list Distribute - SC list 	None
Priority	Priority of each selected service centre	<ul style="list-style-type: none"> Inside Only - SC list Replicate - SC list Distribute - SC list 	50
Weight	Weight of traffic sent to the service centre (for example, a service centre with a weight of 2 will receive twice as many messages as a service centre with a weight of 1)	<ul style="list-style-type: none"> Inside Only - SC list Replicate - SC list Distribute - SC list 	1

Parameter	Description	Applicable Session Model	Default
Outside CIMD Service Description	CIMD service class description, as defined in SMS Applications ► CIMD TC Description	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	1
Outside Authentication Method	<p>Authentication method for the application to use:</p> <ul style="list-style-type: none"> • Password authentication • CLI authentication • One or the other (not both) <p>When password and CLI authentication are both selected, they must both match for the application to be authenticated.</p>	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Outside CIMD Password	<p>Password that the application should use when password authentication has been selected as the outside authentication method; click  to generate a password</p>	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Outside CLI Type	Type of CLI authentication that the application should use when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	IP Address
Outside CLI IP Address	IP address to use for CLI authentication when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	12.0.0.1
Outside CLI IP Mask	IP mask to use for matching the IP when CLI authentication has been	<ul style="list-style-type: none"> • Outside only 	255.255.255.255

Parameter	Description	Applicable Session Model	Default
	selected as the outside authentication method	<ul style="list-style-type: none"> • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	
Outside CLI TCP Port	Port to use for CLI authentication when CLI authentication has been selected as the outside authentication method (0 indicates that any port will be accepted)	<ul style="list-style-type: none"> • Outside only • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	0
Outside CLI Type	Type of CLI source address to use: <ul style="list-style-type: none"> • Address • CLI List 	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Address
CLI List	List of addresses to use for CLI authentication when CLI authentication has been selected as the outside authentication method	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	
Inside Authentication Method	Authentication method for the service centre to use	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Inside CIMD Password	Password for the application to use for sessions toward the service centres; click	<ul style="list-style-type: none"> • Inside Only - All SCs • Inside Only - SC list 	None

Parameter	Description	Applicable Session Model	Default
	 to generate a password	<ul style="list-style-type: none"> Use service class model 	
Inside CIMD Window Size	Window size to use on links between the RTR and the service centre	<ul style="list-style-type: none"> Inside Only - All SCs Inside Only - SC list Use service class model 	255
Number of SMSC Only Sessions	Number of sessions to set up toward each SMSC	<ul style="list-style-type: none"> Inside only - All SCs Inside only - SC list 	1
Allow Notification	Controls whether delivery notifications are allowed for AO-MT messages; if the application requests notification and it is not allowed, the HUB rejects the message	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Selected
Send Short Ack	Controls whether to send acknowledgment to the Application for an outside session request as soon as the HUB receives the first positive acknowledgment from an SMSC(IP) and successfully sets up one inside session. This is applicable only in case of Replicate and Distribute Session Model, or in the case of Use Service Class Model provided the application is associated with a service class configured with either Replicate or Distribute Session Model.	<ul style="list-style-type: none"> Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Not selected
Notification Address Mode	The mode to use for the notification address: <ul style="list-style-type: none"> Transparent—Pass the notification address Clear—Force the address to session-only notification Common IP—Use common IP address of the HUB, including application inside dialout listen port Own IP—Use own IP address of the HUB, including application inside dialout listen port 	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Transparent

Parameter	Description	Applicable Session Model	Default
TCP Keep-Alive	<p>Activates the TCP keep-alive functionality on connections from this application:</p> <ul style="list-style-type: none"> For outside sessions that are successfully authenticated after TCP keep-alive is activated As soon as the connection is started for inside sessions and outside dial-out sessions 	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	False
Outside CIMD Max Sessions	Maximum number of links between the HUB and the application	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	255
Outside CIMD Priority	Priority that the application is allowed to use	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Outside CIMD Tariff Class	Tariff class that the application is allowed to use, as defined in SMS Applications ► CIMD Tariff Class	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None
Outside CIMD Window Size	Window size to use on links between the HUB and the application	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	128
Outside Dialout CIMD Window Size	Window size to use on links between the HUB and the application, when dialout is used	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list 	1

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> Distribute - All SCs Distribute - SC list Use service class model 	
Outside Max Inactivity Time	Maximum number of seconds that a link to an application can be inactive before the HUB disconnects it	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	60
Outside Max Response Time	<p>Maximum number of seconds that the HUB waits for a response from an application before considering it to be timed out.</p> <p>The Outside Max Response Time, should relate to the (RTR's)hubmaxresponsetime attribute (default of 15 seconds) as follows:</p> $T < \text{hubmaxresponsetime} / (1 + (\max(\text{round_down}(W/4), 10) / W))$ <p>Where T is the application's Outside Max Response Time, and W is the application's applicable outside window.</p>	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	5
Respond After Delivery	Controls whether the RTR generates a response after delivery of a message to an MS	<ul style="list-style-type: none"> Outside only Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	Cleared
Outside Dialout Type	Type of dialout connection to use if a dialout request is received on the dialout listen port or in the case of permanent dialout	<ul style="list-style-type: none"> Outside only Inside Only - All SCs Inside Only - SC list Replicate - All SCs Replicate - SC list Distribute - All SCs Distribute - SC list Use service class model 	None

Parameter	Description	Applicable Session Model	Default
Outside Dialout TCP Port	TCP port to use for a dialout connection; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	None
Outside Dialout Inactivity Time	Maximum number of seconds that an outside dialout link to an application is idle before the HUB disconnects it; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	60
Outside Dialout IP Address	IP address to use for a dialout connection only applies if outside dialout type is IP; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	127.0.0.1
Outside Dialout Max Sessions	Maximum number of dialout sessions between the application and the HUB; only applies if outside dialout type is IP	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	0
CIMD User Identity	User identity of the application	<ul style="list-style-type: none"> • Outside only • Inside Only - All SCs • Inside Only - SC list • Replicate - All SCs • Replicate - SC list 	None

Parameter	Description	Applicable Session Model	Default
		<ul style="list-style-type: none"> • Distribute - All SCs • Distribute - SC list • Use service class model 	
CIMD Forward Error Map	Forward error mapping table to use for this application	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Default CIMD forward error map
CIMD Reverse Error Map	Reverse error mapping table to use for this application	<ul style="list-style-type: none"> • Outside only • Inside only - All SCs • Inside only - SC list • Replicate - All SCs • Replicate - SC list • Distribute - All SCs • Distribute - SC list • Use service class model 	Default CIMD forward error map

Note: Application passwords are encoded in the MySQL database.

6.4 Creating SMS Application Categories

Use application categories to organize SMS applications.

To create an SMS application category:

1. In the left navigation bar, select **SMS Applications ► Categories**.
The SMS Application Categories tab appears.
2. Click **Add New**.
A new SMS Application Categories tab appears.
3. Enter a unique name for the category in the **Name** box (up to 31 characters).
4. Optionally enter a description of the category in the **Description** box.
5. Click **Save**.
The MGR creates the application category and closes the tab.
6. Activate the application category.

6.5 Creating Originator Lists

Use originator lists to create whitelists and blacklists of originators. If an AO message matches an entry in the blacklist or does not match an entry in the whitelist, the HUB will send the application a permanent error and block the message.

To create an originator list:

1. In the left navigation bar, select **SMS Applications ► Originator Lists**.

The SMS Application Originator Lists tab appears.

2. Click **Add New**.

A new SMS Application Originator Lists tab appears.

3. Select an SMS application from the **Application** list.
4. Optionally enter a description of the originator list in the **Description** box.
5. From the **List Type** list, select if this will be a whitelist or blacklist.
6. In the **Msisdn Entries** box, enter any MSISDNs that you want to include in the list, each on a separate line.

Note: Ensure that you determine the format in which MSISDNs are sent to the RTR before creating list entries, especially with regard to leading zeros. For example, an MSISDN formatted as 31205557788 will not match list entry 0031205557788.

7. In the **Short Number Entries** box, enter any short numbers that you want to include in the list, each on a separate line.
8. In the **Alphanumeric Entries** box, enter any alphanumeric addresses that you want to including the list, each on a separate line.
9. Click **Save**.

The MGR creates the originator list and closes the tab.

10. Activate the originator list.

6.6 Creating Portable Applications

A portable application is a provisioned SMS application, to which MSISDN aliases can be assigned, so that SMSs addressed to such an alias MSISDN can be routed to that SMS Application (as AT). Multiple MSISDN aliases may be used for the same SMS application. This is for the MO-AT and MT-AT routing paths only.

To create a portable application:

1. In the left navigation bar, select **SMS Applications ► Portable Applications**.

The Portable Application Numbers tab appears.

2. Click **Add New**.

A new Portable Application Numbers tab appears.

3. Select an application from the **Application** list.
4. Optionally enter a description of the portable application in the **Description** box.
5. In the **MSISDN** box, enter an MSISDN alias that shall be mapped to the specified application. The MSISDN must be specified as E.164 number, i.e. an international number.
6. In the **IMSI** box, enter the IMSI that is used in the SRI-SM response, and detected in the subsequent MT-FSM request(s).

For the MSISDNs provisioned as portable application, the RTR handles SRI-SM messages without forwarding the SRI-SM message to a HLR. This means that an IMSI range needs to be allocated for portable application MSISDNs similar to the SMS Firewall and SMS home routing functionality.

7. Click **Save**.

The MGR creates the portable application and closes the tab.

6.7 Creating CIMD Tariff Classes

To create a CIMD tariff class:

1. In the left navigation bar, select **SMS Applications ► CIMD Tariff Class**.

The Tariff Classes tab appears.

2. Click **Add New**.

A new Tariff Classes tab appears.

3. Enter a unique name for the tariff class in the **Name** box (up to 31 characters).
4. Optionally enter a description of the tariff class in the **Description** box.
5. In the **Position** box, enter a value between 0 and 99 that a CIMD application is allowed to specify for the tariff class.
6. Click **Save**.

The MGR creates the tariff class and closes the tab.

6.8 Creating CIMD Tariff Class Descriptions

To create a CIMD tariff class description:

1. In the left navigation bar, select **SMS Applications ► CIMD TC Description**.

The Tariff Class Descriptions tab appears.

2. Click **Add New**.

A new Tariff Class Descriptions tab appears.

3. Enter a unique name for the tariff class description in the **Name** box (up to 31 characters).
4. Optionally enter a description of the tariff class description in the **Description** box.
5. In the **Position** box, enter a value between 0 and 99 that a CIMD application is allowed to specify for the tariff class.

6. Click **Save**.

The MGR creates the tariff class and closes the tab.

6.9 Creating CLI Address Lists

To create a CLI address list:

1. In the left navigation bar, select **SMS Applications ► CLI Addresses**.
The CLI Source Address List tab appears.
2. Click **Add New**.
A new CLI Addresses tab appears.
3. Enter a unique name for the list in the **Name** box (up to 31 characters).
4. Optionally enter a description of the CLI list in the **Description** box.
5. Click **Save**. The MGR creates the CLI source address list and closes the tab.
6. Click the CLI source address list that you just created.
7. Click **Add New**.
A new CLI Addresses tab appears.
8. Select an address type from the **Address Type** list:
 - IP
 - E164
 - X121
9. If you selected IP:
 - a) Enter an IP address in the **IP** box.
 - b) Enter a port number in the **Port** box.
A value of 0 indicates any port will be accepted.
10. If you selected E164, enter an address in the **E164** box.
11. If you selected X121, enter an address in the **X121** box.
12. Click **Save**.
The MGR adds IP address to the list and closes the tab.
13. Add the remaining addresses to the list. A list can contain a mix of address types.
14. Click **Save**.
The MGR saves the CLI address list and closes the tab.
15. Activate the CLI list.



6.10 Configuring Character Set Conversion

The HUB supports configurable character set conversion that converts message data between applications and SMSCs.

For more information about character set conversion, including restrictions, processing flows, and tracing impacts, refer to the HUB Operator Manual.

6.10.1 Modify a Character Conversion Set


To modify a character conversion set:

1. In the left navigation bar, select **SMS Applications ► Character Sets**.
The Character Set Conversions tab appears.
2. Expand a character set by clicking the + to the right of it.
3. To add an input-to-GSM character conversion:
 - a) In the **Input** box under **Input to GSM**, enter the hex code of the character to convert.
 - b) In the **GSM** box, enter the hex code of the replacement character.
 - c) Click **Add**. The MGR adds the characters to the conversion set.
4. To delete an existing input-to-GSM character conversion, click the **Delete** icon  next to the character conversion to delete. The deleted character conversion will be removed from the list.
5. To add a GSM-to-output character conversion:
 - a) In the **GSM** box under **GSM to Output**, enter the hex code of the character to convert.
 - b) In the **Output** box, enter the hex code of the replacement character.
 - c) Click **Add**. The MGR adds the characters to the conversion set.
6. To delete an existing GSM-to-output character conversion, click the **Delete** icon  next to the character conversion to delete. The deleted character conversion will be removed from the list.

Note: You can enter the desired character and the MGR will automatically convert it to its hex code.

6.10.2 Rename a Character Set

To rename a character set:

1. In the left navigation bar, select **SMS Applications ► Character Sets**.
The Character Set Conversions tab appears.
2. Next to the character set that you want to rename, click .
The rename box appears.

3. Type a new name in the **Enter new name** box or click **Cancel** to cancel the renaming operation.
4. Click **Change**.

The MGR renames the character set and closes the rename box.

6.11 Configuring Error Mapping Tables

This section describes the configuration of forward and reverse error mapping tables for the HUB. Forward error mapping tables map the HUB's internal error codes to error responses that are understood by applications and SMSCs. Reverse error mapping tables map error messages that are generated by applications or SMSCs to the HUB's internal error codes.

6.11.1 Modify a Forward Error Mapping Table

To modify a forward error mapping table:

1. In the left navigation bar, select **SMS Applications > Error Mapping > Forward Error Mapping**. The Forward Error Mapping tab appears.

Forward Error Mapping

ID	ST	Name	Last Updated
1	☛	SMPP	2011-03-10 16:35:16
2	☛	UCP	2011-03-10 16:35:16
3	☛	CIMD	2011-03-10 16:35:16
4	↯	Reserved4	2011-03-10 16:35:16
5	↯	Reserved5	2011-03-10 16:35:16
6	↯	Reserved6	2011-03-10 16:35:16
7	↯	Reserved7	2011-03-10 16:35:16
8	↯	Reserved8	2011-03-10 16:35:16
9	↯	Reserved9	2011-03-10 16:35:16

Figure 20: Forward error mapping tables

2. Click the name of the forward error mapping table that you want to modify. The error mapping table's tab appears.

Error Codes

Error Code	New Code	Text
intSystemError	8	Internal system error
intShuttingDown	8	Session shutting down
intMxpFailure	8	Error routing message
intMxpTimeout	69	Error routing message
intTxFailure	69	Error sending message
intTemporaryError	100	Temporary error sending message
intPermanentDestError	101	Permanent error sending message
intPermanentMsgError	102	Permanent error sending message
intDestinationNotAvailable	69	Destination not available
intSourceNotAvailable	69	Source not available
intThroughputExceeded	88	Throughput exceeded
intWindowSizeViolation	255	Window size exceeded

Figure 21: Sample forward error mapping table

Note: The default error mapping tables (those with IDs 1-3) and the reserved error mapping tables (those with IDs 4-9) cannot be deleted. Also, the reserved tables cannot be modified.

3. In the Error Codes section, click the name of the error mapping table entry that you want to modify. The table entry's tab appears.
4. Optionally enter a description of the error mapping table entry in the **Description** box.
5. To modify the error code that should be sent to the application or SMSC, modify the code in the **Replace Error Code** box.
6. To modify the optional error text that should be sent to the application or SMSC, modify the text in the **Replace Error Text** box.
7. Click **Save**.
The MGR saves the entry and closes the tab.
8. On the error mapping table's tab:
 - Click another table entry to modify it, or
 - Click **Save** to save the error mapping table

6.11.2 Add a Forward Error Mapping Table

To add a new forward error mapping table:

1. In the left navigation bar, select **SMS Applications > Error Mapping > Forward Error Mapping**.
The Forward Error Mapping tab appears.
2. Click **Add New**.
A new Forward Error Mapping tab appears.
3. In the **Name** box, enter a name for the table.
4. In the **Description** box, optionally enter a description of the table.
5. From the **Application Protocol** list, select the application protocol for the table:
 - UCP
 - SMPP
 - CIMD
6. Click **Save**.
The MGR saves the table and closes the tab.

The MGR automatically creates the table entries, based on the default error mapping for the application protocol that you selected. Entries cannot be deleted from the table.
7. On the Forward Error Mapping tab, click the name of the table that you just created.
The table opens in a new tab.
8. Modify the table entries as desired.
9. When you are finished, click **Save**.
The MGR saves the table and closes the tab.
10. Activate the table.

6.11.3 Modify a Reverse Error Mapping Table

To modify a reverse error mapping table:

1. In the left navigation bar, select **SMS Applications > Error Mapping > Reverse Error Mapping**.

The Reverse Error Mapping tab appears.

Reverse Error Mapping

ID	ST	Name	Last Updated
1	→	SMPP	2011-03-10 16:35:15
2	→	UCP	2011-03-10 16:35:15
3	→	CIMD	2011-03-10 16:35:15
4	↖	Reserved4	2011-03-10 16:35:15
5	↖	Reserved5	2011-03-10 16:35:15
6	↖	Reserved6	2011-03-10 16:35:15
7	↖	Reserved7	2011-03-10 16:35:15
8	↖	Reserved8	2011-03-10 16:35:15
9	↖	Reserved9	2011-03-10 16:35:15

Figure 22: Reverse error mapping tables

- Click the name of the reverse error mapping table that you want to modify. The error mapping table's tab appears.

Error Codes

Error	Normalised	Class	Action
1	invalidMsgLength	Message Permanent Error	None
2	invalidCommandLength	Message Permanent Error	None
3	invalidCommandId	Message Permanent Error	None
4	invalidBindStatusForCmd	Message Permanent Error	None
5	alreadyLoggedIn	Destination Temporary Error	None
6	invalidPriorityFlag	Message Permanent Error	None
7	invalidRegDeliveryFlag	Message Permanent Error	None

Figure 23: Sample reverse error mapping table

Note: The default error mapping tables (those with IDs 1-3) and the reserved error mapping tables (those with IDs 4-9) cannot be deleted. Also, the reserved tables cannot be modified.

- In the Error Codes section, click the name of the error mapping table entry that you want to modify. The table entry's tab appears.
- Optionally enter a description of the error mapping table entry in the **Description** box.
- To modify the HUB internal error code to use, select a code from the **Normalised Error Code** list.
- To modify the error class, select a type of error from the **Error Class** list:

Option	Description
Source Error	Errors that the HUB detects in the incoming message
Routing Error	Errors that occur while routing the message, such as a timeout on the MXP path or no routing rule for the message
Destination Temporary Error	Errors reported by the destination, for which a fallback path should be attempted (if available)
Destination Permanent Error	Errors reported by the destination for an invalid recipient; no fallback will be attempted
Message Permanent Error	Errors reported by the destination for an invalid message; no fallback will be attempted

- From the Error Action list, select the action to take:

Option	Description
None	Do not take any action
Fallback to another destination	Fallback to another service centre that is assigned to this application's service class (does not have any effect if the application session model is replicate)

8. Click **Save**.
The MGR saves the entry and closes the tab.
9. On the error mapping table's tab:
 - Click another table entry to modify it, or
 - Click **Save** to save the error mapping table

6.11.4 Add a Reverse Error Mapping Table

To add a new reverse error mapping table:

1. In the left navigation bar, select **SMS Applications > Error Mapping > Reverse Error Mapping**.
The Reverse Error Mapping tab appears.
2. Click **Add New**.
A new Reverse Error Mapping tab appears.
3. In the **Name** box, enter a name for the table.
4. In the **Description** box, optionally enter a description of the table.
5. From the **Application Protocol** list, select the application protocol for the table:
 - UCP
 - SMPP
 - CIMD
6. From the **Default Error Code** list, select the internal error code to use if the application or SMSC sends an error that the HUB does not recognize.
7. From the **Default Error Class** list, select the default error class to use if the application or SMSC sends an error that the HUB does not recognize:

Option	Description
Source Error	Errors that the HUB detects in the incoming message
Routing Error	Errors that occur while routing the message, such as timeout on the MXP path, no routing rule for the message, and so on
Destination Temporary Error	Errors reported by the destination, for which a fallback path should be attempted (if available)
Destination Permanent Error	Errors reported by the destination for an invalid recipient; no fallback will be attempted
Message Permanent Error	Errors reported by the destination for an invalid message; no fallback will be attempted

8. From the **Default Error Action** list, select the default to execute if the application or SMSC sends an error that the HUB does not recognize:
 - None
 - Fallback to another destination
9. Click **Save**.
The MGR saves the table and closes the tab.
10. On the Reverse Error Mapping tab, click the name of the table that you just created.
The table opens in a new tab. It contains the default error mapping for the application protocol that you selected.
11. Modify the table entries as desired.
12. When you are finished, click **Save**.
The MGR saves the table and closes the tab.

6.11.5 Add a Reverse Error Text Code

To accommodate applications or SMSCs that send errors containing the same error code but different text, you can add reverse error text codes to the entries of a reverse error mapping table. To add a reverse error text code:

1. In the left navigation bar, select **SMS Applications** ► **Error Mapping** ► **Reverse Error Mapping**.
The Reverse Error Mapping tab appears.
2. Click the name of the reverse error mapping table that you want to modify.
The error mapping table's tab appears.
3. Click the name of the table entry that you want to modify.
The table entry's tab appears.
4. In the Error Text Codes section, click **Add New**.
A new Reverse Error Text table tab appears.
5. From the **Mapping Table** list, select the reverse error mapping table (defaults to the table that you clicked previously).
6. In the **Error** box, enter the error code to map (defaults to the table entry that you clicked previously).
7. In the **Description** box, optionally enter a description of the error text code.
8. From the **Normalised Error Code** list, select the HUB's internal error to which to map the application/SMSC error.
9. From the **Error Class** list, select the type of error:

Option	Description
Source Error	Errors that the HUB detects in the incoming message
Routing Error	Errors that occur while routing the message, such as timeout on the MXP path, no routing rule for the message, and so on
Destination Temporary Error	Errors reported by the destination, for which a fallback path should be attempted (if available)
Destination Permanent Error	Errors reported by the destination for an invalid recipient; no fallback will be attempted

Option	Description
Message Permanent Error	Errors reported by the destination for an invalid message; no fallback will be attempted

10. From the **Error Action** list, select the action:

- None
- Fallback to another destination

11. In the **Message** box, enter the error text that the application or SMSC will return.

12. Click **Save**.

The MGR saves the error text code and closes the tab.

Chapter 7

Environment

Topics:

- *Introduction.....244*
- *Configuring Countries.....244*
- *Adding Networks.....245*
- *Provisioning Own IMSIs.....247*
- *Configuring Outside Listeners.....247*
- *Creating Service Classes.....249*
- *Configuring SMSCs.....250*

7.1 Introduction

To configure the SMS environment, configure:

- Countries
- Networks
- Outside listeners
- Service classes
- SMSC groups
- SS7 SMSCs
- Service centres

7.2 Configuring Countries

Many countries are predefined in the MGR. To add a new country:

1. In the left navigation bar, select **Environment** ► **Countries**.
The Countries tab appears.
2. Click **Add New**.
A new Countries tab appears.
3. Enter the country code in the **Two-letter country code** box.
4. Enter the E164 code for the country in the **Country Code** box.
Note: For example, the country code for the Netherlands is 31.
5. Enter a unique name for the country in the **Name** box.
6. In the **Mobile Country Code** box, enter a comma-delimited list of mobile country codes used for the country.
The list contains at least one mobile country code and at most 16 mobile country codes.
7. Optionally enter E164 area codes for the country in the **Area Codes** box, each on a separate line.
If the country code is used in another country, you must specify area codes.
Note: The length of the country code, concatenated with the area code, must not exceed 6 digits.
8. Click **Save**.
The MGR adds the country and closes the tab.
9. Activate the country, as described in [Activate](#).

Note: To modify a predefined country, first deactivate it (as described in [Deactivate](#)). Then, you can change its properties.

7.3 Adding Networks

Prerequisites:

- Country

To add a network:

1. In the left navigation bar, select **Environment** ► **Networks**.
The Network Table tab appears.
2. Click **Add New**.
A new Network Table tab appears.
3. Enter a unique name for the network in the **Name** box (up to 31 characters).
4. Optionally enter a description of the network in the **Description** box.
5. Optionally enter operator abbreviation of the network in the **Operator Abbreviation** box.
6. Select the network country from the **Country** list.
7. Select the MAP phase to use when communicating with this network from the **Preferred MAP Phase** list.
8. The RTR includes the TCAP user information in the outgoing PDU for the configured network if **Inc. TCAP user info.** is checked. This can be configured only when **Preferred MAP Phase** is "Phase 2" or "Phase 2+".
9. From the **Primary Translation Type** list, select the translation type (TT) value to use in the SCCP called party address of the first SendRoutingInfoForSm (SRI-SM) operation to retrieve the recipient IMSI (defaults to 0).
Note: The default value for ITU-T is 0, while the default for ANSI is 14.
10. Select **Enable Fallback Sri Sm** if a second SRI-SM operation should be issued for the recipient when the HLR that received the first SRI-SM operation indicated that it does not have the subscriber information of the recipient (disabled by default).
11. From the **Fallback Translation Type** list, select the translation type (TT) value to use in the SCCP called party address of the second SRI-SM operation to retrieve the recipient IMSI (defaults to 0).
This setting is only relevant if you select **Enable Fallback Sri Sm**.
Note: The default value for ITU-T is 0, while the default for ANSI is 14.
12. In the **MNP Prefix** box, specify the MNP prefix to use in the SCCP called party address for HLR-terminated operations when the recipient IMSI is known.
When the MNP prefix is applied, the GT is a concatenation of the MNP prefix and the national part of the MSISDN. The NAI in the GT is set to national and the TT is set to 0.
Leaving this field blank disables the MNP prefix, so the HLR is addressed in the normal way.
13. If multiple mobile country codes are specified for the country associated with this network, specify which of the specified mobile country codes applies to this network in the **Mobile Country Code** box.
If only one mobile country code is specified for the country, this parameter is optional.

The MGR adds the network and closes the tab.

25. Activate the network.

7.4 Provisioning Own IMSIs

You can identify IMSIs as belonging to the HPLMN, which enables the RTR to categorize IMSIs in messages as "own" or "foreign". Do so by provisioning IMSI prefixes in the "own IMSIs" table.

To provision IMSIs:

1. In the left navigation bar, select **Environment ► Own IMSIs**.
The Own IMSIs tab appears.
2. Click **Add New**.
A new Own IMSIs tab appears.
3. Enter a unique name for the "own IMSIs" table row in the **Name** box (up to 31 characters).
4. Optionally enter a description of the row in the **Description** box.
5. In the **IMSI Prefix** box, enter the prefix to match against IMSIs that will be categorized as "own" or "foreign".
If this box is empty, all IMSIs will match.
6. Select **Applicable to Suspect MT Traffic** if the IMSI prefix applies when the RTR is identifying the IMSI in an inbound unsolicited MtForwardSm request from an SMSC that is categorized as suspect.
This option is selected by default and is provided for backward compatibility. It should typically be left selected for new rows.
7. Click **Save**.
The MGR saves the own IMSI table row and closes the tab.
8. Activate the row.

7.5 Configuring Outside Listeners

The outside listener is the HUB's TCP listen port for SMS application protocols.

Prerequisites:

- Service class

To configure an outside listener:

1. In the left navigation bar, select **Environment ► Outside Listeners**.
The Outside Listeners tab appears.
2. Click **Add New**.
A new Outside Listeners tab appears.
3. Enter a unique name for the outside listener in the **Name** box (up to 31 characters).

4. Optionally enter a description of the outside listener in the **Description** box.
5. Select the application protocol from the **Protocol** list:
 - SMPP
 - UCP
 - CIMD

6. Select the address type from **Address Type** list:
 - IPv4
 - IPv6

Note: If HUB External IPv6 address is not configured then HUB will not listen for outside session on IPv6.

7. In the **TCP Port** box, enter the TCP/IP port on which to start the outside listener. The TCP Port can be configured with alphanumeric value as well.

Note:

1. If the user needs to define the TCP Port as alphanumeric, then the alphanumeric port name and its corresponding TCP Port should be defined in "/etc/services" file on all the servers where HUB is installed.
 2. The alphanumeric values defined in TCP Port are case sensitive, for example, the port names "port1" and "PORT1" are different entities.
 3. No special characters are supported in TCP Port box.
 4. If the user updates an existing port name present in the file "/etc/services", then to reflect those changes the user has to execute the following command on the servers where HUB is present:
 - a. Switch to `user` root and execute the below command:

```
# service nscd reload
```
 - b. Restart HUB
 5. In case the user provides invalid configuration in the file "/etc/services", for example, if the port name is mapped against an invalid port number, then the HUB cannot behave in a desired manner.
 6. The TCP Port number can be same for two outside listeners as long as the Address Type is different for both, that is, one outside listener listens in IPv4 address and the other listens in IPv6 address.
8. Select a service class (as defined in **Environment ► Service Class**) from the **Service Class** list.
 9. If CLI authentication should be enabled for the outside listener, select **CLI Authentication**.
 10. If the HUB should use the Credential Collector to retrieve caller information, select **CLI Credential Collector**.

Note: The CLI Credential Collector should only be used with the UCP protocol
 11. In the **Max Sessions** box, enter the maximum number of sessions that can be set up with the outside listener.

The listener will be stopped when the maximum is reached and restarted when it can accept new sessions again.
 12. In the **Login Timeout** box, enter the maximum number of seconds that the outside listener will wait for a log-in request when a session for an outside session is established (defaults to 5 seconds).

If no log-in request is received in this time, the connection will be closed. A value of 0 disables log-in time-outs.

Note: The **Login Timeout** only applies to outside sessions for applications with password authentication.

13. Click Save.

The MGR creates the outside listener and closes the tab.

14. Activate the outside listener.

7.6 Creating Service Classes

Service classes:

- Link outside listeners to specific termination points (TCP connect ports)
- Specify the default session model used by applications when connecting to an outside listener
- Introduce an extra level of throughput control across all SMS applications within the service class

To create a service class:

1. In the left navigation bar, select Environment ► Service Class.

The Service Class tab appears.

2. Click Add New.

A new Service Class tab appears.

3. Enter a unique name for the service class in the Name box (up to 31 characters).

4. Optionally enter a description of the service class in the Description box.

5. In the AT Throughput box, enter the maximum number of messages per second to allow from the HUB toward the associated applications (default is 65,535).

6. In the AO Throughput box, enter the maximum number of messages per second to allow from the associated applications toward the HUB (default is 65,535).

Note: Setting the AO throughput to 0 will stop all AO traffic to the SMSC.

7. If dialout should be allowed for the service class, select Dialout Allowed (disabled by default).

8. If modification of messages submitted using the service class should be allowed, select Modification Allowed (selected by default).

9. If the HUB's learning mode applies to the service class, select Learned Enabled (disabled by default).

Refer to the HUB Operator Manual for information about learning mode.

10. If deferred delivery should be allowed for the applications associated with the service class, select Deferred Delivery Allowed (disabled by default).

11. Select the type of traffic that is allowed for the service class from the Allowed Traffic list:

- AO and AT (default)
- AO only
- AT only

12. From the Notification Allowed list, select the type(s) of notification(s) allowed for the service class:

- Buffered
- Not delivered
- Delivered

By default, all types are enabled.

13. From the **Service Model** list, select the session model for the service class:

- Inside only - All SCs
- Outside only
- Replicate - All SCs
- Distribute - All SCs

If the session model for an SMS application is set to something other than "use service class model", it overrides this setting.

14. From the **Charged Party** list, select the party to charge for the service class:

- Originator
- Recipient
- Billing on behalf of (allows an AO message to be charged as if it was submitted by a mobile)

Note: The charged party setting modifies the PBC's Subscription-Id AVP.

15. Click **Save**.

The MGR creates the service class and closes the tab.

16. Activate the service class.

7.7 Configuring SMSCs

You can configure SS7 SMSCs and IP service centres in the MGR. The SMSC group functionality provides greater load balancing control over traffic to SMSCs.

7.7.1 Create SMSC Groups

Prerequisites:

- Service centre

To create an SMSC group:

1. In the left navigation bar, select **Environment ► SMSC ► SMSC Group**.

The Smsc Group tab appears.

2. Click **Add New**.

A new Smsc Group tab appears.

3. Enter a unique name for the SMSC group in the **Name** box (up to 31 characters).

4. Optionally enter a description of the SMSC group in the **Description** box.

5. In the **Service Centres** section, select the SMSC(s) to include in the group.

6. For each SMSC that you select, set a priority between 0 and 99 (defaults to 50).

7. Click **Save**.
The MGR creates the SMSC group and closes the tab.
8. Activate the SMSC group, as described in [Activate](#).

7.7.2 Configure SS7 SMSCs

To configure an SS7 SMSC:

1. In the left navigation bar, select **Environment** ► **SMSC** ► **SMSC (ss7)**.
The SMSCs (SS7) tab appears.
2. Click **Add New**.
A new SMSC (SS7) tab appears.
3. Enter a unique name for the SMSC in the **Name** box (up to 31 characters).
4. Optionally enter a description of the SMSC in the **Description** box.
5. Enter the E164 address of the SMSC (excluding the international prefix) in the **Address** box.
6. In the **Throughput** box, enter the maximum number of messages per second to allow to the SMSC (defaults to 65,535).
If set to 0, throughput will be unlimited.
7. If you want the RTR to periodically send test messages to the SMSC to verify its accessibility, enter the number of seconds between test messages in the **Test-Message Interval** box (defaults to 0).
Setting the test message interval to 0 disables the functionality.
8. In the **MAP address** box, optionally enter the internationally encoded E164 address (excluding the international prefix) to use as the MAP address of the SMSC.
If you do not provide a MAP address, the RTR uses the MAP address in the incoming `MO-ForwardSM`.
9. Click **Save**.
The MGR adds the SMSC and closes the tab.
10. Activate the SMSC.

7.7.3 Configure Service Centres

When your system includes a HUB, you can communicate with service centres over IP

Prerequisites:

- Character conversion set

To configure a service centre:

1. In the left navigation bar, select **Environment** ► **SMSC** ► **Service Centre**.
The Service Centres tab appears.
2. Click **Add New**.
A new Service Centres tab appears.

3. Enter a unique name for the service centre in the **Name** box (up to 31 characters).
4. Optionally enter a description of the service centre in the **Description** box.
5. In the **AO Throughput** box, enter the maximum number of messages per second to allow to the service centre (defaults to 65,535).

Note: Setting the AO throughput to 0 will stop all AO traffic to the SMSC.

6. If you will use this service centre and the replicate session model (see [Session Models](#)), you can optionally enter a weight for load balancing in the **Weight** box.

For example, the HUB will send twice as many messages to a service centre with a weight of 2 than it will to a service centre with a weight of 1.

7. To use character conversion with the service centre (see [Configuring Character Set Conversion](#)), select a character conversion set from the **Character Conversion Set** list.
8. Optionally select a custom error mapping table from the following lists (see [Configuring Error Mapping Tables](#)):

- **SMPP Forward Error Map**
- **SMPP Reverse Error Map**
- **UCP Forward Error Map**
- **UCP Reverse Error Map**
- **CIMD Forward Error Map**
- **CIMD Reverse Error Map**

Each list defaults to the default error mapping table for the application protocol.

9. Click **Save**.

The MGR adds the service centre and closes the tab.

10. Activate the service centre.

7.7.3.1 Configure Service Centre Nodes

When your system includes a HUB, you can communicate with service centres over IP

Prerequisites:

- Service centre

To configure a service centre node:

1. In the left navigation bar, select **Environment** ► **SMSC** ► **Service Centre**.

The Service Centres tab appears.

2. Select a service centre.

Its tab appears.

3. Under Nodes, click **Add New**.

A Service Centre Nodes tab appears.

4. Enter a unique name for the node in the **Name** box (up to 31 characters).
5. Optionally enter a description of the node in the **Description** box.
6. Select a service centre from the **Service Centre** list.

By default, the service centre that you selected in step 2 is selected.

7. In the **IP Address** box, enter the IP address of the node. This can be IPv4, IPv6 or Hostname.

Following are the rules to validate the IP address:

1. If the provided input contains three dots and consecutive numeric values, then it will be treated as IPv4 address.
2. If the provided input contains colon (:), then it will be treated as IPv6 address.
3. For any other input, it will be treated as Hostname

For example:

“255.256.255.245” will be validated as IPv4 address,

“2001:3001” will be validated as IPv6 address.

“1.2.3.4.5” will be validated as hostname.

If IPv6 address is configured, then HUB Internal IPv6 Address must be provisioned.

If the hostname is configured, refer to section [DNS Query Mechanism](#) for more details

8. In the **AO Throughput** box, enter the maximum number of messages per second to allow to the node (defaults to 65,535).

Note: Setting the AO throughput to 0 will stop all AO traffic to the SMSC.

9. Click **Save**.

The MGR adds the node and closes the tab.

10. Activate the node.

7.7.3.2 Configure Service Centre Node Termination Points

When your system includes a HUB, you can communicate with service centres over IP.

- Service centre
- Service centre node

To configure a service centre node termination point:

1. In the left navigation bar, select **Environment** ► **SMSC** ► **Service Centre**.
The Service Centres tab appears.
2. Select a service centre.
Its tab appears.
3. Expand a node.
4. Under **Termination Points**, click **Add New**.
A Service Centre Termination Points tab appears.
5. Enter a unique name for the termination point in the **Name** box (up to 31 characters).
6. Optionally enter a description of the termination point in the **Description** box.
7. Select a node from the **Service Centre Node** list.
By default, the service centre node that you selected in step 3 is selected.
8. Select an application protocol from the **Protocol** list.

9. In the **Remote TCP Port** box, enter the port for this termination point. The port can be configured with alphanumeric value as well.
Note: No special characters are supported in TCP Port box. For configuration of alphanumeric port, refer to point 7 of section [Configuring Outside Listeners](#).
10. Select the service class from the **Service Class** list.
11. In the **AO Throughput** box, enter the maximum number of messages per second to allow to the termination point (defaults to 65,535).
Note: Setting the AO throughput to 0 will stop all AO traffic to the SMSC.
12. In the **Max Sessions** box, enter the maximum number of sessions to allow for the termination point (defaults to 2000).
13. In the **Max Inactivity Time** box, enter the maximum number of seconds that the connection to the termination point can be inactive (defaults to 60).
14. In the **Max Response Time** box, enter the maximum number of seconds that the termination point has to respond before the request is considered to be timed out (defaults to 5).
15. To enable TCP keep-alive functionality on connections toward this termination point, select **TCP Keep-Alive**.
When enabled, TCP keep-alive will be activated on all connections started thereafter. For inside sessions and outside dial-out sessions, TCP keep-alive will be activated immediately upon session start.
16. Click **Save**.
The MGR adds the termination point and closes the tab.
17. Activate the termination point.

Note: If your system is handling AO-AO traffic and you intend to deactivate a termination point for a service class, first deactivate all outside listeners for that service class. This prevents errors from occurring when connection applications continue to send AO-AO traffic after the termination point was deactivated.

Chapter 8

Storage

Topics:

- *Introduction.....256*
- *Creating Delivery Schemes.....256*
- *Configuring Message Queues.....258*
- *Configure Error-Dependent Schemes.....259*
- *Configuring the Icache.....262*

8.1 Introduction

When your system includes an Active Message Store (AMS), you can intelligently store and forward SMS messages according to highly configurable delivery schemes.

The AMS also provides the Mobile Messaging Intermediate Cache (Icache) functionality. When a message passes through the Mobile Messaging system and is then forwarded to an external SMSC, the system can store the message's state and certain parameters in a record in the Icache. The Icache's contents represent the set of messages that are handled and/or stored on an external SMSC.

The combination of AMSs, HUBs, and RTRs can replace the functionality of a traditional SMSC.

8.2 Creating Delivery Schemes

To create a delivery scheme:

1. In the left navigation bar, select **Storage ► Schemes**.

The Delivery Scheme Table tab appears.

2. Click **Add New**.

A new Delivery Scheme Table tab appears.

3. Enter a unique name for the delivery scheme in the **Name** box (up to 31 characters).
4. Optionally enter a description of the delivery scheme in the **Description** box.
5. In the **Maximum Attempts** box, enter the maximum number of times the AMS should attempt to deliver the message before it expires (defaults to 50).

Note: If the configured maximum number of intervals is less than the configured maximum attempts AND the **Retain up to Validity** option is not selected, then the AMS will use the maximum number of intervals for expiring stored messages.

6. In the **Maximum Validity** box, enter the maximum number of hours that the AMS stores a message before it expires (defaults to 168).

Note: The actual validity period will be shorter if a shorter period is specified in the message itself.

7. If the AMS should perform a final delivery attempt before deleting the message when the maximum validity period has expired or when the last scheduled delivery interval has passed, select **Last Attempt** (selected by default).
8. When a new message is stored in a delivery queue, if the delivery scheme should restart for that queue, select **Restart on New Message** (selected by default).

Note: **Restart on New Message** does not apply to messages with an application as the destination and to messages for which the First Delivery Attempt (FDA) by the RTR had resulted in a temporary failure before they were forwarded to the AMS for storing.

9. If this delivery scheme should be allowed to switch to an error-dependent delivery scheme (based on network errors), select **Error Dependent** (selected by default).

- If messages following this delivery scheme need to be retained in their respective queues even after all the delivery intervals have been used up as per this Delivery Scheme, until the validity period of such a message expires, or such a message gets manually deleted or replaced, or an unscheduled delivery attempt triggered by an alert (from network or manual), arrival of a new message, etc, results in either a successful delivery or a permanent error, select **Retain up to Validity** (not selected by default).

Note: Even if no valid delivery intervals are configured for a particular delivery scheme (i.e. the very first interval is set to 0), still the messages following that delivery scheme will be retained if **Retain up to Validity** is selected for the scheme

- Enter the duration of the first interval (in seconds) in the **Interval in Seconds** box.
Each time you add an interval, the interval number appears to the right of the interval.

- To add more intervals, click



to the right of the **Interval in Seconds** box.

The maximum value for each interval is 2592000 (30 days).

The running total of the intervals appears to the right of each interval.

Index:	Auto Generated																															
Name: ✓	Preferred Delivery Scheme																															
Description:	Delivery scheme for preferred messages																															
Maximum Attempts:	50	[num]																														
Maximum Validity: ✓	200	[hrs]																														
Last Attempt:	<input checked="" type="checkbox"/>																															
Restart On New Message:	<input checked="" type="checkbox"/>																															
Error Dependent:	<input type="checkbox"/>																															
Retain up to Validity:	<input checked="" type="checkbox"/>																															
Interval in Seconds:	<table border="1"> <tr> <td>001</td> <td>300</td> <td>00d 00:05:00</td> </tr> <tr> <td>002</td> <td>300</td> <td>00d 00:10:00</td> </tr> <tr> <td>003</td> <td>300</td> <td>00d 00:15:00</td> </tr> <tr> <td>004</td> <td>300</td> <td>00d 00:20:00</td> </tr> <tr> <td>005</td> <td>600</td> <td>00d 00:30:00</td> </tr> <tr> <td>006</td> <td>600</td> <td>00d 00:40:00</td> </tr> <tr> <td>007</td> <td>600</td> <td>00d 00:50:00</td> </tr> <tr> <td>008</td> <td>600</td> <td>00d 01:00:00</td> </tr> <tr> <td>009</td> <td>600</td> <td>00d 01:10:00</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>		001	300	00d 00:05:00	002	300	00d 00:10:00	003	300	00d 00:15:00	004	300	00d 00:20:00	005	600	00d 00:30:00	006	600	00d 00:40:00	007	600	00d 00:50:00	008	600	00d 01:00:00	009	600	00d 01:10:00			
001	300	00d 00:05:00																														
002	300	00d 00:10:00																														
003	300	00d 00:15:00																														
004	300	00d 00:20:00																														
005	600	00d 00:30:00																														
006	600	00d 00:40:00																														
007	600	00d 00:50:00																														
008	600	00d 01:00:00																														
009	600	00d 01:10:00																														
Last Updated:	Auto Generated																															

Figure 24: Sample delivery intervals

Note: Setting an interval to 0 will make it the final retry attempt; the AMS will ignore any intervals added after it.

13. Click **Save**.
The MGR creates the delivery scheme and closes the tab.
14. Activate the delivery scheme.

8.3 Configuring Message Queues

Prerequisites:

- Delivery scheme

To create a message queue:

1. In the left navigation bar, select **Storage ► Queues**.
The Queue Table tab appears.
2. Click **Add New**.
A new Queue Table tab appears.
3. Enter a unique name for the message queue in the **Name** box (up to 31 characters).
4. Optionally enter a description of the message queue in the **Description** box.
5. Enter a message queue priority between 0 and 99 in the **Priority** box (defaults to 50).
Message queues with a higher priority take precedence when scheduling deliveries.
6. In the **Maximum Size** box, enter the maximum number of messages that the message queue can hold.
The maximum size can be between 0 and 500,000,000 (defaults to 1,000,000). When the maximum size is reached, new messages will be rejected.
7. Enter the maximum number of messages allowed in the queue for each recipient in the **Maximum Size / Recipient** box.
The maximum size can be between 0 and 500,000,000 (defaults to 0, which means that this setting will be ignored).
8. Select a delivery scheme for the message queue from the **Delivery Scheme** list.
9. Select Sri-SM Priority for the message queue from the **Sri-SM Priority** list.
10. Select Conversion Table for the message queue from the **Conversion Table List**. Default selection is "None".
11. Enter a timeout value in seconds between 0 and 3600 in the **Concatenated Segment Timeout**.
If a Conversion table is selected in the previous step, the minimum value of **Concatenated Segment Timeout** is 1. If it is set to 0, the timeout value is automatically saved as 15.
12. If all the segments of a concatenated message are not received in set time, it should be handled as incomplete and the AMS should delete them from the system, select **Delete Incomplete Concatenated** (by default, this option is not selected).
Note: If the user configures 0 for **Concatenated Segment Timeout**, then the in sequence functionality will be disabled, the system will not delete the incomplete segments and the message will be processed normally.

13. If surrogate pairs should be unsplit and remain in one segment select **Unsplit Surrogate Pairs** (by default, this option is not selected).
14. Click **Save**.
The MGR creates the message queue and closes the tab.
15. Activate the message queue.

8.4 Configure Error-Dependent Schemes

Use error-dependent delivery schemes to change the delivery scheme in use when network errors occur.

Note: All error-dependent schemes default to the default error scheme that is included with the AMS.

8.4.1 AT Error Dependent Schemes

Prerequisites:

- Delivery scheme

To configure error-dependent delivery schemes for application-terminating (AT) traffic:

1. In the left navigation bar, select **Storage** ► **Error Schemes** ► **AT**.
The Error Dep Scheme - AT tab appears.
2. Select a delivery scheme to use when a "destination not available" error occurs from the **Destination Not Available Error** list.
3. Select a delivery scheme to use when a "response time-out" error occurs from the **Response Timeout Error** list.
4. Select a delivery scheme to use when a "throughput exceeded" error occurs from the **Throughput Exceeded Error** list.
5. Click **Save**.
The MGR saves the changes and closes the tab.

8.4.2 SRI-SM Error-Dependent Schemes

- Delivery scheme

To configure error-dependent delivery schemes for SRI-SM traffic:

1. In the left navigation bar, select **Storage** ► **Error Schemes** ► **SRI-SM**.
The Error Dep Scheme - SriSm tab appears.
2. Select a delivery scheme to use when an "absent subscriber" error occurs from the **Absent Subscriber Error** list.
3. Select a delivery scheme to use when a "call barred" error occurs from the **Call Barred Error** list.
4. Select a delivery scheme to use when a "data missing" error occurs from the **Data Missing Error** list.

5. Select a delivery scheme to use when a "facility not supported" error occurs from the **Facility Not Supported Error** list.
6. Select a delivery scheme to use when an "SCCP aborted" error occurs from the **Sccp Aborted Error** list.
7. Select a delivery scheme to use when a "system failure" error occurs from the **System Failure Error** list.
8. Select a delivery scheme to use when a "TCAP aborted" error occurs from the **Tcap Aborted Error** list.
9. Select a delivery scheme to use when a "time-out" error occurs from the **Timeout Error** list.
10. Select a delivery scheme to use when an "unexpected data value" error occurs from the **Unexpected Data Value Error** list.
11. Select a delivery scheme to use when an "MS Deregistered" error occurs from the **MS Deregistered Error** list.
12. Select a delivery scheme to use when an "MS Purged" error occurs from the **MS Purged Error** list.
13. Click **Save**.

The MGR saves the changes and closes the tab.

14. Activate the scheme.

Note: The 'Absent Subscriber' error has been deprecated for both MT and SRI-SM. Any MT error-dependent scheme configured in the 'Absent Subscriber Error' list should be added to the 'No Paging Error' list, 'Imsi Detached Error' list and 'Roaming Restrictions Error' list; similarly, any SRI-SM error-dependent scheme configured in the 'Absent Subscriber Error' list should be added to the 'MS Deregistered Error' list and 'MS Purged Error' list.

8.4.3 MT Error-Dependent Schemes

Prerequisites:

- Delivery scheme

To configure error-dependent delivery schemes for outgoing mobile-terminating (MT) traffic:

1. In the left navigation bar, select **Storage ► Error Schemes ► MT**.

The Error Dep Scheme - MT tab appears.

2. Select a delivery scheme to use when an "absent subscriber" error occurs from the **Absent Subscriber Error** list.
3. Select a delivery scheme to use when a "data missing" error occurs from the **Data Missing Error** list.
4. Select a delivery scheme to use when an "equipment not SM-equipped" error occurs from the **Equipment Not SM Equipped Error** list.
5. Select a delivery scheme to use when an "equipment protocol" error occurs from the **Equipment Protocol Error** list.
6. Select a delivery scheme to use when a "facility not supported" error occurs from the **Facility Not Supported Error** list.
7. Select a delivery scheme to use when an "invalid SME address" error occurs from the **Invalid SME Address Error** list.

8. Select a delivery scheme to use when a "memory capacity exceeded" error occurs from the **Memory Capacity Exceeded Error** list.
9. Select a delivery scheme to use when an "SCCP aborted" error occurs from the **Sccp Aborted Error** list.
10. Select a delivery scheme to use when a "subscriber busy for MTSM" error occurs from the **Subscriber Busy For MTSM Error** list.
11. Select a delivery scheme to use when a "system failure" error occurs from the **System Failure Error** list.
12. Select a delivery scheme to use when a "TCAP aborted" error occurs from the **Tcap Aborted Error** list.
13. Select a delivery scheme to use when a "time-out" error occurs from the **Timeout Error** list.
14. Select a delivery scheme to use when an "unexpected data value" error occurs from the **Unexpected Data Value Error** list.
15. Select a delivery scheme to use when an "unidentified subscriber" error occurs from the **Unidentified Subscriber** list.
16. Select a delivery scheme to use when a "no paging" error occurs from the **No Paging Response** list.
17. Select a delivery scheme to use when an "imsi detached" error occurs from the **Imsi Detached Error** list.
18. Select a delivery scheme to use when a "roaming restriction" error occurs from the **Roaming Restrictions Error** list.
19. Select a delivery scheme to use when a "Short message type 0 not supported" error occurs from the **Short message Type 0 not supported Error** list.
20. Select a delivery scheme to use when a "Cannot replace short message" error occurs from the **Cannot replace short message Error** list.
21. Select a delivery scheme to use when an "Unspecified TP-PID error" error occurs from the **Unspecified TP-PID Error** list.
22. Select a delivery scheme to use when a "Message class not supported" error occurs from the **Message class not supported Error** list.
23. Select a delivery scheme to use when an "Unspecified TP-DCS" error occurs from the **Unspecified TP-DCS Error** list.
24. Select a delivery scheme to use when a "TPDU not supported" error occurs from the **TPDU not supported Error** list.
25. Select a delivery scheme to use when a "(U) SIM SMS storage full " error occurs from the **SIM SMS storage full Error** list.
26. Select a delivery scheme to use when a "No SMS storage capability in SIM " error occurs from the **No SMS storage capability in SIM** list.
27. Select a delivery scheme to use when an "Error in MS" error occurs from the **Error in MS** list.
28. Select a delivery scheme to use when a "(U)SIM Application Toolkit Busy " error occurs from the **SIM Application Toolkit Busy Error** list.
29. Select a delivery scheme to use when a "(U) SIM data download" error occurs from the **SIM Data Download Error** list.
30. Select a delivery scheme to use when a "Values specific to an application" error occurs from the **Values specific to an application Error** list.

31. Select a delivery scheme to use when an "Unspecified error cause" error occurs from the **Unspecified error cause** list.
32. Select a delivery scheme to use when an "UE Deregistered" error occurs from the **UE Deregistered Error** list.
33. Select a delivery scheme to use when a "No Response Via IPSM-GW" error occurs from the **No Response from IPSM-GW** list.
34. Click **Save**.
The MGR saves the changes and closes the tab.
35. Activate the scheme.

8.5 Configuring the Icache

Prerequisites:

- The installed AMS license must allow Icache functionality
- AMS queue

To configure the Icache:

1. In the left navigation bar, select **Storage ► Intermediate Cache**.
The Intermediate Cache tab appears.
2. To enable the Icache for AO messages, select an option from the **AO Intermediate Cache Support** list:
 - **No Support** (No support of storing of billing data in an Icache store)
 - **Store and Lookup** (Select an AMS queue from **AO AMS Queue**)
 - **Lookup Only**
3. From the **AO AMS Queue** list, select the AMS queue in which to store AO message information (only applicable when **AO Intermediate Cache Support** is set to **Store and Lookup**).
4. To enable the Icache for MO messages, select an option from the **MO Intermediate Cache Support** list:
 - **No Support** (No support of storing of billing data in an Icache store)
 - **Store and Lookup** (Select an AMS queue from **AO AMS Queue**)
 - **Lookup Only**
5. From the **MO AMS Queue** list, select the AMS queue in which to store the MO message information (only applicable when **MO Intermediate Cache Support** is set to **Store and Lookup**).
6. To enable the Icache for IGM messages, select an option from the **IGM Intermediate Cache Support** list:
 - **No Support** (No support of storing of billing data in an Icache store)
 - **Store and Lookup** (Select an AMS queue from **AO AMS Queue**)
 - **Lookup Only**

7. From the **IGM AMS Queue** list, select the AMS queue in which to store the IGM message information (only applicable when **IGM Intermediate Cache Support** is set to `Store` and `Lookup`).
8. Click **Save**.
The MGR saves the configuration and closes the tab.

Chapter 9

IPSMGW

Topics:

- *Introduction.....266*
- *Creating SIP Application.....266*
- *Creating SIP End Point.....266*
- *Creating SIP End Point Group.....267*
- *Creating SIP Headers.....268*

9.1 Introduction

When your system includes an IIW, you can route SMS traffic from IMS network to RTRs, SMS gateways, or SMSCs.

9.2 Creating SIP Application

Prerequisite:

- SIP End Point Group must be active.

To create a SIP Application:

1. In the left navigation bar, select **IPSMGW ► SIP Application**. The SIP Application Table tab appears.
2. Click **Add New**. A new SIP Application tab appears.
3. Enter a unique name for the sip application in the **Name** box (up to 31 characters).
4. Optionally enter a description of the application group in the **Description** box.
5. Select if the content type will be textPlain or applicationVnd3gpp from the **Content Type** dropdown.
6. Specify FROM URI that must be received in SIP INFO request in the **From URI** textbox.
7. Specify TO URI that must be received in SIP INFO request in the **To URI** textbox.
8. Provide the duration to perform health check from SIP INFO to 4G network in seconds in **Healthcheck Interval** textbox.
Note: If the Healthcheck interval is 0, then Health Check will not be performed.
9. Select a SIP End Point Group where SIP outgoing messages should be sent from the **SIP End Point Group** dropdown.
10. Click **Save**. The MGR creates the sip application and closes the tab.
11. Activate the sip application.

9.3 Creating SIP End Point

Prerequisite:

- IIW device must be added

To create a SIP End Point:

1. In the left navigation bar, select **IPSMGW ► SIP End Point**. The SIP End Point Table tab appears.
2. Click **Add New**. A new SIP End Point tab appears.
3. Enter a unique name for the SIP End Point in the **Name** box (up to 31 characters).
4. Optionally enter a description of the SIP End Point in the **Description** box.
5. Enter an address for the SIP End Point in the **Primary Address** box. The address can be a valid IPv4, IPv6 or a hostname.

6. Enter the port number of the SIP End Point in the **Port** box. Port range should be in the range of 0-65535 .
7. Provide the maximum duration in seconds within which the SIP response should be received by IIW in the **Response Timer** textbox.
8. Provide the duration to perform health check in seconds in **HealthCheck Timer** textbox.
9. Select a transport type from the **Transport** list:
 - UDP (by default)
 - SCTP
10. If you select SCTP, then you need to enter the following values:
 - a. An address of type IPv4, IPv6 or hostname in the **Secondary Address** box.
 - b. Local port in the **SCTP Local Port** box. The default value "zero" denotes ephemeral port.
 - c. Duration to perform SCTP health check between IIW and remote SIP End Point in milliseconds in **SCTP HeartBeat Timer** textbox. This parameter is applicable when IIW is configured on RHEL OS.
 - d. Maximum retransmission timeout value in **SCTP Max Retransmit Timeout** box. This parameter is applicable only if the IIW is configured on RHEL OS.
 - e. Maximum number of path retries in **SCTP Max Path Retransmit** box. This parameter is applicable when IIW is configured on RHEL OS.
 - f. Maximum number of association retries in **SCTP Max Association Retransmit** box. This parameter is applicable when IIW is configured on RHEL OS.
 - g. Time in milliseconds to wait before acknowledging SCTP data chunks in **SCTP SACK Delay** box. This parameter is applicable when IIW is configured on RHEL OS.
 - h. Value of **SCTP NoDelay** to "false" if you want to delay the message until the acknowledgement of previous packet is received. This parameter is applicable when IIW is configured on RHEL OS.
11. In the **Device Assignments** section, select the **IIW** device(s) to which this SIP End Point will be associated.
12. Click **Save** . The MGR creates the SIP End Point and closes the tab.

9.4 Creating SIP End Point Group

Prerequisite:

- SIP End Point(s) must be activated

To create a SIP End Point Group:

1. In the left navigation bar, select **IPSMGW**►**SIP End Point Group**. The SIP End Point Group Table tab appears.
2. Click **Add New**. A new SIP End Point Group tab appears.
3. Enter a unique name for the SIP End Point Group in the **Name** box (up to 31 characters).
4. Optionally enter a description of the SIP End Point Group in the **Description** box.
5. In the **SIP End Points** section, select the SIP End Point(s) to include in the group.

6. For each SIP End Point that you select, set a **Priority** and a **Weight**.
7. Click **Save**. The MGR creates the SIP End Point Group and closes the tab.

9.5 Creating SIP Headers

To create a SIP headers:

1. In the left navigation bar, select **IPSMGW** ► **SIP Headers**. The SIP Headers Table tab appears.
2. Click **Add New**. A new SIP Headers tab appears.
3. Enter a unique name for the SIP Header in the **Name** box (up to 64 characters). This field is case-insensitive, i.e. the values 'abcde' and 'ABcde' will be treated as the same name.
4. Click **Save**. The MGR creates the SIP Header and closes the tab. Maximum 10 SIP Header can be configured.

Note: The SIP Header cannot be deleted if they are referred in MO (MOR/MOC/MOX) rules.

Chapter 10

Advanced Filters

Topics:

- [Introduction.....270](#)
- [Create an Advanced Filter.....270](#)
- [Add Conditions to an Advanced Filter.....271](#)
- [Create an Advanced Filter List.....286](#)

10.1 Introduction

When your system includes a RTR/FWL and the Firewall Advanced Filter (FAF), you can:

- Enhance spam message detection and blocking
- Modify the content of offensive messages
- Configure alerts based on unexpected increases in SMS traffic

10.2 Create an Advanced Filter

To create an advanced filter:

1. In the left navigation bar, select **Advanced Filters** ► **Filters**.
The Advanced Filters tab appears.
2. Click **Add New**.
A new Advanced Filters tab appears.
3. Enter a unique name for the filter in the **Name** box (up to 31 characters).
4. Optionally enter a description of the filter in the **Description** box.
5. Enter a filter priority between -100 and 100 in the **Priority** box (defaults to 50).
Filters with a higher priority are evaluated first.
6. From the **Action** list, select the action that the RTR should take if a message meets all conditions when the FAF processes the filter:
 - Return True: The FAF returns true for the message fields.
 - Return False: The FAF returns false for the message fields.
 - Continue: The FAF should continue to process the next filter.

When first creating the filter, select "Return True". Then, after you create and activate the desired conditions for the filter, change the filter action to "Return False". If you create a filter with no conditions and a "Return False" action, the FAF will immediately return "false" to the RTR and will therefore block messages.

7. In **Blacklist Party** field, select which subscriber party should be blacklisted.
 - None: Indicate that no ABL is configured for this filter.
 - Originator: Originator party will be blacklisted.
 - Recipient: Recipient party will be blacklisted.

If the "Auto GT Network Blacklist" license is enabled, there will be two more options to be blacklisted as follows:

- Originating GT: The SMSC GT of message originator to be added to selected ABL list.
- Originating Network: The SMSC Network Number Ranges of message originator to be added to selected ABL List.

The default value is None.

If **Blacklist Party** is None, then continue at step 13.

8. Select the Auto Blacklist service which will be assigned to blacklist subscriber in **Blacklist Servicefield**. This field is visible when the **Filter Blacklist Party** is selected as "Originator" or "Recipient".

Originator Blacklist Service: If **Blacklist Party** is Originator, then only Originator Auto Blacklist service will be listed in **Originator Blacklist Servicefield**.

Recipient Blacklist Service: if **Blacklist Party** is Recipient, then only Recipient Auto Blacklist service will be listed in **Recipient Blacklist Servicefield**.

9. Select the ABL List which the SMSC GT or Network Number Range to be added to. This field is visible when the Filter Blacklist Party is selected as "Originator GT" or "Originating Network".

10. Select the blacklist blocking action in **Blacklist Duration** field.

- Permanent Blocking: Subscriber will be blocked permanently.
- Time-based Blocking: Subscriber will be blocked for the duration specified in **Blacklist Duration** field.
- Absolute Blocking: SMSC GT or Network is to be blacklisted until a specific date time. This option is available only when the Filter Blacklist Party is selected as "Originating GT" or "Originating Network".

If **Blacklist Action** is Absolute Blocking, then continue at step 12.

If **Blacklist Action** is Permanent Blocking, then continue at step 13.

11. In Blacklist Duration field, Indicates time for which subscriber will be blacklisted

Blacklist Duration should be less than 99 days (Maximum allowed duration is 98 Days 23 Hours 59 Minutes). Minimum **Blacklist Duration** is 1 Minute.

Continue at step 13.

12. In the **End Time** field, specify the last date time for which subscriber or network should be blacklisted.

13. In the **Append** box, optionally enter any text that the FAF should append to the message. The FAF will append this text if the message meets all conditions of the filter and if the Data message field was provided to the FAF.

CAUTION: Do not use text replacement/append functions that may make the user data longer than the original user data. When applied to a "full segment" this will lead to an undeliverable message.

14. Click **Save**.

The MGR saves the filter and closes the tab.

15. Activate the filter.

10.3 Add Conditions to an Advanced Filter

Prerequisites:

- Filter

- Filter list (if adding a content condition)

Combine advanced filters and conditions of different types to create filter conditions.

To add a filter condition to a filter:

1. In the left navigation bar, select **Advanced Filters** ► **Filters**.
The Advanced Filters tab appears.
2. Click the name of an existing filter.
3. In the Filter Conditions section, click **Add New**. A Filter Conditions tab appears.
4. If the filter condition should be inverted if the condition is true, select **Invert**.
5. From the **Filter Name** list, select the filter to use (defaults to the filter that you clicked in the Advanced Filters tab).
6. In the **Name** box, enter the name of the filter condition.
7. From the **Type** list, select the condition type.
8. Click **Save**.

The MGR creates the filter condition and closes the tab.

9. Activate the filter condition.

Advanced Filters

Index: 3

Name: ✓ Sample FAF filter

Description: ✓ Sample FAF filter

Priority: ✓ 20

Action: Return True

Append: ✓ filtered

Last Updated: 2009-10-06 11:37:23

Save

Filter Conditions

ID	ST	Inv.	Name	Type	Last Updated	Action
1		=	Content ...	Content	2009-10-06 11:37:51	
Content Condition						
Field:		data				
List:		list-1				
Accuracy:		Case Insensitive				
Modify:		Mask String				
Replacement Text:		XXXX				
2		=	Flood co...	Flooding	2009-10-06 11:38:21	

Add New

Figure 25: Sample filter with conditions

10.3.1 Add an Expression Condition

When adding an expression condition:

1. In the **Test Expression** box, enter the expression to test:

Below there are examples of expressions:

```
messagetype == 4
```

```
totalsegments >= 4
```

```
messagetype == 0 && totalsegments >= 4
```

In case of a concatenated SM, it is counted by message, not by segment. So, in concatenated message counted only the first segment of a concatenated message. Expression condition is used to filter the segments of SM. In this configuration, expression condition must be configured in the filter condition.

For example:

```
totalsegments < 2 || currentsegment == 1
```

Filter Conditions

Invert:	<input type="checkbox"/>
Filter Name:	FAF Blacklist Filters
Name:	Allow unsegment or first segmen
Type:	Expression
Test Expression:	totalsegments < 2 currentsegment == 1
Assignment Expression:	
Last Updated:	2017-09-15 19:03:25

- In the **Assignment Expression** box, enter the expression to assign a value to a variable.

For example:

```
eciattribute2 = 1
```

10.3.1.1 Expression Variables

The following variables are available for use in expression conditions:

Variable	Valid Values	Can be used in...
messagetype	<ul style="list-style-type: none"> 0: MO short message 1: MT short message 2: AO short message 3: AT short message 4: HLR SRI-SM request 5: HLR SRI-SM response 6: MT delivery notification 7: AT delivery notification 	Test expression
failuremessagekey	An integer	Test expression and assignment expression
eciattribute[n] where [n] is 1 through 32	0 or 1	Test expression and assignment expression

Variable	Valid Values	Can be used in...
totalsegments	An integer. Range - 0 to 255 totalsegments will have the value of 0 in case the message is not segmented.	Test expression

Note: A test expression containing the expression variable "totalsegments" will be evaluated against the value received for the ECI message field "cmTotalSegments" in the ECI validation request. If "cmTotalSegments" is not included for the ECI application, the "totalsegments" expression will be assigned the value of 0.

By default, the ECI message field "cmTotalSegments" is not included for the ECI application.

10.3.1.2 Expression Operators

The expression condition supports the following operators:

Operator	Meaning
	Logical OR
&&	Logical AND
<	Less than
<=	Less than or equal to
>	Greater than
>=	Greater than or equal to
==	Equal to
!=	Not equal to
+	Plus
-	Minus
*	Multiplied by
/	Divided by
%	Modulo (remainder of division)

10.3.2 Add a Content Condition

When adding a content condition:

1. From the **Field** list, select the message field to which the condition should be applied; the default and most commonly used field is Data (message content).
Refer to [Message Field Options](#) for a complete list of available message fields and descriptions.

2. From the **List** list, select the advanced filter list to use.
3. From the **Accuracy** list, select the accuracy level for matching:
 - Exact
 - Case-insensitive
 - Tokenised
 - Normalised
 - Regular Expression

The accuracy indicates an implicit transformation that the FAF performs on all text involved in the match before the match is calculated.

Note: The case-insensitive match only works for characters that are supported by operating system function call `tolower()`. In most operating systems, the `tolower()` function supports basic ASCII. Some operating systems also support extended ASCII that includes German and Nordic characters. You can verify the characters supported by the operating system `tolower()` function with the following command on the command line interface:

```
# locale -k LC_CTYPE
```

4. In the **Whole Words Match** checkbox specify if the FAF should perform matching on whole words only. For example:
 - Exact matching: "apple" matches text "this is an apple.", but not "this is a pineapple." or "these are apples."
 - Case-insensitive matching: "apple" matches "Apple is good.", but not "PineApple is good."

Note: This checkbox is only available for the Exact and Case-insensitive **Accuracy** matches.
5. From the **Modify** list, select how the target text should be modified:
 - None
 - Mask string (will not increase the length of the target string)
 - Replace string (may affect the length of the target string)
 - Replace message

CAUTION: Do not use text replacement/append functions that may make the user data longer than the original user data. When applied to a "full segment" this will lead to an undeliverable message.

6. If you select a content modification option other than **None**, enter the text that should mask or replace the target text in the **Replacement Text** box.
 - Note that the **Modify** option is relevant only for the user data field and should be set to **None** for all other message fields.

10.3.2.1 Message Field Options

The message fields that can be selected in **Field** list for the content, duplicates, flooding, and bulk conditions:

Field (number)	ECI Field	Description	Additional Information
path (1)	routingPath	Routing path	Integer format. Supported values are: <ul style="list-style-type: none"> • moMo (0) • moMt (1) • moMtMo (2) • moMtAt (3) • moAt (4) • moDiscardWithNack (5) • moDiscardWithAck (6) • moDiscardSilently (7) • mtMt (10) • mtBlockWithTemporaryError (11) • mtBlockWithPermantError (12) • mtBlockWithNoResponse (13) • mtBlockWithAck (14) • aoAo (20) • aoMt (21) • aoMtAo (22) • aoAt (23) • aoDiscardWithAck (24) • aoDiscardWithNak (25) • atAt (30) • atBlockWithTemporaryError (31) • atBlockWithPermanentError (32) • atBlockWithAck (33)
submit (3)	originalSubmitTime	Not adjusted submit time	Original submission time, in Unix time format.
uniq (4)	uniqueSubmitTime	Adjusted (made unique) submit time	Time the message was submitted to the RTR. Note that this field contains the potentially adjusted submission time as described in the RTR Operator Manual chapter on Service Center Time Stamps.
deliv (5)	deliveryTime	Delivery time	Time the RTR delivered or deleted the message. In Unix time format.
orig (6)	originatorAddress	Originator address	Self explanatory. In ASCII string format with prefix. National number is with prefix "N", international is with prefix "+", unknown is with prefix "U", alphanumeric is with prefix "A". For example, N12345678, Aalphanumeric.
origImsi (7)	originatorImsi	Originator IMSI	Self explanatory. In ASCII string format.

Field (number)	ECI Field	Description	Additional Information
smsc (8)	smscAddress	SMSC address	Self explanatory. In ASCII string format.
msc (9)	mscAddress	MSC address	Self explanatory. In ASCII string format.
recip (10)	recipientAddress	Recipient address	Self explanatory. An ASCII string format with the same prefix as "orig".
recipImsi (11)	recipientImsi	Recipient IMSI	Self explanatory. In ASCII string format.
segTotal (12)	cmTotalSegments	Total number of segments	Total number (0-255) that indicates the total number of pieces in a concatenated message (only present in case of a concatenated message when received as a part of SMPP <code>sar_total_segments</code> or as a part of 8 bit reference or 16 bit reference number UDH IEI).
segId (13)	cmCurrentSegment	Segment number	Current segment number (0-255) of the concatenated message. A running number for each part of a concatenated message (only present in case of a concatenated message when received as a part of SMPP <code>sar_segment_seqnum</code> or as a part of 8 bit reference or 16 bit reference number UDH IEI).
len (15)	lengthOfMessage	Length of message	Number of characters in septets or octets, depending on the data coding scheme (DCS).
header (17)	userDataHeader	User data header	<p>Value specified in one of the information element identifiers (IEIs) of the user data header (UDH) of the message. Only evaluates positively if there is an exact match with the information element identifier (00-FF, hexadecimal) of the UDH.</p> <p>Refer to technical specification 3GPP 23.040 for more information. Most common IEI values:</p> <ul style="list-style-type: none"> • 00: Concatenated short message • 01: Special SMS message indication • 04: Application port addressing scheme, 8-bit address

Field (number)	ECI Field	Description	Additional Information
			<ul style="list-style-type: none"> • 05: Application port addressing scheme, 16-bit address • 06: SMSC control parameters • 07: UDH Source Indicator
encoding (18)	dataCodingScheme	Data Coding Scheme (DCS)	Data coding scheme (DCS) specified in the message. The value is in decimal format.
data (19)	userData	Message data	The content can be already modified by other filters. Decoded into UTF-8 format.
statrepinfo (20)	statusReportInfo	Status report information	Opaque value containing the reference for the SS7 Status Report assigned by the TPR.
smppMsgId (21)	smppMessageId	SMPP message ID	In string format.
dataorg (22)	userData	User data	This is the original message content from ECI. Decoded into UTF-8 format.
segRef (23)	cmReferenceNr	Segment reference	Same for all segments in a concatenated SMS (received as a part of SMPP sar_msg_ref_num or as a part of 8 bit reference or 16 bit reference number UDH IEI).
notifreq (24)	notificationRequest	Notification request	Indicates whether notification or status report was requested for this message (true) or not (false).
callingGt (25)	callingPartyAddress	Calling global title	GT of the SCCP Calling Party Address in the message. In ASCII string format.
calledGt (26)	calledPartyAddress	Called global title	GT of the SCCP Called Party Address in the message. In ASCII string format.
delstat (42)	deliveryStatus	Delivery status	Result of a delivery attempt as reported in a notification on an AO/SM. In integer format. Supported values are: <ul style="list-style-type: none"> • noStatusAvailable (0) • inProgress (1) • validityPeriodExpired (2) • deliveryFailed (3) • deliverySuccessful (4) • noResponse (5) • lastNoResponse (6)

Field (number)	ECI Field	Description	Additional Information
			<ul style="list-style-type: none"> • cancelled (7) • deleted (8) • deletedByCancel (9) • scheduled (10) • accepted (11) • rejected (12) • skipped (13) • replaced (14)
exconrule (55)	selectedExternalConditionRule	Name of external condition rule	Name of the external condition rule used to forward the message to the FAF.
protocolId (60)	protocolId	Protocol identifier	<p>Indicates the value of the TP-PID field (included in the MAP header), if the message was MO or MT. Otherwise (i.e. for AO or AT messages) it indicates the value of the protocol id parameter included (if any) in the message.</p> <p>This field is not applicable for status reports and notifications.</p> <p>Valid values are in the range 0-255.</p>

Note: The 'protocolId' message field should not be selected while configuring a duplicates, flooding or bulk filter condition, because it has no relevant use case for these filters.

10.3.3 Add a Duplicates Condition

When adding a duplicates condition:

Note: Certain parameter changes in the duplicates filter condition may take a long time to effect due to the large state that is kept in the filters. Especially when the filter is full (has the maximum amount of memory state), it can take quite some time for the changes to take effect (sometimes 30 minutes or more).

1. From the **Field** list, select the message field to evaluate; the default and most commonly used field is Data.
Refer to [Message Field Options](#) for a complete list of available message fields and descriptions.
2. In the **Spacing** box, enter the number of allowed dissimilar messages (2-99,999) between two similar messages (default 1,000).
If more messages than this are found between two similar messages, the similar messages are not considered duplicates.
3. In the **Min. Size** box, enter the minimum number of messages (2-1,000) required to start a duplicates cluster (defaults to 10).

4. In the **Length** box, enter the minimum number of features (4-160) required for to start duplicates clustering (defaults to 4).
5. In the **Threshold** box, enter the minimum number of messages (2-999,999) that must be in the cluster for the duplicates condition to return true (defaults to 10).
6. In the **Similarity** box, enter the percentage (0-100) that messages must be similar to be placed in the same cluster (defaults to 80%).
100% means the messages must match exactly.
7. In the **Delete Age** box, enter the number of seconds (0-999,999) that a never-matched cluster is allowed to exist before it is deleted (0 means clusters are never deleted).
If the cluster is matched, the timer restarts for the cluster.

10.3.4 Add a Flooding Condition

When adding a flooding condition:

1. From the **Field** list, select the message field to evaluate.
The field should depend on the type of traffic that is being evaluated for flooding. For example, for MO traffic, the MSC should be used; for MT traffic, the SMSC should be used.
Refer to [Message Field Options](#) for a complete list of available message fields and descriptions.
2. In the **Significant Digits** box, enter the number of digits (0-16) of the specified field that are taken into account when tracking originators (defaults to 16, which is recommended).
The first digits of the number are used; for example, for a setting of 6, the originator numbers 15562235 and 155622234 map to the same trackable originator.
More digits may be taken into account if the FAF detects higher traffic.
3. In the **Minimal Traffic** box, enter the minimum number of messages per second (1-1,000,000) required for the filter to become active (defaults to 5, which is recommended).
This is the constant threshold used to compute the flooding detection threshold. Use this setting to prevent spurious flooding detection at low traffic levels. Higher values make flooding detection less likely.
4. In the **Traffic Increase Rate** box, enter a relative increase in traffic (1-10,000%) used to compute the flooding detection threshold.
This is the traffic increase that is required to trigger the filter. The value is relative to the long-term traffic average. Higher values make flooding detection less likely.
5. In the **Time Delay** box, enter the number of seconds (1-10,000) that the short-term traffic average must exceed the flooding detection threshold before the filter becomes active (defaults to 30).
The condition only yields true this number of seconds after the flooding detection threshold has been exceeded. Higher values make flooding detection less likely.
6. In the **Filter Period Flooding** box, enter the number of seconds (1-10,000) to use to calculate the short-term traffic average (default 10).
This is the response time used to compute the short-term traffic average. Fluctuations shorter than this period are filtered out. Higher values make flooding detection less likely.
7. In the **Filter Period Baseline Traffic** box, enter the number of seconds (1-10,000) to use when calculating the long-term traffic average (defaults to 3600).

Fluctuations slower than this are not considered flooding. This value should be significantly higher than the **Time Delay**; a factor of at least 20 is recommended. Higher values make flooding detection less likely.

8. In the **Margin** box, enter the threshold, in messages per 1000 seconds (1-100,000), below which traffic from a trackable originator is not tracked (default 5).

For example, for a value of 10, originators sending less than 10 messages per 1000 seconds are not tracked. Use this parameter to avoid using FAF processing performance for message originators for which the traffic lies below a level of interest. Higher values make flooding detection less likely.

10.3.5 Add an Enhanced Messaging (EMS) Condition

When adding an enhanced messaging (EMS) condition:

1. In the **Protocol Id Values** box, enter the desired protocol id value(s) against which the EMS filter condition should compare the protocol id of a message. If no protocol id value is entered, then the filter condition will match any message protocol id.
2. Select one of more Information Element IDs (IEIs) on which to filter:
 - 00 - Concatenated short messages, 8-bit reference number
 - 01 - Special SMS Message Indication
 - 03 - Value not used to avoid misinterpretation as LF character
 - 04 - Application port addressing scheme, 8 bit address
 - 05 - Application port addressing scheme, 16 bit address
 - 06 - SMSC Control Parameters
 - 07 - UDH Source Indicator
 - 08 - Concatenated short message, 16-bit reference number
 - 09 - Wireless Control Message Protocol
 - 10 - Text Formatting
 - 11 - Predefined Sound
 - 12 - User Defined Sound (iMelody max 128 bytes)
 - 13 - Predefined Animation
 - 14 - Large Animation (16*16 times 4=128 bytes)
 - 15 - Small Animation (8*8 times 4 = 8*4 = 32 bytes)
 - 16 - Large Picture (32*32 = 128 bytes)
 - 17 - Small Picture (16*16 = 32 bytes)
 - 18 - Variable Picture
 - 19 - User prompt indicator
 - 20 - Extended Object
 - 21 - Reused Extended Object
 - 22 - Compression Control
 - 23 - Object Distribution Indicator
 - 24 - Standard WVG Object
 - 25 - Character Size WVG Object
 - 26 - Extended Object Data Request Command
 - 32 - RFC 822 E-Mail Header
 - 33 - Hyperlink format element
 - 34 - Reply Address Element

- 35 - Enhanced Voice Mail Information
- 36 - National Language Single Shift
- 37 - National Language Locking Shift

If the user data header (UDH) of a message contains the selected IEI(s), FAF will return "true" for the condition. The EMS condition uses a logical OR operation; therefore, if you select multiple IEIs and also configure certain protocol id values for one EMS condition and the message contains any of the selected IEIs OR any of the configured protocol ids, the condition will return "true". Refer to the 3GPP 23.040-920 specification for a description of EMS IEIs.

3. If you selected "04 - Application port addressing scheme, 8 bit address":
 - a. Enter an 8-bit source port number in the **8 Bit Source Port** box.
 - b. Enter an 8-bit destination port number in the **8 Bit Destination Port** box.

If the source port and/or destination port in the UDH of a message matches the provisioned port, FAF will return "true" for the condition. If you do not provision port numbers, FAF simply checks for the presence of the IEI, and returns "true" if it is present.

4. If you selected "05 - Application port addressing scheme, 16 bit address":
 - a. Enter a 16-bit source port number in the **16 Bit Source Port** box.
 - b. Enter a 16-bit destination port number in the **16 Bit Destination Port** box.

If the source port and/or destination port in the UDH of a message matches the provisioned port, FAF will return "true" for the condition. If you do not provision port numbers, FAF simply checks for the presence of the IEI, and returns "true" if it is present.

10.3.6 Add a Volume Condition

When adding a volume condition:

1. From the **Group By** list, select a value that determines on which fields to group and count messages for the Volume filter condition.

Possible options are:

- **Nothing** — Count all messages
- **Originator** — Group and count messages based on originator address (as specified in the TP-Originating-Address (TP-OA) field of the SMS Message).
- **Content** — Group and count messages based on raw SMS user data content (as specified in the TP-User Data (TP-UD) field of the SMS Message).
- **Originator + Content** — Group and count messages based on originator address and raw SMS user data content

2. In the **Memory** field, enter the amount of memory in Megabytes (MB) to dedicate for the tracking of elements in the filter. Valid values range from 256 to 65,536 MB. Default is 1024 MB.

This value is a hard memory limit on the amount of memory dedicated for storing data for this filter. When the memory limit is reached, a trap is generated.

Refer to the FAF Operator Manual, Volume Condition for more information on memory dimensioning.

3. In the **Period** field, enter the tracked period of time in seconds. Valid values range from 60 seconds (one minute) to 86,400 seconds (one day) . Default is 3600 seconds (one hour).
4. In the **Threshold** field, enter the number of messages in each grouping after which the condition shall apply (return 'true'). Valid values range from 0 to 2,147,483,647 messages. Default is 200 messages.
5. In the **Daily Reset** field, select **Absolute Time** to reset the volume counter for the subscriber. The default value is **None**, meaning that no volume counter will be reset.
6. In the **Reset At** field, enter the hours, minutes and seconds (default 0, 0, 0 respectively). This is the absolute time when the volume counter for subscriber will be reset. This field is applicable when **Daily Reset** is set to **Absolute Time**.

The interval format is HH MM SS, where:

- HH is the hour, 0-23
- MM is Minute, 0-59
- SS is Second, 0-59

Note: While doing configuration of this field from `tp_shell`, the user needs to provide the duration (HHMMSS) in `fafVolumeDailyResetTimeHour`, `fafVolumeDailyResetTimeMinute` and `fafVolumeDailyResetTimeSecond` fields.

10.3.7 Add a Bulk Condition

When adding a bulk condition:

Note: Certain parameter changes in the bulk filter condition may take a long time to effect due to the large state that is kept in the filters. Especially when the filter is full (has the maximum amount of memory state), it can take quite some time for the changes to take effect (sometimes 30 minutes or more).

1. From the **Field** list, select the message field to evaluate; the default and most commonly used field is `Orig`.
Refer to [Message Field Options](#) for a complete list of available message fields and descriptions.
2. In the **Threshold** box, enter the minimum number of seconds (0-999,999) to mark a message as bulk (defaults to 10).
When the average time span between messages is lower than this threshold, the message is regarded as bulk and the condition returns false.
3. In the **Window Size** box, enter the window size (0-999,999) used to calculate the average timespan (defaults to 64).

This is the filter constant for the auto-regressive low-pass filter, which is based on the following algorithm:

$$\text{new_value} = \text{old_value} * C + \text{window_size} * (1 - C)$$

Where:

- `window_size` is the timepan between two subsequent messages
- `window` is this parameter
- $C = \exp(-\text{timespan}/\text{window})$

The larger the window size, the slower the low-pass filter becomes; that is, the less responsive the filter becomes to quick changes in value.

4. In the **Expiration Period** box number of seconds (0-999,999) before a record expires (default 3600). When a record matches, the FAF updates the record's timestamp. When the timestamp is older than the expiration time, the FAF deletes the record.

10.3.8 Add a Spread Condition

When adding a spread condition:

1. In the **Max. Subscribers** box, enter the maximum number of subscriber numbers the spread filter can contain. Entries are replaced on a least recently used (LRU) basis. This variable can only be changed when the admin state is `inactive`. The valid range is 1-64800000 and the default value is 864000.
2. In the **Recipient Count** box, enter the size of the recipient bitmap. The recipients are hashed via hash function to an entry in the recipient bitmap. This variable can only be changed when the admin state is `inactive`. The valid range is 0-99999 and the default value is 1000. It is recommended to set this to at least thrice the size of the **Recipient Limit**.
3. In the **Search Limit** box, enter the number of records to search for a free slot in the maintained subscriber list by the Spread filter where the new record can be inserted. The starting point of the search in the list will be the index calculated on the basis of hash value of the Originator contained in the message. Increasing this value will increase the accuracy of search in the subscriber list but will also increase CPU time for the spread filter. This variable can only be changed when the admin state is `inactive`. The valid range is 1-999 and the default value is 16.
4. In the **Message Limit** box, enter the limit of number of messages per subscriber. If the number of total sent messages exceeds this value, the number of entries in the recipient bitmap is counted. This variable can be changed when the admin state is `active`. The valid range is 0-2147483647 and the default value is 1000.
5. In the **Recipient Limit** box, enter the limit of different entries in the recipient bitmap that approximates the number of different recipients the originator has sent their messages to. If both this limit and the Message Limit are exceeded, then the spread filter returns true. This variable can be changed when admin state is `active`. Valid range is (0-9999) and the default value is 300.
6. From the **Reset At** field, select **Daily** to reset the spread filter daily, select **Weekly** to reset the spread filter weekly, or select **Monthly** to reset the spread filter monthly. Default is **Daily**.
7. From the **Day of the Week** field, select a day of week to reset the spread filter weekly. Default is **Monday**. This field is applicable only if **Reset At** is set as **Weekly**.
8. From the **Day of the Month** field, select a day of month to reset the spread filter monthly. Default is 1. This field is applicable only when **Reset At** is set to **Monthly**.

9. In the **Reset Time** field, enter the hours, minutes and seconds (default 0, 0, 0 respectively). This is the absolute time when the spread filter will be reset.

The interval format is HH MM SS, where:

- HH is the hour, 0-23
- MM is the minute, 0-59
- SS is the second, 0-59

Note: While doing the configuration of this field from `tp_shell`, the user needs to provide the duration (HHMMSS) in the fields `fafSpreadResetTimeHour`, `fafSpreadResetTimeMinute` and `fafSpreadResetTimeSecond`.

10.3.9 Add a Delta Condition

When adding a delta condition:

1. In the **Max. Subscribers** box, enter the maximum number of subscriber numbers the delta filter can contain. Entries are replaced on a least recently used (LRU) basis. This variable can only be changed when the admin state is `inactive`. The valid range is 1-64800000 and the default value is 864000.
2. In the **Search Limit** box, enter the number of records to search for a free slot in the maintained subscriber list by the Delta filter where the new record can be inserted. The starting point of the search in the list will be the index calculated on the basis of hash value of the MSISDN contained in the message. Increasing this value will increase the accuracy of search in the subscriber list but will also increase CPU time for the delta filter. This variable can only be changed when the admin state is `inactive`. The valid range is 1-999 and the default value is 16.
3. In the **Recv Send Percent** box, enter the ratio percentage between SMS received and SMS sent by a subscriber. If the ratio percentage is equal to or lesser than the configured value of this field and the total number of messages for that subscriber reaches a value equal to or greater than the value of configured **Message Limit**, the filter matches. This variable can be changed when the admin state is `active`. The valid range is 0-100 and the default value is 5.
4. In the **Message Limit** box, enter limit of number of messages per subscriber. If the number of total messages (send + receive) is equal to or above this value and the ratio percentage between SMS received and SMS sent is lower than or equal to the configured value of field **Recv Send Percent**, the Delta filter returns true. This variable can be changed when the admin state is `active`. The valid range is 0-2147483647 and the default value is 1000.
5. From the **Reset At** field, select **Daily** to reset the delta filter daily, select **Weekly** to reset the delta filter weekly, or select **Monthly** to reset the delta filter monthly.
6. From the **Day of the Week** field, select a day of week to reset the delta filter weekly. This field is applicable only if **Reset At** is set as **Weekly**.
7. From the **Day of the Month** field, select a day of month to reset the delta filter monthly. This field is applicable only when **Reset At** is set to **Monthly**.
8. In the **Reset Time** field, enter the hours, minutes and seconds (default 0, 0, 0 respectively). This is the absolute time when the delta filter will be reset.

The interval format is HH MM SS, where:

- HH is the hour, 0-23
- MM is the minute, 0-59
- SS is the second, 0-59

Note: While doing the configuration of this field from `tp_shell`, the user needs to provide the duration (HHMMSS) in the fields `fafDeltaResetTimeHour`, `fafDeltaResetTimeMinute` and `fafDeltaResetTimeSecond`.

10.4 Create an Advanced Filter List

Use filter lists with the FAF's content condition type to filter certain words or phrases.

To create a filter list:

1. In the left navigation bar, select **Advanced Filters ► Lists**.

The Filter List tab appears.

2. Click **Add New**.

A new Filter List tab appears.

3. Enter a unique name for the list in the **Name** box (up to 31 characters).
4. Optionally enter a description of the list in the **Description** box.
5. In the **Text** box, enter the word(s) and/or phrase(s) the FAF should detect, each on a separate line.
6. Click **Save**.

The MGR creates the filter list and closes the tab.

7. Activate the list.

Chapter 11

Billing

Topics:

- *Introduction.....288*
- *Configuring Prepaid Billing.....288*
- *Configuring Post-Paid Billing.....289*

11.1 Introduction

Manage billing profiles and billing properties for all types of traffic. The MGR supports the following billing file formats:

- Formatted call detail record (FDCR)
- Nokia call detail record (NCDR)
- Ericsson call detail record (ECDR)
- Comverse call detail record (CCDR)
- Ss8 call detail record
- Logica call detail record (LCDR)
- Huawei comma-separated values (CSV) call detail record (HCDR)
- CCDR 3G Format (CCDRG)

11.2 Configuring Prepaid Billing

When your system includes the eXternal Service Short Message Copy (XS-CPY) and/or eXternal Service Short Message Forward (XS-FWD) component, you can implement prepaid billing for messages that are copied or forwarded.

Prerequisites:

- EC application

To configure prepaid billing:

1. In the left navigation bar, select **Billing** ► **Pre-paid Billing** ► **Properties**.

The Pre-paid Billing Properties tab appears.

2. From the **Originator Copy Billing Application** list, select the EC application to use for billing originator-requested (MO) copies.
3. If the RTR should ignore a negative billing result (that is, the PBC returning "false") for the MO copy and the XS-CPY service should continue, select **Ignore Negative Billing Result**.
4. From the **Recipient Copy Billing Application** list, select the EC application to use for billing recipient-requested (MT) copies .
5. If the RTR should ignore a negative billing result (that is, the PBC returning "false") for the MT copy and the XS-CPY service should continue, select **Ignore Negative Billing Result**.
6. From the **Unc. Forwarding Billing Application** list, select the EC application to use for billing unconditional forwarding
7. From the **Cond. Forwarding Billing Application** list, select the EC application to use for billing conditional forwarding
8. If the RTR should ignore a negative billing result (that is, the PBC returning "false") for forwarding and the XS-FWD service should continue, select **Ignore Negative Billing Result**.
9. From the **Recipient Copy to Email Billing Application** list, select the EC application to use for billing recipient-requested copies to e-mail address(es).

10. If the RTR should ignore a negative billing result (that is, the PBC returning "false") for the recipient copy to e-mail and the XS-CPY service should continue, select **Ignore Negative Billing Result**.
11. From the **Unc. Forward to Email Billing Application** list, select the EC application to use billing unconditional forwarding to email address(es).
12. If the RTR should ignore a negative billing result (that is, the PBC returning "false") for unconditional forwarding to email and the XS-FWD service should continue, select **Ignore Negative Billing Result**.
13. Click **Save**.
The MGR saves the billing properties and closes the tab.

Pre-paid Billing Properties

Originator Copy Billing Application:	▼	PBC EC Application	▼
Ignore Negative Billing Result:	▶	<input checked="" type="checkbox"/>	
Recipient Copy Billing Application:	▼	PBC EC Application	▼
Ignore Negative Billing Result:	▶	<input type="checkbox"/>	
Unc. Forwarding Billing Application:	▼	Don't Charge	▼
Cond. Forwarding Billing Application:	▼	Don't Charge	▼
Recipient Copy to Email Billing Application:	▼	xscopy	▼
Ignore Negative Billing Result:	▶	<input checked="" type="checkbox"/>	
Unc. Forward to Email Billing Application:	▼	xsfwd	▼
Ignore Negative Billing Result:	▶	<input type="checkbox"/>	
Last Updated:		1970-01-01 01:00:00	

Figure 26: Prepaid billing properties

11.3 Configuring Post-Paid Billing

This section describes the configuration of post-paid billing.

11.3.1 Creating Billing Profiles

To create a billing profile:

1. In the left navigation bar, select **Billing** ► **Post-paid Billing** ► **Profile**.
The Billing Profile tab appears.
2. Click **Add New**.
A new Billing Profiles tab appears.
3. Enter a unique name for the billing profile in the **Name** box.
4. Optionally enter a description of the billing profile in the **Description** box.
5. In the **Processing Directory** box, enter the directory in which to store the billing files while they are being created (defaults to `/var/TextPass/processing`).

Note: In a multi-instance setup, the processing directory should be specific to the user, i.e. where the billing files for a particular user need to be stored during creation.

6. In the **Finished Directory** box, enter the directory in which to store the billing files after they are created (defaults to `/var/TextPass/billing`).

Note: In a multi-instance setup, the finished directory should be specific to the user, i.e. where the billing files for a particular user need to be stored.

7. In the **Copy 1 of Finished Directory** through **Copy 9 of Finished Directory** boxes, enter directories in which to create hard links to the billing files in the finished directory (by default, there are no copies of the finished directory).

Note: The finished directory and all finished directory copies must be on the same disk partition as the processing directory.

8. In the **Filename Template** box, enter the template that will be used to name the billing files (defaults to `cdr_%h_%U_%Y%m%d_%H%M%S_%3.dat`).

Important: If multi-instances of RTR are running on the same node, then it is important to include the `%U` escape sequence, which will be translated to UID (operating system user identifier). This ensures that multiple components will not try to create billing files with identical names.

9. In the **Max. File Size** box, enter the maximum size of a billing file in bytes (defaults to 1048576 bytes, which is 1 MB). The range is 1024 bytes (1 KB) to 1073741824 bytes (1 GB).
10. In the **Max. File Duration** box, enter the maximum duration of a billing file in seconds (defaults to 3600 seconds, which is 1 hour). The range is 1 second to 2,678,400 seconds (1 month).
11. In the **Max. File Records** box, enter the maximum number of records to allow in a billing file (defaults to 10000 records). The range is 1 record to 10,000,000 records.
12. In the **Starting Sequence Number** box, enter the number with which to start the billing file numbering sequence (defaults to 0).
13. Select one or more types of messages that this billing profile applies to from the **Affected Message Types** list.
14. If this billing profile should be restricted to successful deliveries, select **Applicable For Successful Cases Only** (disabled by default).
15. Select **Use SMPP SAR info.** if the concatenation information received in the SMPP SAR TLVs is to be used to store the UDH information in the CDRs. This field is not applicable for Comverse CDRs. (disabled by default).
16. Select the file format for this billing profile from the **File Format** list.
17. Click **Save**.

The MGR saves the billing profile and closes the tab.

18. Activate the profile.

Billing Profiles

Index:	Auto Generated
Name:	<input type="text"/>
Description:	<input type="text"/>
Processing Directory:	<input type="text" value="/var/TextPass/processing"/>
Finished Directory:	<input type="text" value="/var/TextPass/billing"/>
Copy 1 Of Finished Directory:	<input type="text"/>
Copy 2 Of Finished Directory:	<input type="text"/>
Copy 3 Of Finished Directory:	<input type="text"/>
Copy 4 Of Finished Directory:	<input type="text"/>
Copy 5 Of Finished Directory:	<input type="text"/>
Copy 6 Of Finished Directory:	<input type="text"/>
Copy 7 Of Finished Directory:	<input type="text"/>
Copy 8 Of Finished Directory:	<input type="text"/>
Copy 9 Of Finished Directory:	<input type="text"/>
Filename Template:	<input type="text" value="cdr_%h_%U_%Y%m%d_%H%M%S_%3.c"/>
Max. File Size:	<input type="text" value="1048576"/> [byte]
Max. File Duration:	<input type="text" value="3600"/> [sec]
Max. File Records:	<input type="text" value="10000"/> [num]
Starting Sequence Number:	<input type="text" value="0"/>
Affected Message Types:	<input type="checkbox"/> 0 - MO <input type="checkbox"/> 1 - MT <input type="checkbox"/> 2 - AO <input type="checkbox"/> 3 - AT
Applicable For Successful Cases Only:	<input type="checkbox"/>
Use SMPP SAR info.:	<input type="checkbox"/>
File Format:	▼ <input type="text" value="FCDR-Formatted Call Detail Record"/> ▼
Not Delivered Status:	▶ <input type="text" value="submitted"/> ▼

Figure 27: Post-paid billing profile

11.3.1.1 Billing File Name Template

Use the following case-sensitive variables to construct the billing file name template:

Variable	Description
%Y	Year formatted with four digits (for example, 2008)
%y	Year formatted with two digits (for example, 08)
%m	Month formatted with two digits (for example, 01 for January and 10 for October)
%d	Day formatted with two digits (for example, 01 for the first day of May and 31 for the last day of May)
%H	Hour in 24-hour time format
%M	Minutes
%S	Seconds
%h	Host name

Variable	Description
%U	UID (operating system user identifier) of the user from which RTR process is running
%i	Value of the <code>billingid</code> parameter in the semi-static configuration file
%1	One-digit sequence number
%2	Two-digit sequence number
%3	Three-digit sequence number
%4	Four-digit sequence number
%5	Five-digit sequence number
%6	Six-digit sequence number
%7	Seven-digit sequence number
%8	Eight-digit sequence number
%n5	Number of records (lines) in the file, in five digits (HCDR only)
%n6	Number of records (lines) in the file, in six digits (HCDR only)
%n7	Number of records (lines) in the file, in seven digits (HCDR only)
%n8	Number of records (lines) in the file, in eight digits (HCDR only)
%n9	Number of records (lines) in the file, in nine digits (HCDR only)

Sample File Names

For example, the default file name template, `cdr_%h_%Y%m%d_%H%M%S_%3.dat`, results in the following files:

- `cdr_southhost_20080830_023145_111.dat`
- `cdr_southhost_20080831_141020_112.dat`
- `cdr_southhost_20080901_220500_113.dat`

Sample File Names (on multi-instance setup)

For example, the default file name template for `textpass` user, `cdr_%h_%U_%Y%m%d_%H%M%S_%3.dat`, results in the following files:

- `cdr_southhost_200_20080830_023145_111.dat`
- `cdr_southhost_200_20080831_141020_112.dat`
- `cdr_southhost_200_20080901_220500_113.dat`

11.3.1.2 Billing File Formats

This section describes the customisable properties of CDRs.

11.3.1.2.1 Formatted Call Detail Record (FCDR)

This section lists the customizable properties for formatted call detail records (FCDRs).

Customizable Status Fields

You can customize the following status fields:

Field	Description	Default
Not Delivered Status	Value to use in the FCDR Status field when a message is not sent to an application due to decimation or because a rule with an action to discard with ACK was applied	Submitted
Mt Sri Only Status	Value to use in the FCDR Status field when an SRI-SM was executed for an MT delivery attempt (AO-MT or MO-MT)	Deleted
Mt Failed Status	Value to use in the FCDR Status field when an MT delivery attempt failed	Submitted
Mt Success Status	Value to use in the FCDR Status field when an MT delivery attempt succeeded	Delivered

Address Formats

The FCDR address format fields can have the following formats:

Format	Description
Transparent	The RTR passes the address to its destination in the same format as received in the original message.
National	Before passing the address to its destination, the RTR converts national addresses to national format, including the trunk prefix (0); for example, 06309303100. The RTR converts international addresses to international format, including the international prefix (00); for example, 00380676750000. In these cases, the TON is unknown and the NPI is E164. Short numbers are not converted.
International	Before passing the address to its destination, the RTR converts the address to international format, excluding the international prefix (00); for example, 31627093038. In these cases, the TON is international and the NPI is E164. Short numbers are not converted.

Customizable Address Fields

You can customize the following FCDR address format fields:

Field	Description	Default
Format Orig Address	How the origAddress field should be specified in the CDR	Transparent
Format Orig Address GSM	How the origAddressGSM field should be specified in the CDR	Transparent
Format Recip Address	How the recipAddress field should be specified in the CDR	Transparent
Format Recip Address GSM	How the recipAddressGSM field should be specified in the CDR	Transparent

Field	Description	Default
Format Notif Address	How the notifAddress field should be specified in the CDR	Transparent
Format Notif Address GSM	How the notifAddressGSM field should be specified in the CDR	Transparent
Format Ogti Address	How the ogtiAddress field should be specified in the CDR	Transparent
Format Ogti Address GSM	How the ogtiAddressGSM field should be specified in the CDR	Transparent
Format Dgti Address	How the dgtiAddress field should be specified in the CDR	Transparent
Format Dgti Address GSM	How the dgtiAddressGSM field should be specified in the CDR	Transparent
Format Calling Line Id	How the callingLineId field should be specified in the CDR	Transparent
Format Calling Line Id GSM	How the callingLineIdGSM field should be specified in the CDR	Transparent

Customizable ASN.1 Fields

You can customize the following SMSC-compatible ASN.1 fields:

Field	Description	Default
Encrypt User Data	Controls whether the userData part of the smsContents will be encrypted. By default, this property is set to 'false'. It requires the licGenEncryptUserData license to be set to 'true'. Note: Encrypt User Data is supported only if Lang and SMS Content fields are included in the FCDR Billing Profile.	Cleared
Use AO for consolidation for AO AT	For AO-AT routing, controls whether the FCDR's consolidation field is set to the consolidation field of the destination application (cleared) or of the originating application (selected).	Cleared
Use Short Number as Originator for AO	Controls whether the origAddress and origAddressGSM fields of FCDRs for AO messages shall always contain the originating application's short number rather than the originator address indicated in the message. By default, this property is set to 'false' (cleared). When set to 'true' (selected), the short code of the originating application will be used, unless the message is flagged as 'billing on behalf of' (BOBO). In that case the	Cleared

Field	Description	Default
	originator address as indicated in the message will be used.	
Inc. Charge Info	Proprietary field only used for NewNet native Diameter. This field controls whether the chargeInfo field should be included in the CDR (only applies when PBC is in use with the NewNet native Diameter protocol).	Cleared
Inc. Originator Cell Id	Proprietary field that controls whether the originatorCellId field should be included in the CDR (only applies to Mobile Originated flows and visible in GUI when MAP-ATI bit in license is enabled).	Cleared
Inc. Recipient Cell Id	Proprietary field that controls whether the recipientCellId field should be included in the CDR (only applies to Mobile Terminated flows and visible in GUI when MAP-ATI bit in license is enabled).	Cleared
Inc. Originating App. Charging Units	Controls whether the originatorApplicationChargingUnits field should be included in the CDR (only applies when PBC is in use).	Cleared
Inc. Recipient App. Charging Units	Controls whether the recipientApplicationChargingUnits field should be included in the CDR (only applies when PBC is in use).	Cleared
Subscriber Status	Proprietary field that controls whether the subscriberStatus field should be included in the CDR (only applies when PBC is in use).	Cleared
Subscriber Status Of Recipient	Proprietary field that controls whether the subscriberStatusOfRecipient field should be included in the CDR (only applies when PBC is in use).	Cleared
Prepaid Result Code	Proprietary field that controls whether the prepaidResultCode field should be included in the CDR (only applies when PBC is in use with the Diameter protocol).	Cleared
Prepaid Billing State	Proprietary field that controls whether the prepaidBillingState field should be included in the CDR (only applies when PBC is in use).	Cleared
Prepaid Billing State Of Recipient	Proprietary field that controls whether the prepaidBillingStateOfRecipient field should be included in the CDR (only applies when PBC is in use).	Cleared
Inc. Smsc Presentation Address	Proprietary field that controls whether the smscPresentationAddress field should be	Cleared

Field	Description	Default
	included in the CDR (only applies to the MT-MT routing path).	
Inc. Smsc Presentation Address Gsm	Proprietary field that controls whether the <code>smscPresentationAddressGSM</code> field should be included in the CDR (only applies to the MT-MT routing path), formatted according to TS 3GPP 23.040.	Cleared
Inc. Orgl Orig Address	Controls whether the <code>orglOrigAddress</code> field should be included in the CDR.	Selected
Inc. Orgl Orig Address Gsm	Controls whether the <code>orglOrigAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected
Inc. Orgl Recip Address	Controls whether the <code>orglRecipAddress</code> field should be included in the CDR.	Selected
Inc. Orgl Recip Address Gsm	Controls whether the <code>orglRecipAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected
Inc. Orgl Notif Address	Controls whether the <code>orglNotifAddress</code> field should be included in the CDR.	Selected
Inc. Orgl Notif Address Gsm	Controls whether the <code>orglNotifAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected
Inc. External Attributes	Proprietary field that controls whether the <code>externalAttributes</code> field should be included in the CDR (only applies when an ECI application has set or reset attributes in the response).	Cleared
Inc. Cimd Priority	Proprietary field that controls whether the <code>cimdPriority</code> field should be included in the CDR (only applies to AO messages submitted by a CIMD application).	Cleared
Inc. Cimd Service Description	Proprietary field that controls whether the <code>cimdPriority</code> field should be included in the CDR (only applies to AO messages submitted by a CIMD application).	Cleared
Inc. Cimd Tariff Class	Proprietary field that controls whether the <code>cimdTariffClass</code> field should be included in the CDR (only applies to AO messages submitted by a CIMD application).	Cleared
Inc. Orig Address	Controls whether the <code>origAddress</code> field should be included in the CDR.	Selected
Inc. Orig Address Gsm	Controls whether the <code>origAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected

Field	Description	Default
Inc. Recip Address	Controls whether the <code>recipAddress</code> field should be included in the CDR.	Selected
Inc. Recip Address Gsm	Controls whether the <code>recipAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected
Inc. Submit Date	Controls whether the <code>recipDate</code> field should be included in the CDR.	Cleared
Inc. Submit Time	Controls whether the <code>recipTime</code> field should be included in the CDR.	Cleared
Inc. Status	Controls whether the <code>status</code> field should be included in the CDR.	Selected
Inc. Termin Date	Controls whether the <code>terminDate</code> field should be included in the CDR.	Selected
Inc. Termin Time	Controls whether the <code>terminTime</code> field should be included in the CDR.	Selected
Inc. Length Of Message	Controls whether the <code>lengthOfMessage</code> field should be included in the CDR.	Selected
Inc. Prio Indicator	Controls whether the <code>prioIndicator</code> field should be included in the CDR.	Selected
Inc. Validity Period	Controls whether the <code>validityPeriod</code> field should be included in the CDR.	Cleared
Inc. Defer Indicator	Controls whether the <code>deferIndicator</code> field should be included in the CDR.	Cleared
Inc. Defer Period	Controls whether the <code>deferPeriod</code> field should be included in the CDR.	Cleared
Inc. Notif Indicator	Controls whether the <code>notifIndicator</code> field should be included in the CDR.	Selected
Inc. Notif Address	Controls whether the <code>notifAddress</code> field should be included in the CDR.	Selected
Inc. Notif Address Gsm	Controls whether the <code>notifAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected
Inc. Virtual SMSC Id	Controls whether the <code>vsmcId</code> field should be included in the CDR.	Selected
Inc. Virtual SMSC Type	Controls whether the <code>vsmcType</code> field should be included in the CDR.	Selected
Inc. Dgti Address	Controls whether the <code>dgtiAddress</code> field should be included in the CDR.	Cleared

Field	Description	Default
Inc. Dgti Address Gsm	Controls whether the <code>dgtiAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Cleared
Inc. Dest Point Code	Controls whether the <code>destPointCode</code> field should be included in the CDR.	Cleared
Inc. Ogti Address	Controls whether the <code>ogtiAddress</code> field should be included in the CDR.	Selected
Inc. Ogti Address Gsm	Controls whether the <code>ogtiAddressGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Selected
Inc. Orig Point Code	Controls whether the <code>origPointCode</code> field should be included in the CDR.	Selected
Inc. Orgl Submit Date	Controls whether the <code>orglSubmitDate</code> field should be included in the CDR.	Selected
Inc. Orgl Submit Time	Controls whether the <code>orglSubmitTime</code> field should be included in the CDR.	Selected
Inc. Transparent Pid	Controls whether the <code>transparentPid</code> field should be included in the CDR.	Selected
Inc. Mesg Reply Path	Controls whether the <code>mesgReplyPath</code> field should be included in the CDR.	Selected
Inc. Intl Mobile Sub Id	Controls whether the <code>intlMobileSubId</code> field should be included in the CDR.	Cleared
Inc. Calling Line Id	Controls whether the <code>callingLineId</code> field should be included in the CDR.	Cleared
Inc. Calling Line Id Gsm	Controls whether the <code>callingLineIdGSM</code> field should be included in the CDR, formatted according to TS 3GPP 23.040.	Cleared
Inc. Consolidation	Controls whether the <code>consolidation</code> field should be included in the CDR.	Selected
Inc. Port Number	Controls whether the <code>portNumber</code> field should be included in the CDR.	Selected
Inc. Aser	Controls whether the <code>aser</code> field should be included in the CDR.	Cleared
Inc. Mser	Controls whether the <code>mser</code> field should be included in the CDR.	Cleared
Inc. Nser	Controls whether the <code>nser</code> field should be included in the CDR.	Cleared
Inc. Xser	Controls whether the <code>xser</code> field should be included in the CDR.	Cleared

Field	Description	Default
Inc. XS Message Type	Proprietary field that controls whether the <code>xsMessageType</code> field should be included in the CDR.	Cleared
Inc. Orig Intl Mobile Sub Id	Controls whether the <code>origIntlMobileSubId</code> field should be included in the CDR.	Selected
Inc. XS Tie Billing Id	Proprietary field that controls whether the <code>xsTieBillingId</code> field should be included in the CDR (only applies when XS-TIE is in use).	Cleared
Inc. Furnish Charging Info	Controls whether the Camel-specific <code>furnishChargingInfo</code> field should be included in the CDR.	Cleared
Inc. Bill Id	Controls whether the <code>billId</code> field should be included in the CDR.	Cleared
Inc. Recipient RN	Proprietary field that controls whether the <code>RecipientRoutingNumber</code> field should be included in the CDR.	Cleared
Inc. Pp Pser	Controls whether the <code>ppPser</code> field should be included in the CDR.	Cleared
Inc. Cm Reference Nr	Controls whether the <code>cmReferenceNr</code> field should be included in the CDR.	Cleared
Inc. Current Segment	Controls whether the <code>currentSegment</code> field should be included in the CDR.	Cleared
Inc. Segments Total	Controls whether the <code>segmentsTotal</code> field should be included in the CDR.	Cleared
Inc. Lang	Controls whether the <code>lang</code> field should be included in the CDR.	Cleared
Inc. Sme Reference	Controls whether the <code>smeReference</code> field should be included in the CDR.	Cleared
Inc. SMS Content Dcs	Controls whether the <code>smsContentDcs</code> field should be included in the CDR.	Cleared
Inc. SMS Contents	<p>Controls whether the <code>smsContents</code> field should be included in the CDR.</p> <p>Note: In order to display the content correctly, the following points must be considered:</p> <ol style="list-style-type: none"> 1. "Inc. SMS Content Dcs" must also be selected. 2. "License option <code>licTpfLoggingTransparentUserDataLevel.0</code>" must be set to 0. <p>Note: If the encryption feature is enabled and applied for this profile, the user data will be encrypted. In order</p>	Cleared

Field	Description	Default
	to display the encrypted content, the following points must be considered: <ol style="list-style-type: none"> 1. "Encrypt User Data" must also be selected. 2. "License option licGenEncryptUserData.0" must be set to true. 3. Lang and SMS Content fields should be included. 	
Inc. Message Reference	Controls whether the messageReference field should be included in the CDR.	Cleared
Inc. Originator Lasn	Controls whether the origLASN field should be included in the CDR.	Cleared
Inc. Recipient Lasn	Controls whether the recipLASN field should be included in the CDR.	Cleared
Inc. Orig Msg Id	Controls whether the origMsgID field should be included in the CDR.	Cleared
Inc. Service Type	Controls whether the serviceType field should be included in the CDR.	Cleared
Inc. Untransl Orig Address	Controls whether the untranslOrigAddress field should be included in the CDR.	Cleared
Inc. Untransl Orig Address Gsm	Controls whether the untranslOrigAddressGSM field should be included in the CDR.	Cleared
Inc. Untransl Recip Address	Controls whether the untranslRecipAddress field should be included in the CDR.	Cleared
Inc. Untransl Recip Address Gsm	Controls whether the untranslRecipAddressGSM field should be included in the CDR.	Cleared
Inc. Tp Dcs	Controls whether the tpDCS field should be included in the CDR.	Cleared
Inc. Generic Urgency Level	Controls whether the genericUrgencyLevel field should be included in the CDR.	Cleared
Address Information Includes Msisdn Utf8	Controls whether the FCDR fields of the type 'address information' contain a subordinate msisdnuTF8 field or not.	Cleared
Inc. Ss8 Last Failure Reason	Controls whether the ss8LastFailureReason field should be included in the CDR. Note: This field is a proprietary field defined by NewNet.	Cleared
Inc. Delivery Attempts	Controls whether the deliveryAttempts field should be included in the CDR.	Cleared

Field	Description	Default
Inc. Originator SSI	Controls whether the <code>originatorSsi</code> field should be included in the CDR.	Cleared
Inc. Recipient SSI	Controls whether the <code>recipientSsi</code> field should be included in the CDR.	Cleared
Inc. Signature Present	Controls whether the <code>signaturePresent</code> field should be included in the CDR.	Cleared
Inc. Originator User-Equipment PANI	Controls whether the Originator User-Equipment P-Access-Network-Info header field (<code>originatorPaniUE</code>) should be included in the CDR. Note: It is applicable only for IPSM-GW Transport Level Interworking.	Cleared
Inc. Originator Network Provided PANI	Controls whether the Originator Network-Provided P-Access-Network-Info header field (<code>originatorPaniNP</code>) should be included in the CDR. Note: It is applicable only for IPSM-GW Transport Level Interworking.	Cleared
Inc. Originator PCNI	Controls whether the Originator P-Cellular-Network-Info header field (<code>originatorPcni</code>) should be included in the CDR. Note: It is applicable only for IPSM-GW Transport Level Interworking.	Cleared
Inc. Recipient Network-Provided PANI	Controls whether the Recipient Network-provided P-Access-Network-Info header field (<code>recipientPaniNP</code>) should be included in the CDR. Note: It is applicable only for IPSM-GW Transport Level Interworking.	Cleared

11.3.1.2.2 Nokia Call Detail Record (NCDR)

You can customise the following properties for Nokia call detail records (NCDRs).

Property	Description	Default
Format Version	File format version to use to create NCDRs	sc5b-cd3
Inc. Format Version	Controls whether to include the file format version in the header of CDR blocks	Selected
Close Empty File	Controls whether empty CDR files (that is, files that only contain a header and trailer) should be closed (this occurs when the max file duration expires with no traffic)	Selected

Property	Description	Default
Use Gmt Timestamp	Controls whether the timestamp in the CDR records will be in GMT time (otherwise, they will be in local time)	Cleared
Min Tariff Class	Minimum threshold for the tariff class; only tariff classes greater than or equal to this value will be included in the CDR recorded	0
Default Tariff Class	Default tariff class to use for CDR records	1
Fallback Tariff Class	Tariff class to use for messages that are delivered through the fallback leg of the routing path	0
Default Service Description	Default service description to use when creating CDR records	1
Record Type Submit *	Value to place in the record_type field for Submit events (when 0, the event is not included)	1
Record Type Deliver *	Value to place in the record_type field for Deliver events (when 0, the event is not included)	2
Record Type Receive *	Value to place in the record_type field for Receive events (when 0, the event is not included)	3
Record Type Deleted *	Value to place in the record_type field for Deleted events (when 0, the event is not included)	4
Record Type Status 1 *	Value to place in the record_type field for Status1 events (when 0, the event is not included)	7
Record Type Status 2 *	Value to place in the record_type field for Status2 events (when 0, the event is not included)	8
Record Type Expired *	Value to place in the record_type field for Expired events (when 0, the event is not included)	9

* Ensure that each of these properties has a unique value.

Note: Nokia CDR billing profile supports the creation of notification CDR for the status report only. Thus, no NCDR will be created for the AT Notification.

11.3.1.2.3 Ericsson Call Detail Record (ECDR)

You can customise the following properties for Ericsson call detail records (ECDRs).

Note: Some of these fields contain values which the RTR cannot compute (for example, location information or IMEI). The values of these fields can be specified by the operator and are present to make integration with billing systems that require these fields possible.

Property	Description	Default
Use Blocks	Indicator specifying whether or not to use block CDRs. Blocking support is only implemented for the Ericsson CDR format.	false

Property	Description	Default
	<p>Normally, CDRs are emitted into the CDR file, one after the other. With blocking enabled CDRs are written to the CDR file one after the other in blocks, where only complete CDRs are fitted in a block. No CDR is permitted to cross a block boundary (specified by Block Size).</p> <p>If a CDR does not fit a block, the rest of the block is padded with zero byte padding at the end, including the final block. As a result, no matter what maximum block size is specified, you always get a file size which is a positive integer multiple of the block size.</p>	
Block Size	Specifies the block size in the range of 512 to 65535 bytes. Only applicable when Use Blocks is set to true.	2048 bytes
Record Type	<p>Which Ericsson CDR record type to use:</p> <ul style="list-style-type: none"> • msOriginatingSmsInMsc • msOriginatingSmsInSmsIwMsc • msTerminatingSmsInMsc • msTerminatingSmsInSmsGmsc <p>A record type represents a selection of the available ECDR fields. Refer to ECDR Record Type Mapping for a mapping of each ECDR field to the applicable record type.</p>	msOriginatingSmsInSmsIwMsc
Tac Tsc	Value to place in the TSC subfield within the TAC field	3
Tac Tos	Value to place in the TOS subfield within the TAC field	2
Tac Toi	Value to place in the TOI subfield within the TAC field	9
Type Of Calling Subscriber	Value to use for the TypeOfCallingSubscriber field	1
Charged Party	<p>Value to use for the ChargedParty field:</p> <ul style="list-style-type: none"> • chargingOfCallingSubscriber • chargingOfCalledSubscriber • noCharging 	chargingOfCallingSubscriber
Origin For Charging	Value to use for the originOfCharging field	0
Exchange Identity	Exchange Identity	MSC

Property	Description	Default
Incoming Route	Value to use for the <code>incomingRoute</code> field	ROUTE
Outgoing Route	Value to use for the <code>outgoingRoute</code> field	ROUTE
Gsm Tele Service Code	Value to use for the <code>gsmTeleServiceCode</code> field: <ul style="list-style-type: none"> • <code>allSms</code> • <code>mtSms</code> • <code>moSms</code> 	<code>moSms</code>
Inc. Tac	Controls whether to include the TAC field in the CDR	Selected
Inc. Call Identification Number	Controls whether to include the <code>callIdentificationNumber</code> field in the CDR	Selected
Inc. Record Sequence Number	Controls whether to include the <code>recordSequenceNumber</code> field in the CDR	Selected
Inc. Date For Start Of Charge	Controls whether to include the <code>dateForStartOfCharge</code> field in the CDR	Selected
Inc. Time For Start Of Charge	Controls whether to include the <code>timeForStartOfCharge</code> field in the CDR	Selected
Inc. Charged Party	Controls whether to include the <code>chargedParty</code> field in the CDR	Selected
Inc. Exchange Identity	Controls whether to include the <code>exchangeIdentity</code> field in the CDR	Selected
Inc. Msc Identification	Controls whether to include the <code>mscIdentification</code> field in the CDR	Selected
Inc. Gsm Tele Service Code	Controls whether to include the <code>gsmTeleServiceCode</code> field in the CDR	Selected
Inc. Service Centre Address	Controls whether to include the <code>serviceCentreAddress</code> field in the CDR	Selected
Inc. Msc Number	Controls whether to include the <code>mscNumber</code> field in the CDR	Selected
Inc. Called Party Number	Controls whether to include the <code>calledPartyNumber</code> field in the CDR	Selected
Inc. Called Subscriber Imsi	Controls whether to include the <code>calledSubscriberImsi</code> field in the CDR	Selected
Inc. Incoming Route	Controls whether to include the <code>incomingRoute</code> field in the CDR	Selected

Property	Description	Default
Inc. Outgoing Route	Controls whether to include the <code>OutgoingRoute</code> field in the CDR	Selected
Inc. Origin For Charging	Controls whether to include the <code>OriginForCharging</code> field in the CDR	Selected
Inc. Type Of Calling Subscriber	Controls whether to include the <code>TypeOfCallingSubscriber</code> field in the CDR	Selected
Inc. Calling Party Number	Controls whether to include the <code>CallingPartyNumber</code> in the CDR	Selected
Inc. Calling Subscriber Imsi	Controls whether to include the <code>CallingSubscriberImsi</code> in the CDR	Selected
Inc. Number Of Short Messages	Controls whether to include the <code>NumberOfShortMessages</code> field in the CDR	Selected
Inc. Message Type Indicator	Controls whether to include the <code>MessageTypeIndicator</code> field in the CDR	Cleared
Inc. Originating Address	Controls whether to include the <code>OriginatingAddress</code> field in the CDR	Cleared
Inc. Destination Address	Controls whether to include the <code>DestinationAddress</code> field in the CDR	Cleared
Inc. Message Reference	Controls whether to include the <code>MessageReference</code> field in the CDR	Cleared
Inc. Called Subscriber IMEI	Controls whether to include the <code>CalledSubscriberIMEI</code> field in the CDR	Cleared
Inc. Called Subscriber IMEISV	Controls whether to include the <code>CalledSubscriberIMEISV</code> field in the CDR	Cleared
Called Subscriber IMEI TAC	This field specifies the Type Allocation Code that will be used for the <code>CalledSubscriberIMEI</code> and <code>CalledSubscriberIMEISV</code> fields	00000000
Called Subscriber IMEI SNR	This field specifies the Serial Number that will be used for the <code>CalledSubscriberIMEI</code> and <code>CalledSubscriberIMEISV</code> fields	000000
Called Subscriber IMEI SVN	This field specifies the Software Version Number that will be used for the <code>CalledSubscriberIMEISV</code> field	00
Inc. Calling Subscriber IMEI	Controls whether to include the <code>CallingSubscriberIMEI</code> field in the CDR	Cleared
Inc. Calling Subscriber IMEISV	Controls whether to include the <code>CallingSubscriberIMEISV</code> field in the CDR.	Cleared

Property	Description	Default
Calling Subscriber IMEI TAC	This field specifies the Type Allocation Code that will be used for the <code>CallingSubscriberIMEI</code> and <code>CallingSubscriberIMEISV</code> fields	00000000
Calling Subscriber IMEI SNR	This field specifies the Serial Number that will be used for the <code>CallingSubscriberIMEI</code> and <code>CallingSubscriberIMEISV</code> fields	000000
Calling Subscriber IMEI SVN	This field specifies the Software Version Number that will be used for the <code>CallingSubscriberIMEISV</code> field	00
Inc. Output Type	Controls whether to include the <code>OutputType</code> field in the CDR	false
Output Type	Specifies the value of <code>OutputType</code> field. Only applicable when Inc. Output Type is set to true. Valid values are: <ul style="list-style-type: none"> noOutput iCIOutputForCallingSubscriber iCIOutputForCalledSubscriber iCIOutputForCallingAndCalledSubscribers tTOutputOnly tTAndICIForCallingSubscriber tTAndICIForCalledSubscriber tTAndICIForCallingAndCalledSubscribers 	noOutput
Inc. Switch Identity	Controls whether to include the <code>SwitchIdentity</code> field in the CDR	false
Switch Identity	Specifies the value of <code>SwitchIdentity</code> field. Only applicable when Inc. Switch Identity is set to true. This field is present to make integration with billing systems that require this field possible. Valid values are 0 through 65535.	0
Inc. Frequency Band Supported	Controls whether to include the <code>FrequencyBandSupported</code> field in the CDR	false
Frequency Band Supported	Specifies the value of <code>FrequencyBandSupported</code> field. Only applicable when Inc. Frequency Band Supported is set to true. Valid values are: <ul style="list-style-type: none"> none (all bits set to 0) pgsm egsm pgsm-egsm 	none

Property	Description	Default
	<ul style="list-style-type: none"> gsm1800 gsm1800-pgsm gsm1800-pgsm-egsm 	
Inc. First Called Location Information	Controls whether to include the <code>CalledLocationInformation</code> field in the CDR	false
Mobile Country Code	This field specifies the Mobile Country Code (MCC) that will be used for the First Called Location Information. Only applicable when Inc. First Called Location Information is set to true.	000
Mobile Network Code	This field specifies the Mobile Network Code (MNC) that will be used for the First Called Location Information. Only applicable when Inc. First Called Location Information is set to true.	000
Location Area Code	This field specifies the Location Area Code (LAC) that will be used for the First Called Location Information. Only applicable when Inc. First Called Location Information is set to true.	0
Service Area Code	This field specifies the Service Area Code (SAC) that will be used for the First Called Location Information. Only applicable when Inc. First Called Location Information is set to true.	0
Inc. Last Called Location Information	Controls whether to include the <code>LastCalledLocationInformation</code> field in the CDR	false
Mobile Country Code	This field specifies the Mobile Country Code (MCC) that will be used for the Last Called Location Information. Only applicable when Inc. Last Called Location Information is set to true.	000
Mobile Network Code	This field specifies the Mobile Network Code (MNC) that will be used for the Last Called Location Information. Only applicable when Inc. Last Called Location Information is set to true.	000
Location Area Code	This field specifies the Location Area Code (LAC) that will be used for the Last Called Location Information. Only applicable when Inc. Last Called Location Information is set to true.	0

Property	Description	Default
Service Area Code	This field specifies the Service Area Code that (SAC) will be used for the Last Called Location Information. Only applicable when Inc. Last Called Location Information is set to true.	0
Inc. First Calling Location Information	Controls whether to include the <code>FirstCallingLocationInformation</code> field in the CDR	false
Mobile Country Code	This field specifies the Mobile Country Code (MCC) that will be used for the First Calling Location Information. Only applicable when Inc. First Calling Location Information is set to true.	000
Mobile Network Code	This field specifies the Mobile Network Code (MNC) that will be used for the First Calling Location Information. Only applicable when Inc. First Calling Location Information is set to true.	000
Location Area Code	This field specifies the Location Area Code (LAC) that will be used for the First Calling Location Information. Only applicable when Inc. First Calling Location Information is set to true.	0
Service Area Code	This field specifies the Service Area Code (SAC) that will be used for the First Calling Location Information. Only applicable when Inc. First Calling Location Information is set to true.	0
Write Composite CDR	Indicator specifying whether not to emit Composite CDRs	false
Composite CDR Start Tag	<p>Specifies the value of the Composite CDR start tag value. Valid values are 0 through 30. Only applicable when Write Composite CDR is set to true.</p> <p>Composite CDRs are part of the Ericsson CDR specification. ECDRs can be output as a single CDR or as several single CDRs in sequence. Several single CDRs in sequence are called a Composite CDR.</p> <p>What this means in practice is that there is a two byte header, where the second byte is specified by Composite CDR Start Tag, and a two zero byte footer in the CDR file. Inside the header and footer, the CDRs are back to back single CDRs.</p>	1

Property	Description	Default
	Note: When both blocking and composite are on (both Use Blocks and Write Composite CDR are set to true), the Composite CDR will start with the two byte Composite CDR header, the content will be block CDRs, but the final two Composite CDR zero bytes will not be added.	

11.3.1.2.3.1 ECDR Record Type Mapping

The table provides a mapping of the ECDR fields to the ECDR record types.

"X" indicates if a field is included in the record type.

ECDR Field	ECDR Record Types			
	msOriginating SmsInMsc	msOriginating SmsInSmsIwMsc	msTerminating SmsInMsc	msTerminating SmsInSmsGmsc
calledPartyNumber			X	X
calledSubscriberIMEI			X	
calledSubscriberIMEISV			X	
calledSubscriberIMSI			X	X
callIdentificationNumber	X	X	X	X
callingPartyNumber	X	X		
callingSubscriberIMEI	X			
callingSubscriberIMEISV	X			
callingSubscriberIMSI	X			
chargedParty	X	X	X	X
dateForStartOfCharge	X	X	X	X
destinationAddress	X			
exchangeIdentity	X	X	X	X
firstCalledLocationInformation			X	
firstCallingLocationInformation	X			
frequencyBandSupported	X		X	
gsmTeleServiceCode	X	X	X	X
incomingRoute	X			
lastCalledLocationInformation			X	
messageReference	X			
messageTypeIndicator	X		X	

ECDR Field	ECDR Record Types			
	msOriginating SmsInMsc	msOriginating SmsInSmsIwMsc	msTerminating SmsInMsc	msTerminating SmsInSmsGmsc
mscIdentification	X	X	X	X
mscNumber				X
numberOfShortMessages			X	X
originatingAddress			X	
originForCharging	X		X	
outgoingRoute			X	
outputType	X	X	X	X
recordSequenceNumber	X	X	X	X
serviceCentreAddress	X	X	X	X
switchIdentity	X	X	X	X
Tac	X	X	X	X
timeForStartOfCharge	X	X	X	X
typeOfCallingSubscriber	X			

11.3.1.2.4 Comverse Call Detail Record (CCDR)

You can customize the following properties for Comverse call detail records (CCDRs).

Property	Description	Default
Inc. saOptionsIntN	Controls whether to include the saOptionsIntN field.	Selected
Inc. Prepaid Indicator	Controls whether to include the extended field containing the prepaid indicator (saOptionsCharN) in the CDR	Cleared
Inc. Diameter Details	Controls whether to include the extended field containing Diameter billing details in the CDR	Cleared
Default SM Class	Specifies the value to be used in the Comverse CDR sm_class field, unless specified by another configuration item. Valid value is one ASCII character.	M
AT SM Class	Specifies the value to be used in the Comverse CDR sm_class field for an application-terminated (AT) message. Valid value is one ASCII character.	M
Notification SM Class	Specifies the value to be used in the sm_class field of Comverse notification CDRs. Valid value is one ASCII character.	N
Alphanumeric Orig Allowed	Indicator specifying whether an alphanumeric originator address is allowed to be used in Comverse CDRs or not.	Cleared

Note: In addition to the above properties, there is a semi-static configuration parameter `includeconcatenatedmsginfoincdr` that determines whether certain optional fields related to concatenated message segments should be included in the generated CDR records. Refer to [Converse Call Detail Record \(CCDR\)](#) and RTR Operator Manual for more details.

11.3.1.2.5 SS.8 Call Detail Record (SCDR)

You can customise the following properties for SS.8 call detail records (SCDRs).

Property	Description	Default
Inc. SM	Controls whether to include the SM field in the CDR.	Cleared
Inc. Orig. IMSI	Controls whether to include the Originator IMSI field in the CDR; note that this field is relevant only for MO messages.	Cleared
Inc. Orig. MSC GT Type and Addr.	Controls whether to include the Originator MSC GT address type and Originator MSC GT address fields in the CDR; note that this field is relevant only for MO messages.	Cleared
Inc. Dest. MSC Addr.	Controls whether to include the Destination MSC Address field in the CDR; note that this field is relevant only for MT messages.	Cleared
Sequence Number	Current record sequence number for SCDRs (this number is incremented for each CDR that is written and is persistent); you should only change this number while the device is active.	0

Figure 28: MGR GUI Snapshot for SCDR Billing Profile, with Default Configuration

11.3.1.2.6 Logica Call Detail Record (LCDR)

You can customise the Logica call detail record (LCDR) format in the **LCDR Custom Format** field. The field contains a sequence of decimal numbers (each preceded by @) that represent certain CDR fields. For example:

@6@20@15@13

Figure 29: LCDR Custom Format

11.3.1.2.6.1 Formatting Field Value Appearance

You can adjust the appearance of a field value by using C printf-style formatting.

For example:

```
@6$%-20s@20$%03d@15$%dC@13$%12.12s
```

This format string will ensure that the LCDR output contains fields 6, 20, 15 and 13, in the following format:

Field	Type	Appearance	Space Used
6	String	Left-aligned	20 characters
20	Integer	Padded with zeroes on the left	3 characters
15	Integer	Has the character C after it	
13	String	Will always use the space of 12 characters, regardless of the size of the original variable	12 characters

11.3.1.2.6.2 UTF-8 Message Text Fields

Because the LCDR UTF-8 message text field (@206) cannot be parsed if its length is unknown, the UTF-8 message text length field (@205) must appear to the left of field @206 in the custom format string. If it does not, field @206 will contain an empty string.

For privacy reasons, the content of field @206 is subject to the Logging Transparent User Data Level (LIC_FWL_LOGGING_TUDL) license. Refer to the RTR Operator Manual for more information about licenses.

11.3.1.2.7 CCDR 3G Format (CCDRG)

You can customize the CCDR 3G Format (CCDRG) format with the following fields:

File Format:	▼	CCDR 3G Format	▼
Version:	▶	1	
Priority:	▶	Non Priority	▼
Charging ID:	▶	Charge to Sender	▼
Billing Mode:	▶	Bill to Store and Forward	▼

Figure 30: CCDRG File Format

Parameter	Description	Default
Version	This field defines the 3G CDR version, which will be used to fill the CDR Header Information. The valid range for this field is 1 to 999.	1
Priority	This field defines the 3G CDR priority, which will be used while creating the CDR for MO and MT Traffic. Valid values are: <ul style="list-style-type: none"> • Bulk • Low • Medium • High 	Bulk

Parameter	Description	Default
Charging ID	This field defines the 3G CDR Charging ID field, which will be used to fill the CDR charging ID field. Values are in decimals.	Charge to Sender
Billing Mode	This field defines the 3G CDR Billing Mode, which will be used to fill the CDR Billing Mode field.	Bill to Store and Forward

11.3.2 Configuring Billing Properties

After you create a billing profile, you can set it to be the default billing profile for certain types of traffic. By default, no traffic type has a default billing profile assigned to it.

Prerequisites:

- Billing profile

To configure billing properties:

1. In the left navigation bar, select **Billing > Post-paid Billing > Properties**.
The Billing Properties tab appears.
2. From the **Default Profile For MO** list, select a default billing profile for mobile-originating (MO) traffic.
3. From the **Default Profile For MT** list, select a default billing profile for mobile-terminating (MT) traffic.
4. From the **Default Profile For AO** list, select a default billing profile for application-originating (AO) traffic.
5. From the **Default Profile For AT** list, select a default billing profile for application-terminating (AT) traffic.
6. From the **Default Profile For IGM** list, select a default billing profile for internally generated messages (IGM) traffic.
7. From the **Profile For Successful Signature** list, select a billing profile to use for the service CDR generated if the message with the inserted signature was handled successfully (e.g. delivery).
Default is None.
8. From the **Profile For Failed Signature** list, select a billing profile to use for the service CDR generated if the message with the inserted signature has failed (e.g. failure to deliver).
Default is None.
9. From the **Default Profile For MO Spoofing** list, select a billing profile for generating CDRs for messages which are rejected due to MO Spoofing.
10. From the **Default Profile For MT Spoofing** list, select a billing profile for generating CDRs for messages which are rejected due to MT Spoofing.
11. From the **Default Profile For MNP Violation** list, select a billing profile for generating CDRs for messages which are rejected due to MNP Violation.
12. If alphanumeric addresses should be stored in the `origAddressGsm` field of AO messages with alphanumeric addresses, select **Enable Alphanumeric Address** (selected by default).
If you do not select this option, the short number is placed in the `origAddressGsm` field.

13. From the **Enable Alphanumeric Format** list, select a format for alphanumeric addresses in the MSISDN field:
 - empty—MSISDN field is empty (length 0)
 - numeric—Decoded as if the address were numeric (this is the default)
 - alphanumeric—Decoded as a readable string (UTF-8)
14. From the **Intermediate Cache Timeout Status** list, select the status that the RTR will put in the CDR if the SMSC does not send a notification about a message with a record in the Icache before the AMS expires the record:
 - delivered
 - expired (this is the default)
 - deleted
 - replaced
 - submitted
15. Click **Save**.

The MGR saves the changes and closes the tab.

Chapter 12

Logging

Topics:

- [Introduction.....316](#)
- [Message Logging.....316](#)
- [Event Logging.....323](#)
- [Configuring Logging Properties.....326](#)
- [Background Query.....327](#)
- [Flexible User Data Text Search using LGV.....329](#)

12.1 Introduction

When your system includes the Log Processor (LGP), you can use logs of system activity to troubleshoot the network, trace messages associated with customer issues, and control SMS fraud attempts.

12.2 Message Logging

12.2.1 Creating Message Logging Profiles

To create a logging profile:

1. In the left navigation bar, select **Logging** ► **Messages** ► **Profile**.
The Logging Profiles tab appears.
2. Click **Add New**.
A new Logging Profiles tab appears.
3. Enter a unique name for the profile in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the profile in the **Description** box.
5. Select the message type(s) that the profile applies to:
6. In the **Processing Directory** box, enter the location in which to store the log files while they are being created (defaults to `/var/TextPass/log/processing`).
Note: In a multi-instance setup, the processing directory will be shared by all the RTR instances running on a node.
7. In the **Finished Directory** box, enter the location in which to store the log files after they are created (defaults to `/var/TextPass/log/available`).
Note: In a multi-instance setup, the finished directory will be shared by all the RTR instances running on a node.
8. In the **Copy 1 of Finished Directory** through **Copy 9 of Finished Directory** boxes, enter directories in which to create hard links to the files in the finished directory (by default, there are no copies of the finished directory).
Note: The finished directory and all finished directory copies must be on the same disk partition as the processing directory.
9. In the **Filename Template** box, enter the template to use to name the log files (defaults to `log_%h_%U_%Y%m%d_%H%M%S_%3.dat`).
Important: If multi-instances of RTR are running on the same node, then it is important to include `%U` escape sequence, which will be translated to `UID` (operating system user identifier). This ensures that multiple instances of RTR do not try to create files with identical names.
10. In the **Max. File Size** box, enter the maximum size of a log file in bytes (defaults to 1048576 bytes, which is 1 MB). The range is 1024 bytes (1 KB) to 1073741824 bytes (1 GB).

11. In the **Max. File Duration** box, enter the maximum duration of a log file in seconds (defaults to 3600 seconds, which is 1 hour). The range is 1 second to 2,678,400 seconds (1 month).
12. In the **Max. File Records** box, enter the maximum number of records to allow in a log file (defaults to 10000 records). The range is 1 record to 10,000,000 records.
13. Select the file format from the **File Format** list:
 - ASN.1 Extended
 - ANS.1 Extended with country and network info (default)
14. In the **Starting Sequence Number** box, enter the number with which to start the log file numbering sequence (defaults to 0).
15. From the **Suspect/Trusted Messages** list, select the type of messages to log:
 - Only suspect
 - Only trusted
 - Both suspect and trusted (default)

Suspect/Trusted Messages logging pertains to whether the RTR/FWL considers the message source to be suspect or trusted. Inbound MO messages may come from a suspected or trusted MSC, while inbound SendRoutingInfoForSm operations and MT messages may come from a suspected or trusted SMSC. Refer to the Firewall Guide for more information about suspect and trusted qualifications.

16. From the **Failed/Succeeded Messages** list, select the type of messages to log:
 - Only failed
 - Only succeeded
 - Both failed and succeeded (default)

Failed/Succeeded Messages logging pertains to whether a message was successfully delivered from the Mobile Messaging system to the destination. For outbound MT messages, the destination is an MSC (MS). For outbound AT messages, the destination is an application.

17. From the **Accepted/Rejected Messages** list, select the type of messages to log:
 - Only accepted
 - Only rejected
 - Both accepted and rejected (default)

Accepted/Rejected Messages logging pertains to whether the Mobile Messaging system accepts a message or not. This applies to inbound MO and inbound AO messages only.

18. From the **Legitimate/Violated Messages** list, select the type of messages to log:
 - Only legitimate
 - Only violated
 - Both legitimate and violated (default)

Legitimate/Violated Messages logging pertains to whether a message passes or fails a spoof check. Legitimate messages are messages that passed the spoof check. Violated messages are messages that failed the spoof check.

19. From the **Expired/Deleted Messages** list, select the type of messages to log:
 - Do not log (default)
 - Only expired

- Only deleted
- Both expired and deleted
- Only replaced
- Both expired and replaced
- Both deleted and replaced
- Expired, deleted and replaced

Expired/Deleted Messages logging pertains to the AMS delivery result. Expired messages reached their validity period expiration or their maximum number of delivery attempts. Deleted messages were manually deleted from the AMS by a user or by an application. Replaced messages were replaced in the AMS.

20. From the **Status Report Messages** list, select the type of messages to log:

- Do not log (default)
- Status reports

21. From the **Copied/Forwarded Messages** list, select the type of messages to log:

- Do not log (default)
- Only copied
- Only forwarded
- Both copied and forwarded

22. From the **Transparent User Data Level** list, select the level of user data logging:

- Always
- Protocol Violation
- Never
- Encrypt Always
- Use Global Setting (default)

In the license file, if `Logging Transparent User Data Level` is set to:

- `always` - the MGR will display all the above mentioned options.
- `protocolViolationsOnly` - the MGR will display only the options 'Protocol Violation' and 'Never'.
- `never` - the MGR will display only the option 'Never'.

Note: The MGR will display the option 'Encrypt Always' only if the license "Encrypt User Data" is enabled.

23. Click **Save**.

The MGR creates the logging profile and closes the tab.

24. Activate the profile.

12.2.2 Configuring Message Logging Properties

The message logging properties are used to set a log profile as the default log profile for certain messages or violation types.

Note: Changing the default profile will change the logging for all rules that are configured with this default profile.

Prerequisites:

- Logging profile

To configure logging properties:

1. In the left navigation bar, select **Logging > Messages > Properties**.

The Logging Properties tab appears.

2. Select a logging profile for mobile-originating or IMS-originating traffic from the **MO Messages** list.
3. Select a logging profile for mobile-terminating traffic from the **MT Messages** list.
4. Select a logging profile for application-originating traffic from the **AO Messages** list.
5. Select a logging profile for application-terminating traffic from the **AT Messages** list.
6. Select a logging profile to use in case of a fatal protocol violation in a mobile-originating message from the **MO Violations** list.
7. Select a logging profile to use in case of a fatal protocol violation in a mobile-terminating message from the **MT Violations** list.
8. Select a logging profile to be used for mobile-originating SMS commands from the **MO Commands** list.
9. Select a logging profile to be used for application-originating SMS commands from the **AO Commands** list.
10. Select a logging profile to be used for mobile number portability (MNP) violations of originator (in case of MO message) from the **MNP Violations** list.
11. Click **Save**.

The MGR saves the logging properties and closes the tab.

12.2.3 Configuring Message Log Filters

Prerequisites:

- A Log Processor (LGP) must be installed and configured.

To configure a message log filter:

1. In the left navigation bar, select **Logging > Messages > Filters**.

The Filters tab appears.

2. Click **Add New**.

A new Filters tab appears.


3. Enter a unique name for the filter in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the filter in the **Description** box.
5. From the list on the left, select matching:

- Match all elements
- Match any element

6. Click **Add Element**.

The list of available elements appears.

7. Add an element to the filter by doing one of the following:

- Clicking an element (highlighted in gray)
- Clicking  to expand a list of elements, then clicking an element

8. Select a condition for the element from the **Condition** list:

- Equals
- Does not equal
- Contains
- Does not contain
- Is not set
- Starts with
- Ends with
- Match Flexibly

Note:

1. The “Match flexibly” condition is supported only for the user data fields (“*messagefields_userData*”, “*smsSubmit_smsUserData*”, “*smsDeliver_smsUserData*” and “*userData_normalizedText*”). It is meant for efficient searching of the user data text when the LGP ‘flexible text search’ functionality is licensed and also enabled through the configuration. Refer to [Flexible User Data Text Search using LGV](#) for more details.

2. The field “*userData_normalizedText*” supports only the “Match flexibly” option and none of the other matching conditions listed above.

9. Enter a value in the **Value** box.

10. Optionally add more elements to the filter and set their conditions and values.

Note: To remove an element from the filter, click



next to it.

11. Click **Save**.

The MGR creates the message log filter and closes the tab.

12.2.4 Configuring Message Log View Columns

Prerequisites:

- A Log Processor (LGP) must be installed and configured.



To configure a message log view column:

1. In the left navigation bar, select **Logging > Messages > View Columns**.

The View Columns tab appears.

2. Click **Add New**.

A new View Columns tab appears.



3. Enter a unique name for the view column in the **Name** box.
4. Optionally enter a description of the view column in the **Description** box.
5. Click **Add Element**.
The list of available elements appears.
6. Add an element to the view column by doing one of the following:
 - Clicking an element (highlighted in gray)
 - Clicking  to expand a list of elements, then clicking an element
7. Enter a value in the **Name** box (maximum 32 characters).
Note: This value will act as a display name in the output when a search query is performed.
8. Enter a value in the **Width** box (between 50px and 200px).
9. Optionally add more elements to the view column and set their names and widths.
Note: At most 5 elements can be added.
Note: To remove an element from the view column, click  next to it.
10. Click **Save**.
The MGR creates the message log view column and closes the tab.

12.2.5 Using Message Log Search

Prerequisites:

- A Log Processor (LGP) must be installed and configured
- Message log filter
- Message log column

To search the information in the logs:

1. In the left navigation bar, select **Logging > Messages > Search**.
The Search Messages tab appears.
2. Click  next to the **Start Date** box and select the date and time at which to start the log search.
3. Click  next to the **End Date** box and select the date and time at which to end the log search.
4. In the **Max Results** box, specify a maximum number of log records to return.
5. Select a log filter from the **Filter** list.

Note: A warning message will be shown in the result page if the filter contains the 'userData' field when the encryption license is enabled. This is because a filter with 'userData' field would normally return empty results with encrypted data.

6. Select a view column from the **View Columns** list. The option **Default** can be selected to get a result with the default columns.

Note: There are 5 fixed columns (**ID, Date/Time, Hostname, originator Number, recipient Number**). The dynamic columns will be added after the fixed columns, according to the selected View Column. Although the same information is mentioned correctly in MGR operator manual in section - 12.2.5 (Using Message Log Search) at point no.- 6, which can also be referred for necessary correction in LGP OM.

Note: If user data is included in View Columns and the user data is encrypted while **View Encrypted Data** is false for the user, the user data will be empty in the results.

7. Select the checkbox next to **Execute Query in Background** to perform the search in background.

The dynamic columns in the output columns will be available with the background query.

Note: The background query result-set will be available on **Logging ► Background Query** link. Refer to section [Background Query](#) for more details on background query.

8. Click **Search**.

The MGR searches for records based on the starting time, ending time, and filter, and returns any log records that match (up to the maximum number that you specify).

Note: The maximum size of a request is 20kB. If the size is bigger than 20kB, an error will be returned.

Note: If a decryption error occurred (e.g. reading the key file) while decrypting the UserData, the UserData field will be used to show the error.

9. To export the search results as a comma-separated value (CSV) file that can be opened in programs such as Microsoft Excel and OpenOffice.org Calc, click **Export**.

Note: Message Log Search displays all the matching logs on GUI irrespective of whether the 'File Format' is selected as 'ASN.1 Extended' or 'ASN.1 Extended with country and network info' during the configuration of Log Profile on MGR. For Message Log Search using 'inboundMessageType' as the Filter Element, Filter Value can only be selected as

'trustedMtFwdSmWithCountryAndNetworkInfo'.

For example, add a new filter with unique name (say: messagetype) on Filter Element 'inboundMessageType' with Condition 'equals' and Value 'trustedMtFwdSmWithCountryAndNetworkInfo'.

Log search result for this filter will fetch the records for both "trustedMtFwdSm" and "trustedMtFwdSmWithCountryAndNetworkInfo".

12.3 Event Logging

12.3.1 Creating Event Logging Profiles

To create a logging profile:

1. In the left navigation bar, select **Logging > Events > Profile**.
The Event Logging Profiles tab appears.
2. Click **Add New**.
A new Event Logging Profiles tab appears.
3. Enter a unique name for the profile in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the profile in the **Description** box.
5. In the **Processing Directory** box, enter the location in which to store the log files while they are being created (defaults to `/var/TextPass/log/processing`).

Note: In a multi-instance setup, the processing directory will be shared by all the NMM component instances running on a node.

6. In the **Finished Directory** box, enter the location in which to store the log files after they are created (defaults to `/var/TextPass/log/available`).

Note: In a multi-instance setup, the finished directory will be shared by all the NMM component instances running on a node.

7. In the **Filename Template** box, enter the template to use to name the log files (defaults to `%N_event_%U_%h_%Y%m%d_%H%M%S_%3.dat`).

Important: As multiple components on the same system may share an event logging profile configuration, it is important to include the `%N` escape sequence, which will be translated to the component name. This ensures that multiple components will not try to create files with identical names.

Important: If multi-instances of NMM components are running on the same node, then it is important to include `%U` escape sequence, which will be translated to `UID` (operating system user identifier). This ensures that multiple components will not try to create files with identical names.

8. In the **Max. File Size** box, enter the maximum size of a log file in bytes (defaults to 1,048,576 bytes, which is 1 MB). The range is 1024 bytes (1 KB) to 1,073,741,824 bytes (1 GB).
9. In the **Max. File Duration** box, enter the maximum duration of a log file in seconds (defaults to 3600 seconds, which is 1 hour). The range is 1 second to 2,678,400 seconds (1 month).
10. In the **Max. File Records** box, enter the maximum number of records to allow in a log file (defaults to 10,000 records). The range is 1 record to 10,000,000 records.
11. In the **Starting Sequence Number** box, enter the number with which to start the log file numbering sequence (defaults to 0).

12. Click **Save**.

The MGR creates the logging profile and closes the tab.

13. Activate the profile.

12.3.1.1 Configuring Event Logging Copies

For each event logging profile, you can create a list of directories in which the LGP will save copies of the files in the profile's **Finished Directory**. You can use this functionality to ensure that an automatic backup of completed files exists. The list for each event logging profile can contain up to 10 directories.

Note: The **Finished Directory** and all directories containing copies must be on the same disk partition as the **Processing Directory**.

Prerequisites:

- Event logging profile

To add a directory to an event logging copies list:

1. In the left navigation bar, select **Logging > Events > Profile**.
The Event Logging Profiles tab appears.
2. Click the name of an event logging profile.
3. In the Event Logging Copies section, click **Add New**. A new Event Logging Copies List tab appears.
4. In the **Copy Directory** box, enter a directory in which the LGP should create hard links to the files in the **Finished Directory** (defaults to `/var/TextPass/backup`).
You can only add a directory to the list if the event logging profile is deactivated.
5. From the **Event Log Profile** list, select the profile to use for this copy location (defaults to the profile that you clicked earlier).
6. Click **Save**.
The MGR closes the tab and adds the directory to the Event Logging Copies list.
7. On the event logging profile tab, click **Add New** to add another directory to the list, or click **Save** to save the profile.

12.3.2 Configuring Event Logging Properties

The event logging properties are used to set a specific log profile for certain events.

Prerequisites:

- Event logging profile

To configure event logging properties:

1. In the left navigation bar, select **Logging > Events > Properties**.
The Event Logging Properties tab appears.
2. Select an event logging profile for:

Option	Description
Short Message Events	Events related to the processing of Short Messages, that are used for the Event Log Search within the Customer Care Interface (CCI) component.
Unexpected TCAP Events	Events that are used for unexpected TCAP messages (that is, TCAP messages for which no TCAP dialog exists). All unexpected TCAP End

Option	Description
	and TCAP Continue messages with a <code>ReturnResult</code> message will be logged to this profile when they arrive at the RTR.

3. Click **Save**.

The MGR saves the event logging properties and closes the tab.

12.3.3 Configuring Event Log Filters

Event log filtering is available for unexpected TCAP events, but it is not available for the short message events.

Prerequisites:

- A Log Processor (LGP) must be installed and configured.

To configure an event log filter:

1. In the left navigation bar, select **Logging > Events > Filters**.

The Filters tab appears.

2. Click **Add New**.

A new Filters tab appears.

3. Enter a unique name for the filter in the **Name** box (maximum 31 characters).

4. Optionally enter a description of the filter in the **Description** box.

5. From the list on the left, select matching:

- Match all elements
- Match any element

6. Click **Add Element**.

The list of available elements appears.

7. Add an element to the filter by doing one of the following:

- Clicking an element (highlighted in gray)
- Clicking



to expand a list of elements, then clicking an element

8. Select a condition for the element from the **Condition** list:

- Equals
- Does not equal
- Contains
- Does not contain
- Is not set
- Starts with
- Ends with

9. Enter a value in the **Value** box.

10. Optionally add more elements to the filter and set their conditions and values.

Note: To remove an element from the filter, click



next to it.

11. Click **Save**.

The MGR creates the log filter and closes the tab.

12.3.4 Using Event Log Search

Prerequisites:

- A Log Processor (LGP) must be installed and configured
- Event log filter.
- Message view column

To search the information in the logs:

1. In the left navigation bar, select **Logging > Events > Search**.

The Search Events tab appears.

2. Click



next to the **Start Date** box and select the date and time at which to start the log search.

3. Click



next to the **End Date** box and select the date and time at which to end the log search.

4. In the **Max Results** box, specify a maximum number of log records to return.

5. Select a log filter from the **Filter** list.

6. Select the checkbox next to **Execute Query in Background** to perform the search in background.

Note: The background query result-set will be available on **Logging > Background Query** link. Refer to section [Background Query](#) for more details on background query.

7. Click **Search**.

The MGR searches for records based on the starting time, ending time, and filter, and returns any log records that match (up to the maximum number that you specify).

Note: The maximum size of a request is 20kB. If the size is bigger than 20kB, an error will be returned.

8. To export the search results as a comma-separated value (CSV) file that can be opened in programs such as Microsoft Excel and OpenOffice.org Calc, click **Export**.

12.4 Configuring Logging Properties

To configure logging properties:

1. In the left navigation bar, select **Logging ► Properties**.

The Properties tab appears.

2. In the **Convert To Archive Storage After** field specify the period (in hours) after which the LGP log record tables will be converted to archive storage. The default value is -1 which indicates that no archiving will be performed. The maximum allowed value is 26304 hours (1096 days).
3. In the **Database Archive Schedule** field specify the time when LGP starts converting the log records tables into Archive format or vice-versa (i.e. un-archiving already archived table records). DB archive schedule is written as a comma separated list of hh24mm time schedules. For example 1 AM and 1 PM is 0100,1300. Default value is 0135. Maximum 24 durations can be configured as DB archive schedule.

Note: DB archive schedule must be set to off-peak hours period. Archival/Un-archival procedure can take time and transaction/event files are not loaded during archival/un-archival. Configuring DB archive schedule parameter to peak-hours will impact the performance of LGP loader and LGP query module.

4. In the **Background Query Max Run Time** field specify the maximum run time (in seconds) for a background query. Default value is '36000' (10 Hours). Maximum allowed value is 65535.

12.5 Background Query

When you execute Message or Event search in background then MGR sends the search request to LGP and waits for response in background. During the background search you can perform other tasks on MGR GUI. Background query is not impacted by logout. You can logout of MGR and later re-login to see background query result . You can track the status of background queries using **Logging ► Background Query** link. When the query is completed, the status will be displayed as **completed**. You can click on the completed background query result row to view the result-set or download as CSV. When the background query completes, an indication is displayed on top-right corner of MGR GUI. Indication icon is displayed when you login or refresh MGR page or open a new tab after completion of Background Query.

Prerequisites to perform Background Query:

- A Log Processor (LGP) must be installed and configured
- Message or Event log filter

To search the information in the logs:

1. In the left navigation bar, select **Logging ► Messages ► Search** for message search or select **Logging ► Events ► Search** for event search.

The Search Messages tab appears.

2. Click



next to the Start Date box and select the date and time at which to start the log search.

3. Click



next to the End Date box and select the date and time at which to end the log search.

4. In the Max Results box, specify a maximum number of log records to return.

5. Select a log filter from the Filter list.
6. Select the checkbox next to **Execute Query in Background** to perform the search in background.
7. Select a view column from the **View Columns** list. The option **Default** can be selected to get a result with the default columns.

Note: If the user changes the selected **View Columns** while a search is in-progress, the result for background query will be as per the altered view set.

8. Click Search.
9. An alert message will appear to indicate that the query will be executed in background. Select "OK" to start executing background query.

The MGR searches for records based on the starting time, ending time, and filter, and returns any log records that match (up to the maximum number that you specify).

Note: The maximum size of a request is 20kB. If the size is bigger than 20kB, an error will be returned.

10. You can track the status of background queries (In-progress or completed) using **Logging** ► **Background Query** link.
11. Once background query is completed, there would be indication icon displayed on MGR GUI at right top with Green color. Indication icon is displayed when user logged-in, refresh page or open a new tab after completion of background query.
12. Once query status is changed to **Completed**, you can click on background query row to view the result-set.
13. To export the search results as a comma-separated value (CSV) file that can be opened in programs such as Microsoft Excel and OpenOffice.org Calc, click Export.

Background Query is helpful in performing long searches, searching on LGP Archive records which may take a very long duration.

Note: There are some restrictions on Background Query

1. You are not allowed to delete in-progress query.
2. Only one background query can be in-progress state in a domain.

12.5.1 Background Query Configuration

For Background Query following parameters should be provisioned in `/usr/TextPass/etc/mgr.cnf`:

1. `background_query_dir`: This parameter specifies path where MGR will store Background Query search results. You must ensure that sufficient space is available on disk at this path otherwise Background Query cannot be performed. You can change the path of this directory when MGR is in stopped state. Please ensure that old results are copied to new path otherwise you will not be able to view older results on MGR GUI.

Note: You must ensure that the owner of `background_query_dir` folder is `textpass` and `textpass` user is able to create files in `background_query_dir` folder.

2. `minimum_size_required`: Minimum free disk space required to perform Background Query is set in '`minimum_size_required`'. Default value is '1024 MB'. If the free space available in `background_query_dir` is less than `minimum_size_required`, then background query will not be performed.

3. `max_background_query_records`: Maximum records that can be retrieved by a Background Query. The default value is 65535.

Note: Due to browser and cache memory limitation, it is strongly recommended not to increase the value of this parameter more than 65535. If there can be more than 65535 records, the background query can be split in multiple queries using shorter search ranges.

Sample configuration

```
<logviewer maximum_records="1000" background_query_dir="/var/TextPass/MGR/lgp"
minimum_size_required="1024" max_background_query_records="65535"/>
```

Note: KeepAlive Timer settings must be configured on MGR to detect background query failure due to unexpected issues like remote server restart or network cable failure. Please refer to the section Configure KeepAlive Timer of the Full Element Installation Manual.

12.6 Flexible User Data Text Search using LGV

For the user data fields (`messagefields_userData`, `smsSubmit_smsUserData`, `smsDeliver_smsUserData`), an additional matching condition “Match flexibly” is supported along with the other conditions, as shown below.

The “Match flexibly” option allows efficient and enhanced searching of the user data text by leveraging the MySQL Full Text Search (FTS) capability. Note that this option is supported only if the **Enable Full Text Search** license is enabled and the semi-static configuration parameter `lgpfulltextsearch` is set to “true”.

The screenshot shows a configuration window for a filter element. At the top left, there is a dropdown menu set to 'match all elements'. Below it is a table with three columns: 'Filter Element', 'Condition', and 'Value'. The first row shows 'messageFields_userData' in the 'Filter Element' column, '- SELECT -' in the 'Condition' column, and an empty text box in the 'Value' column. A dropdown menu is open from the 'Condition' cell, listing several options: '- SELECT -', 'equals', 'does not equal', 'contains', 'does not contain', 'is not set', 'starts with', 'ends with', and 'match flexibly'. The 'match flexibly' option is highlighted with a red rectangular box. To the right of the table are three buttons: 'Add Element', 'Save', and 'Cancel'.

Filter Element	Condition	Value
messageFields_userData	- SELECT -	

Figure 31: MessageFields->userData condition options

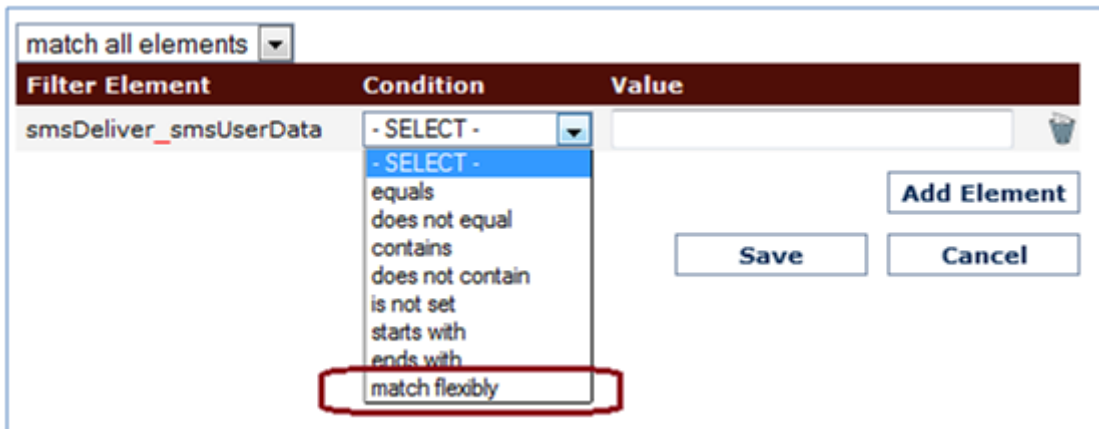


Figure 32: smsDeliver->userData condition options

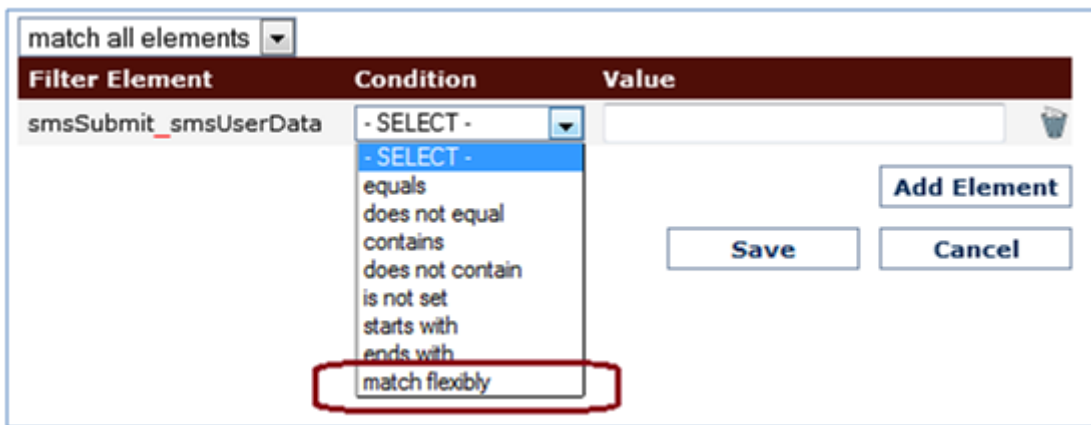


Figure 33: smsSubmit->userData condition options

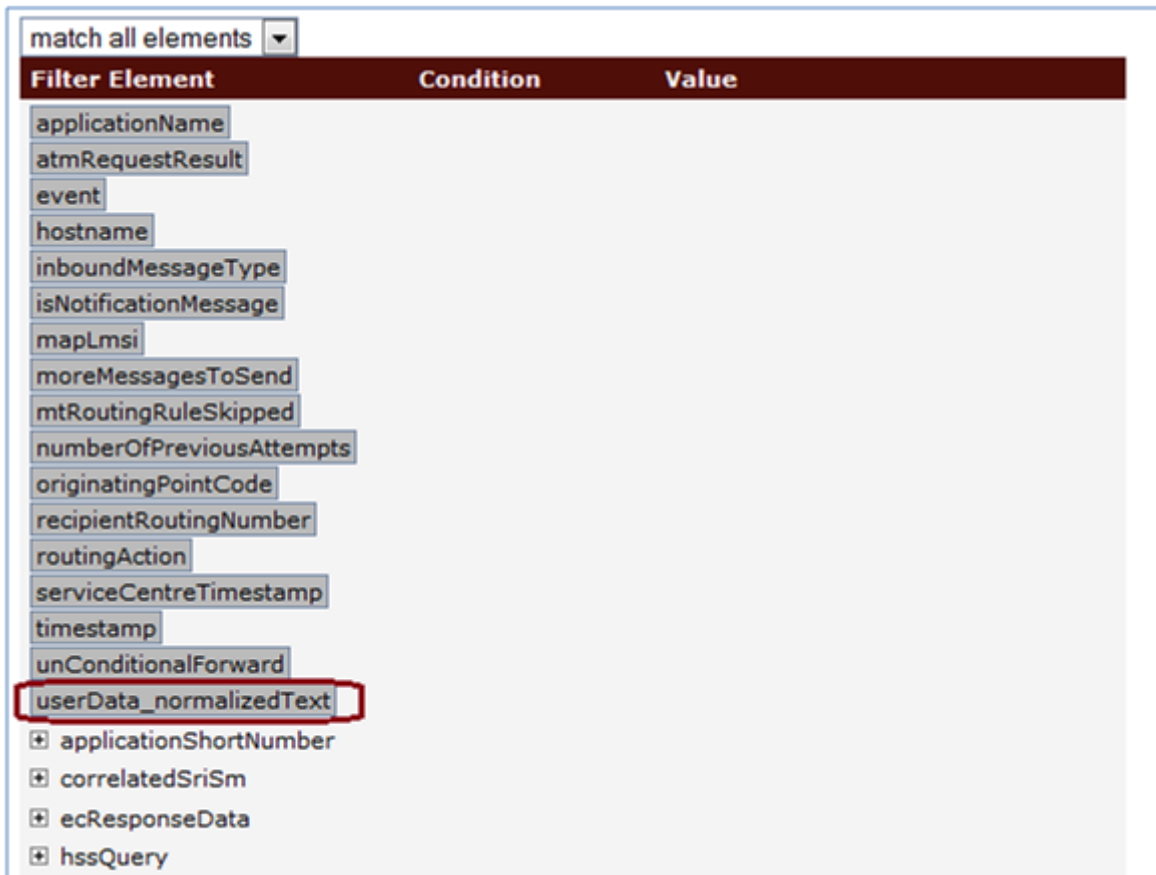


Figure 34: Filter Element *userData_normalizedText* for Message Filters

A new filter element “*userData_normalizedText*” will support only the “Match flexibly” filter condition.

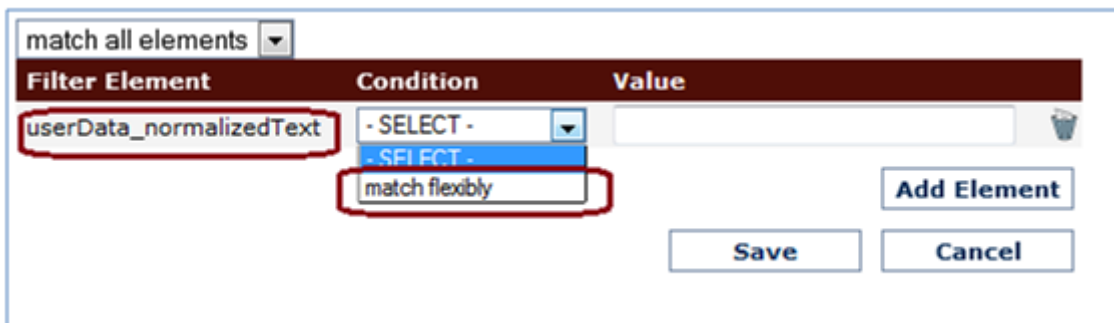


Figure 35: *userData_normalizedText* condition option

Note:

1. If an error message is received from LGP in query response XML then same error message will be displayed on the GUI.
2. In case “Match flexibly” filter criteria query is executed in background and an error message is received from LGP in response XML then same error message will be stored in `lgpBackgroundQueryTable` as error text field.

Chapter 13

SPF Services

Topics:

- *Introduction.....334*
- *User Privileges.....334*
- *Create a Service.....334*
- *Add/Modify Command Aliases.....341*
- *Add/Modify Parameter Aliases.....341*
- *Message Template String Format.....342*

13.1 Introduction

When your system includes a Service Provisioning Framework (SPF), you can create services via the **SPF Services** menu.

SPF Services provides configuration options for, keywords, keyword aliases, commands, command aliases, message template strings, etc., used for SMS based provisioning (refer to SPF Operator Manual for details).

13.2 User Privileges

To perform SPF Services configuration, make sure that the MGR User has the right **SPF Services** User Group privileges assigned. This can be set via **Settings > User Admin > Groups**.

13.3 Create a Service

The services that can be created and provisioned using the SPF are:

- ARP—SMS Auto Reply service provided by XS-ARP
- BWL—SMS Black- and Whitelist service provided by XS-BWL
- CPY—SMS Copy to Phone service provided by XS-CPY
- CTA—SMS Copy to Application service provided by XS-CPY
- DIL—SMS Distribution List service provided by XS-DIL.
- FWD—SMS Forward to a provisioned address provided by XS-FWD
- SIG—SMS Signature service provided by XS-SIG
- NPS—Non-Provisionable Service, which is used for services that can not be self-provisioned using the SPF (such as XS-INT, XS-TIE or third-party services)
- ABL— Auto Blacklist service used by FAF to blacklist the subscriber
- OPT— Opt-In/Opt-Out service that allows the end-user to switch a service ON or OFF
- CTE—SMS Copy to Email service provided by XS-CPY
- FTE—SMS Forward to Email service provided by XS-FWD

A maximum of 32 services can be defined.

Note: For the FWD, BWL, DIL, ARP, SIG, CTE, and FTE service, only one instance can be created.

To create a service:

1. In the left navigation bar, select **SPF Services > SPF Services**.
The SPF Service tab appears.
2. Click **Add New**.
A new SPF Service tab appears.
3. Enter a unique name for the service in the **Name** box (maximum 31 characters).

4. Enter a description for the service in the **Service Description** box (maximum 100 characters). This description is also shown in the Customer Care Interface (CCI).
5. From the **Service Type** list, select the type of service:
 - **Black and Whitelist** (BWL)
 - **Copy to Phone** (CPY)
 - **Distribution List** (DIL)
 - **Forward** (FWD)
 - **Other Service** (NPS)
 - **Copy to Application** (CTA)
 - **Auto Reply** (ARP)
 - **Signature** (SIG)
 - **Auto Blacklist** (ABL)
 - **Opt-In/Opt-Out** (OPT)
 - **Copy to Email** (CTE)
 - **Forward to Email** (FTE)

6. Depending on the chosen **Service Type**, provision the following fields.

If **Service Type** is set to... Then ...

Black and Whitelist From the **Invoking Address** list, select **Recipient**.

Continue at [Step 7](#)

Copy to Phone

1. From the **Invoking Address** list, select to whom a service is to be applied:
 - **Both**—This is both an originator and a recipient service
 - **Originator**—This is an originator service only
 - **Recipient**—This is a recipient service only

2. In the **Max Service Rules** box, enter the maximum number of service rules allowed per copy to phone service, per subscriber. The default is 10. The range is 1-10.

When the maximum is reduced, no service rules will be removed from subscribers exceeding the maximum. These subscribers can only create service rules with conditions again when they have deleted enough service rules so they are below the new maximum again. Editing and deletion is still possible with service rules exceeding the maximum, these service rules also continue to function normally.

Note: The default service rule (no conditions) is not included in the maximum number of service rules count.

3. From the **Originator** list, select the value that should go into the originator field of the copied message:
 - **Original Originator**—The originator of the original message (default)
 - **Original Recipient**—The recipient of the original message

If Service Type is set to... Then ...

4. From the **Use Header** list, select whether to add a header to copied messages. If set to `true`, configure the following:
 - In the **GSM Header** box, enter a header string to be added to GSM 7-bit encoded copied messages (max. 100 characters).
 - In the **UCS2 Header** box, enter a header string to be added to UCS-2 encoded copied messages (max. 50 characters).

Where:

- %a is replaced with the message's original originator address;
- %b is replaced with the message's original recipient address.

Note: These settings will override the header and footer settings specified in the XS-CPY host-specific configuration file.

5. From the **Use Footer** list, select whether to add a footer to copied messages. If set to `true`, configure the following:
 - In the **GSM Footer** box, enter a footer string to be added to GSM 7-bit encoded copied messages (max. 100 characters).
 - In the **UCS2 Footer** box, enter a footer string to be added to UCS-2 encoded copied messages (max. 50 characters).

Where:

- %a is replaced with the message's original originator address;
- %b is replaced with the message's original recipient address.

Note: These settings will override the header and footer settings specified in the XS-CPY host-specific configuration file.

Continue at [Step 7](#)

Distribution List

1. From the **Invoking Address** list, select **Originator**.
2. In the **Max List Number** box, enter the upper bound for list numbers within the Distribution List service. The default is 99. The range is 0-99.

Note: Do not reduce this value after distribution lists have been created. Reducing the value will cause issues if higher-numbered lists exist.
3. In the **Max Number of Lists per Subscriber** box, enter the maximum number of distribution lists allowed for a subscriber. The default is 10. The range is 1-100.
4. In the **Max Number of Addresses per Subscriber** box, enter the maximum number of addresses per distribution list for a subscriber. The default is 50. The range is 1-100.

Continue at [Step 7](#)

Forward

1. From the **Invoking Address** list, select **Recipient**.

If Service Type is set to... Then ...

2. In the **Max Service Rules** box, enter the maximum number of service rules allowed per forward service, per subscriber. The default is 10. The range is 1-10.

When the maximum is reduced, no service rules will be removed from subscribers exceeding the maximum. These subscribers can only create service rules with conditions again when they have deleted enough service rules so they are below the new maximum again. Editing and deletion is still possible with service rules exceeding the maximum, these service rules also continue to function normally.

Note: The default service rule (no conditions) is not included in the maximum number of service rules count.

Continue at [Step 7](#)

Other Service

From the **Invoking Address** list, select to whom a service is to be applied:

- **Both**—This is both an originator and a recipient service
- **Originator**—This is an originator service only
- **Recipient**—This is a recipient service only

Continue at [Step 18](#).

Copy to Application

1. From the **Invoking Address** list, select to whom a service is to be applied:

- **Both**—This is both an originator and a recipient service
- **Originator**—This is an originator service only
- **Recipient**—This is a recipient service only

2. In the **Originator Copy** box, select the application to copy to if an originator copy to application is triggered. Default is None.

If set to None, no requests are triggered for originating traffic.

It is allowed to select the same as **Recipient Copy**, however, per ECI request only one copy to a unique destination will be created.

3. In the **Recipient Copy** box, select the application to copy to if a recipient copy to application is triggered. Default is None.

If set to None, no requests are triggered for recipient traffic.

It is allowed to select the same as **Originator Copy**, however, per ECI request only one copy to a unique destination will be created.

4. In the **Allow Self Provisioning** box, select whether the subscriber can set the service ON or OFF, for example, by using an SMS command or via the Customer Care Interface (CCI). Default value is true.

If Service Type is set to... Then ...

If this field is set to `false` then the CTA service is activated/deactivated by the operator in the service profile + subscriber specific override setting (Continue at [Step 18](#)).

Note: This field can only be changed once. After the first activation this field cannot be changed anymore. Removal of the service is then required if this field needs to be changed.

Continue at [Step 7](#)

Auto Reply

1. From the **Invoking Address** list, select **Recipient**.
2. In the **Max GSM7 Length** box, enter the maximum auto reply text length for GSM 7-bit encoded messages. The default is 160. The range is 0-160.
3. In the **Max UCS2 Length** box, enter the maximum auto reply text length for UCS-2 encoded messages. The default is 70. The range is 0-134.
4. In the **Max Service Rules** box, enter the maximum number of service rules allowed per auto reply service, per subscriber. The default is 10. The range is 1-10.

When the maximum is reduced, no service rules will be removed from subscribers exceeding the maximum. These subscribers can only create service rules with conditions again when they have deleted enough service rules so they are below the new maximum again. Editing and deletion is still possible with service rules exceeding the maximum, these service rules also continue to function normally.

Note: The default service rule (no conditions) is not included in the maximum number of service rules count.

Continue at [Step 7](#)

Signature

1. From the **Invoking Address** list, select **Originator**.
2. In the **Max GSM7 Length** box, enter the maximum signature text length for GSM 7-bit encoded messages. The default is 63. The range is 0-144.
3. In the **Max UCS2 Length** box, enter the maximum signature text length for UCS-2 encoded messages. The default is 63. The range is 0-130.
4. In the **Max Service Rules** box, enter the maximum number of service rules allowed per signature service, per subscriber. The default is 10. The range is 1-10.

When the maximum is reduced, no service rules will be removed from subscribers exceeding the maximum. These subscribers can only create service rules with conditions again when they have deleted enough service rules so they are below the new maximum again. Editing and deletion is still possible with service rules

If Service Type is set to... Then ...

exceeding the maximum, these service rules also continue to function normally.

Note: The default service rule (no conditions) is not included in the maximum number of service rules count.

Continue at [Step 7](#)

Auto Blacklist

1. From the **Invoking Address** list, select to whom a service is to be applied:
 - **Originator** - This is an originator service only.
 - **Recipient** - This is a recipient service only.
2. In the **Profile Id** box, enter the "Profile Id" to use when a new subscriber is blacklisted using this service.

Note: You should make sure that the Profile Id is provisioned in the SPF before using it at the time of Auto Blacklist service creation. SPF Service provisioning will be successful even if Profile Id is not provisioned in the SPF. But SPF will not be able to block a new subscriber using this Auto Blacklist SPF service and trap will be generated by the SPF.

Continue at [Step 18](#)

Opt-In/Opt-Out

1. From the **Invoking Address** list, select to whom a service is to be applied:
 - **Originator** - This is an originator service only.
 - **Recipient** - This is a recipient service only.
2. The "Service Default Value" checkbox indicates the default state of the OPT service. When the checkbox is selected, the subscriber states for that OPT service is set to enabled by default. This means that when a subscriber is added to a profile, the subscriber state for that service will automatically be enabled.

However, this is NOT applicable for the existing subscribers of a profile when the OPT service is added to that profile.

For all such existing subscribers the default state of the OPT service will remain as disabled.

Note: The default state of "Service Default Value" checkbox is un-checked on MGR GUI.

Continue at [Step 7](#)

Copy to Email

From the Invoking Address list, select Recipient.

If Service Type is set to... Then ...

Continue at [Step 7](#)

Forward to Email

From the Invoking Address list, select Recipient.

Continue at [Step 7](#)

7. In the **Keyword** box, enter the unique keyword by which this service is identified in the SMS provisioning requests. For example COPY or BLOCK.
8. In the **Success Message** box, enter the template for sending a confirmation message after a successful provisioning action for this service. The default is %k: %c successful. For details, see the definition of [Message Template String Format](#). This is a fall-back string, in case no command-level strings are found.
9. In the **Failure Message** box, enter the template for sending a reject message when a provisioning action for this service failed. The default is %k: %c unsuccessful. For details, see the definition of [Message Template String Format](#). This is a fall-back string, in case no command-level strings are found.
10. In the **Enabled** box, enter a string used to denote the 'enabled' state of a service as provisioned by the subscriber. The default is ON. This string is used during message template expansion.
11. In the **Disabled** box, enter a string used to denote the 'disabled' state of a service as provisioned by the subscriber. The default is OFF. This string is used during message template expansion.
12. In the **Keyword Alias** box, enter a keyword alias, by which this service is identified in the provisioning requests. For example, CPY or BLK.
13. In the **Success Message Alias** box, enter the template for sending a confirmation message after a successful provisioning action for this service. The default is %k: %c successful. For details, see the definition of [Message Template String Format](#). This is a fall-back string, in case no command-level strings are found.
14. In the **Failure Message Alias** box, enter the template for sending a reject message when a provisioning action for this service failed. The default is %k: %c unsuccessful. For details, see the definition of [Message Template String Format](#). This is a fall-back string, in case no command-level strings are found.
15. In the **Enabled Alias** box, enter a string used to denote the 'enabled' state of a service as provisioned by the subscriber. The default is ON. This string is used during message template expansion.
16. In the **Disabled Alias** box, enter a string used to denote the 'disabled' state of a service as provisioned by the subscriber. The default is OFF. This string is used during message template expansion.
17. The **Available When SSI is Unknown** checkbox, indicates if the corresponding service shall be assumed to be available for any subscriber in case the SSI information is unknown (i.e. was not retrieved or irretrievable). By default, services are not available (not checked).

CAUTION: Use this option with care. For example, when normally 2% of the traffic is effectively copied (subscriber has CPY service switched on) and send to the XS-CPY (using SSI in the EC rule), setting the CPY service to available when SSI information is unknown, 100% of the traffic will now go to XS-CPY. This is a 50x increase for which the XS-CPY might not be dimensioned.

18. Click **Save**.

The MGR creates the service and closes the tab.

13.4 Add/Modify Command Aliases

To add or modify SMS command aliases:

1. In the left navigation bar, select **SPF Services** ► **SPF services**.
The SPF Service tab appears.
2. Click on a service for which you want to modify SMS command aliases.
The service opens in a SPF Service tab.
3. If the command (in the **Command Aliases** list) you want to modify is active, deactivate it (as described in [Deactivate](#)).
4. In the **Command Aliases** list, click on the deactivated command that you want to modify.
A new Aliases tab appears.
5. In the **Keyword** box, enter the primary keyword for this command.
6. In the **Success Message** box, enter the template for a confirmation message after a successful provisioning action for this command. For details see the definition of
7. In the **Failure Message** box, enter the template for a failure message after a failed provisioning action for this command. For details see the definition of [Message Template String Format](#).
8. In the **Enabled** box, enter a string used to denote the 'enabled' state of a service (for example ON), to be used during message template expansion.
Note: This field is only applicable for the 'status' command.
9. In the **Disabled** box, enter a string used to denote the 'disabled' state of a service (for example OFF), to be used during message template expansion.
Note: This field is only applicable for the 'status' command.
10. In the remaining fields, up to three aliases can be defined for each of the following fields:
 - **Keyword**
 - **Success Message**
 - **Failure Message**
 - **Enabled** (for the 'status' command only)
 - **Disabled** (for the 'status' command only)
11. Click **Save**.
The MGR creates command aliases and closes the tab.
12. Activate the command alias, as described in [Activate](#).

13.5 Add/Modify Parameter Aliases

Note: This applies to the `set` command used by the BWL and FWD only.

To add or modify `set` command parameters aliases:

1. In the left navigation bar, select **SPF Services** ► **SPF services**.
The SPF Service tab appears.
2. Click on the service for which you want to add or modify `set` command parameter aliases.
The service opens in a SPF Service tab.
3. If the `set` command (in the **Command Aliases** list) is active, deactivate it (as described in [Deactivate](#)).
4. In the **Command Aliases** list, click on the deactivated `set` command.
A new Aliases tab appears.
5. In the **Parameter Text** list, click on the parameter you want add or modify.
A new Aliases tab appears.
For BWL these parameters apply:
 - blacklist
 - whitelist
 For FWD these parameters apply:
 - conditional
 - unconditional
6. In the **Keyword** box, enter the primary keyword for this parameter.
7. In the remaining **Alias** fields, up to three aliases can be defined for this parameter.
8. Click **Save**.
The MGR creates parameter aliases and closes the tab.

13.6 Message Template String Format

These parameters can be used in the message template string attributes:

Parameter	Description	Applies to...
%k	Keyword for the service	All services
%n	Name of the service	All services
%c	Command alias used at SM provisioning time	All services
%s	Subscriber MSISDN	All services
%e	Enabled/disabled state of the service for the subscriber	All services
%l	List of parameter values: <ul style="list-style-type: none"> • For non-DIL services, this means param1 or list table data • For DIL service, this means all distribution list numbers 	All services

Parameter	Description	Applies to...
%p	Parameter values provisioned by the user	All services
%pN	N th parameter value provisioned by the user, where N has a value of 1 up to 50	All services
%d	Number of entries in subscriber's parameter list	Non-DIL services
%1	First parameter for the subscriber for this service	Non-DIL services
%2	Second parameter for the subscriber for this service	Non-DIL services
%a	Addresses in a distribution list	DIL service only
%t	Status of the service: <ul style="list-style-type: none"> • For BWL, blacklist or whitelist • For FWD, conditional or unconditional Note: %t1 is the same as %t.	Non-DIL services
%t2	Name of alias1	Non-DIL services
%t3	Name of alias2	Non-DIL services
%t4	Name of alias3	Non-DIL services

Chapter 14

Batch Sending

Topics:

- *Introduction.....346*
- *Configuration Item Dependencies.....346*
- *Creating SMS Templates.....346*
- *Adding Distribution Lists.....347*
- *Configuring Delivery Schemes.....350*
- *Viewing Batch Job Status.....350*
- *Creating Batch Jobs.....351*
- *Configuring Batch Applications.....352*
- *Configuring Batch SMSCs.....353*
- *Configuring Batch Termination Points.....354*
- *Configuring Batch Properties.....355*

14.1 Introduction

When your system includes the Batch Server (BAT), you can send the same short message to many users (bulk SMS).

14.2 Configuration Item Dependencies

The following diagram illustrates the dependencies among BAT dynamic configuration items. The arrows point to the dependency.

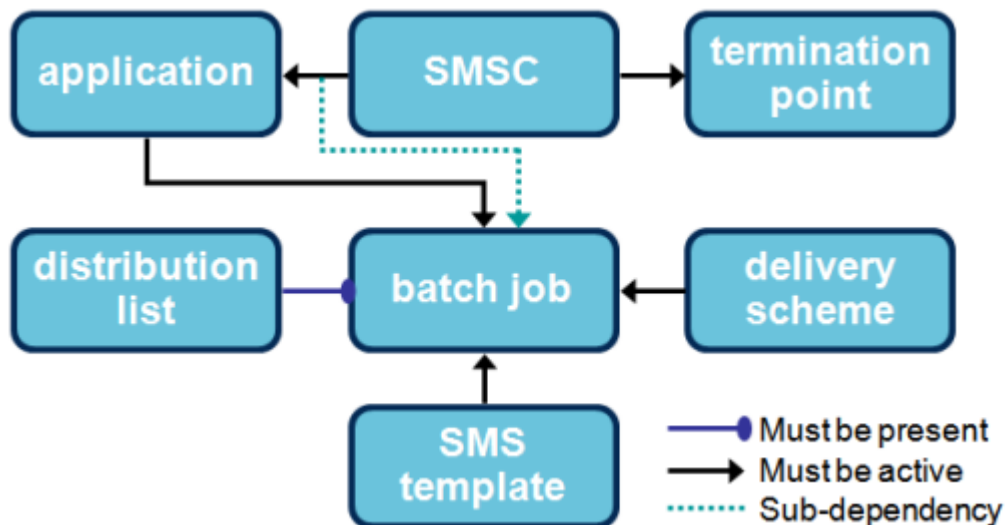


Figure 36: BAT dynamic configuration dependencies

The application configuration must exactly match the corresponding configuration on the HUB or external SMSC. In the case of the HUB, this means that you must create an:

- SMS application with the same settings as the batch application
- Outside listener with the same settings as the batch termination point

14.3 Creating SMS Templates

To create an SMS template:

1. In the left navigation bar, select **Batch Sending** ► **SMS Templates**.
The Template tab appears.
2. Click **Add New**.
A new Template tab appears.

3. Enter a unique name for the template in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the template in the **Description** box.
5. In the **Text** box, enter the message text (maximum 600 octets).

You can use the following variables in the message text:

- #MSISDN—Will be replaced with the recipient's MSISDN, as provided in the distribution list.
- #FNAME—Will be replaced with the recipient's first name, as provided in the distribution list. If the recipient's first name is omitted from the list, the variable will be replaced with the configured default first name.
- #SNAME—Will be replaced with the recipient's last name, as provided in the distribution list. If the recipient's last name is omitted from the list, the variable will be replaced with the configured default last name.
- ##—Will be replaced with a single number sign (#).

Variable names are case-insensitive. Long messages will be split into up to five parts, after all variables are replaced with the appropriate values.

6. In the **Originator** box, enter an alphanumeric string, short code, or national number to use as the message originator (maximum 15 numeric characters or 11 characters).
7. Enter the string to use as the recipient's first name if the first name is not present in the distribution list in the **Default Recipient First Name** box (maximum 30 octets).
8. Enter the string to use as the recipient's last name if the last name is not present in the distribution list in the **Default Recipient Last Name** box (maximum 30 octets).
9. Select the text format from the **Format** list:
 - GSM 7 (default)
 - GSM 8
 - UCS-2 (16-bit)

10. In the **Validity Period** box, enter the number of hours that the SMSC will retry delivery of the message; after this period, the message will expire (default 72).

11. Click **Save**.

The MGR creates the SMS template and closes the tab.

12. Activate the template.

Note: A short message template can only be modified or deactivated if it is not associated with an active batch job.

14.4 Adding Distribution Lists

To add a distribution list:

1. In the left navigation bar, select **Batch Sending ► Distribution Lists**.
The Batch Distribution List tab appears.
2. Click **Add New**.
A new tab appears.

3. Click **Browse**.
The File Upload dialog appears.
4. Navigate to the location of the distribution list text file.
Note: The file name must not exceed 32 characters.
5. Select the distribution list text file and click **Open**.
The File Upload dialog closes.
6. Click **Upload**.
The MGR uploads the distribution list text file and closes the tab.
7. Activate the distribution list.

Note: A distribution list can only be deleted if it is not associated with a batch job.

To ensure that you can restore your distribution lists after a MGR failure, regularly back up the `/var/TextPass/MGR/distribution_lists/` folder. After the MGR is restored, you can upload the distribution lists from most recent backup.

14.4.1 Downloading Distribution Lists

You can download distribution lists from the MGR in comma-separated value (CSV) files. Use this functionality to back up distribution lists or to modify distribution lists for use in future batch jobs. You can download the distribution list from any batch job, even one that is running.

Note: You cannot replace the distribution list of a batch job that has already started.

To download a distribution list:

1. In the left navigation bar, select **Batch Sending** ► **Distribution Lists**.
The Batch Distribution List tab appears.
2. Do one of the following:
 - Right-click the desired distribution list and select **Download**.
 - Select the check box next to one or more desired distribution lists and select **Download** from the **Action** menu.The Save As dialog box appears.
3. Select a location to save the list(s).
The default file name is the name of the list in the MGR.
4. Click **Save**.
The MGR saves the list(s) in CSV format.

You can open the distribution list file in any software that can open CSV files. A distribution list can contain up to 10,000,000 entries; some software, such as Microsoft Excel, may have a lower limitation on the number of entries allowed in CSV files.

14.4.2 Distribution List File

The distribution list file is a valid CSV file that contains the MSISDN, first name, and last name of each member of the list, in comma-delimited format:

```
MSISDN,firstname,lastname
```

The MSISDN can be in:

- International format: MSISDN beginning with a plus sign (+) and the country code; for example, +495891234567 (49 is the country code)
- National format: MSISDN beginning with a single zero and no country code; for example, 058912345

Duplicate MSISDNs are not allowed.

If a list member's first or last name contains a comma, you must enclose that part of their name in quotation marks.

In **Batch Sending ► SMS Templates**, you can configure a default first name and last name to use if an entry is missing one or both. Note that, if the first name and/or last name is omitted from a distribution list entry, the commas must still be included.

Sample Distribution List

```
+407206666604,Jamie,Dunmore
+407206666605,Max,Sester
+407206666606,Melisa,Rotenberry
+407206666607,Lonnie,Calahan
+407206666608,Tanisha,de Porche
+407206666609,Karina,Bang
+407206666610,Nelson,Brackin
+407206666611,Max,Renken
+407206666612,Ted,Schwan
+407206666613,Jamie,Funderburke
+407206666614,Guy,Babich
+407206666615,Clayton,Wattles
+407206666616,Odessa,Tropea
+407206666617,Jeanie,Borchert
+407206666618,Milagros,Lenahan
+407206666619,Chandra,Exline
```

Sample Distribution List Member Name with Comma

```
+407206666620,Hugh,"Reitman, Jr."
```

Sample Distribution List with Omitted Names

```
+407206666600,Liza,Sailer
+407206666601,Lonnie,de Boice
+407206666602,Tabatha,
+407206666603,Jessie,
+407206666621,,Longmore
+407206666622,,Mcgrady
```

14.5 Configuring Delivery Schemes

To configure a delivery scheme:

1. In the left navigation bar, select **Batch Sending** ► **Delivery Schemes**.
The Batch Delivery Scheme tab appears.
2. Click **Add New**.
A new Batch Delivery Scheme tab appears.
3. Enter a unique name for the scheme in the **Name** box (maximum 31 octets).
4. Optionally enter a description of the scheme in the **Description** box.
5. From the **Submission Type** list, select the submission type:
 - Immediate
 - Deferred
 - Periodic
6. If you selected **Deferred**:
 - a) Enter the submission time in the **Submit Time** box (HH:MM format).
 - b) Enter the submission date in the **Submit Date** box (YYYYMMDD format).
7. If you selected **Periodic**, enter the repetition scheme in the **Repetition Scheme** box (default 0 0 * * 1-7).
The repetition scheme format is m h D M W, where:
 - m is the minute, 0-59
 - h is the hour, 0-23
 - D is the day of the month, 1-31
 - M is the month, 1-12
 - W is the day of the week, 1-7 where 1 is Sunday
8. Click **Save**.
The MGR creates the delivery scheme and closes the tab.
9. Activate the delivery scheme.

Note: A delivery scheme can only be modified if it is not associated with an active batch job.

14.6 Viewing Batch Job Status

The MGR periodically retrieves the operational status of sub-jobs and consolidates them for each batch job.

If a server becomes unavailable at the time that the information is retrieved, the batch job status in the MGR will show the last known value. The **Settings** ► **Network Layout** ► **Devices** tab will show an error message for the stopped BAT.

To view the operational state of each batch job, go to **Batch Sending** ► **Batch Jobs Status** in the MGR Web interface. The view shows the percentage of the job that has been completed.

To see the operational state of a particular batch job, hover the mouse pointer over the job's row. To see the counters for a batch job, click it.

To refresh the view, click **Refresh**.

Batch Job Status

Job Name	BAT1	Total
Job1	52 %	52 %

Figure 37: Example batch job status

14.7 Creating Batch Jobs

Prerequisites:

- SMS template
- Distribution list
- Batch application
- Delivery scheme

To create a batch job:

1. In the left navigation bar, select **Batch Sending** ► **Batch Jobs**.
The Batch Job tab appears.
2. Click **Add New**.
A new Batch Job tab appears.
3. Enter a unique name for the job in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the job in the **Description** box.
5. Enter the job's priority in the **Priority** box (0-99, default 50).
6. Select the message template from the **Template** list.
7. Select the distribution list from the **Distribution List** list.
8. Select the batch application from the **Application** list.
9. Select the delivery scheme from the **Delivery Scheme** list.
10. To enable delivery notification from the SMSC, select **Delivery Tracking** (enabled by default).
It is recommended that delivery tracking be disabled when BAT interfaces directly with a third-party SMSC.
11. Enter the maximum number of messages that can be sent in one second for the batch job in the **Max. Submission** box (default 25).
12. Enter a validity period for the batch job in the **Validity Period** box (default 72 hours).
The validity period ensures that the batch job does not indefinitely remain in a running or delivery pending state, in the event of a failure. If the validity period ends before all messages are submitted

and all delivery notifications are received, the batch job's operational state will be changed to "expired", and no further action will be taken unless a user restarts the batch job.

13. Click Save.

The MGR creates the batch job and closes the tab.

14. Activate the batch job.

14.8 Configuring Batch Applications

Prerequisite:

- SMSC

To configure a batch application:

1. In the left navigation bar, select **Batch Sending ► **Applications** ► **Applications**.**

The Batch Application tab appears.

2. Click Add New.

A new Batch Application tab appears.

3. Enter a unique name for the application in the **Name box (maximum 31 characters).**

4. Optionally enter a description of the application in the **Description box.**

5. Enter the application short code in the **Short Code box.**

6. Select the application protocol to use between the application and the HUB/SMSC from the **Protocol list:**

- SMPP (default)
- UCP

7. If the protocol is SMPP:

a) Enter the password in the **SMPP Password box.**

To generate a random password, click



b) Enter the window size in the **SMPP Window Size box (default 255).**

c) Enter the ID to use when identifying the External Short Messaging Entity (ESME) that is requesting to bind as transceiver with the SMSC (default BAT).

d) Enter the type of system to use when identifying the ESME that is requesting to bind as transceiver with the SMSC (default USSD).

Note: In SMPP, only 0 through 9, a through z, and A through Z are supported for alphanumeric originator addresses. Special characters cannot be used.

8. If the protocol is UCP:

a) Enter the password in the **UCP Password box.**

To generate a random password, click



b) Enter the window size in the **UCP Window Size** box (default 100.)

Note: All GSM 7-bit characters can be used for alphanumeric originator addresses.

9. Enter the number of allowed SMPP or UCP sessions in the **Number of Sessions** box (default 1).

Each BAT server will distribute this number of sessions equally across all termination points that are configured for the SMSCs to which this batch application is assigned.

For example, assume that the allowed number of sessions is 6 and the application is assigned to SMSC1 and SMSC2. SMSC1 has two termination points: Ta and Tb. SMSC2 has three termination points: Tc, Td, and Te. Each BAT server would distribute three sessions each to Ta and Tb, and two sessions each to Tc, Td, and Te. If there are ten BAT servers, there would be 30 sessions each to Ta and Tb, and 20 sessions each to Tc, Td, and Te.

10. Enter the number of seconds after which to send a keep-alive signal on an active session with the SMSC in the **Keep Alive Interval** box (default 60).
11. Enter the maximum number of seconds that the BAT waits for a response from the HUB/SMSC before considering a session to be expired in the **Maximal Response Time** box.
12. Enter the number of seconds to wait after disconnection before reconnecting the session in the **Session Timer** box.
13. In the **Max Session Retry Attempts** box, enter the maximum number of allowed log-in attempts before the BAT stops attempting to log in.
14. In the Batch SMSC section, select the SMSC(s) for which this application should be used.
15. Click **Save**.

The MGR creates the batch application and closes the tab.

16. Activate the application.

The settings in steps 5 through 12 must exactly match the corresponding configuration on the HUB or SMSC.

Note: An application can only be modified if it is not associated with an active batch job.

14.9 Configuring Batch SMSCs

To configure a batch SMSC:

1. In the left navigation bar, select **Batch Sending** ► **Applications** ► **SMSC's**.

The Batch SMSC tab appears.

2. Click **Add New**.

A new Batch SMSC tab appears.

3. Enter a unique name for the SMSC in the **Name** box (maximum 31 characters).

4. Optionally enter a description of the SMSC in the **Description** box.

5. Click **Save**.

The MGR creates the batch SMSC and closes the tab.

6. Activate the SMSC.

Note: An SMSC can only be modified if it is not associated with an application and all termination points have been deleted from it. An SMSC can only be deleted if it is not associated with an application.

14.10 Configuring Batch Termination Points

If BAT will be interfacing with the HUBs in the system, it is not necessary to create a termination point for a load balancer. However, to provide failover and redundancy, you should create a termination point for each HUB. This ensures that, if one HUB fails, BAT can connect to a different HUB.

Prerequisites:

- Batch SMSC

To create a batch SMSC termination point:

1. In the left navigation bar, select **Batch Sending** ► **Applications** ► **SMSCs**.

The Batch SMSC tab appears.

2. Click an existing SMSC.

A new Batch SMSC tab appears.

Note: The termination point will default to the SMSC that you clicked, but you can change it while creating the termination point.

3. Under Termination Points, click **Add New**.

A Batch Termination Point tab appears.

4. Enter a unique name for the termination point in the **Name** box (maximum 31 characters).

5. Optionally enter a description of the termination point in the **Description** box.

6. Enter the SMSC IP address in the **IP Address** box.

7. Enter the SMSC DNS name in the **DNS Name** box.

The DNS name is resolved to an IP address before making a TCP connection with the SMSC. If there is a connection failure, DNS resolution will be retried once.

Note: The IP address and DNS name are not both required. Only one must be configured.

8. Enter the SMSC port number in the **Port Number** box (default 1200).

9. In the **Retry Timer** box, enter the number of seconds before retrying the TCP connection (default 60).

10. In the **Retry Attempts** box, enter the number of times to retry the TCP connection (default 0).

After this number is exhausted, the sessions for this termination point will be distributed to other termination points.

Setting this parameter to 0 instructs BAT to attempt the connection an infinite number of times. If multiple termination points are configured, each termination point will be attempted twice, with the interval set in the **Retry Timer** parameter between attempts.

11. Select the session protocol from the **Protocol** list:

- SMPP (default)
- UCP

Applications will only connect to termination points that are set to the same protocol as the application.

- From the **SMSC** list, select the SMSC to which the termination point should be assigned (defaults to the SMSC that you initially clicked).

- Click **Save**.

The MGR creates the termination point and closes the tab.

- Activate the termination point.

Note: A termination point cannot be assigned to more than one SMSC.

14.11 Configuring Batch Properties

To configure BAT properties:

- In the left navigation bar, select **Batch Sending ► Properties**.
The Batch Properties tab appears.
- In the **Maximum Throughput** box, enter the maximum number of protocol data units (PDUs) that the BAT can send per second (default 250).

Note: The maximum throughput should not greatly exceed the maximum physical capacity.

- Select the shutdown method from the **Shutdown Type** list:
 - Graceful:** Upon graceful shutdown, BAT will finish distributing active jobs, disable job distribution (if it is the master BAT), withdraw from the pool of available BATs accepting sub-jobs, submit all pending messages, and close all SMPP or UCP sessions with the HUB/SMSC.
 - Forced** (default): Upon forced shutdown, the BAT will disable job distribution (if it is the master BAT), terminate the submission of all pending messages, and close all SMPP or UCP sessions with the HUB/SMSC.
- In the **Minimum BAT Count** box, enter the minimum number (quorum) of BATs that must be available for master and subordinate selection (default 1).

The recommended value is $n/2 + 1$, where n is the total number of BAT nodes.

- To enable logging, select **Enable Logging**.
- If you are enabling logging, enter the template for the log file name in the **Log File** box (default %h_%y%m%d_%H%M%S_%4.dat).

The available file name template variables are:

Variable	Description
%Y	Four-digit year
%y	Two-digit year
%m	Two-digit month
%d	Two-digit day of the month
%H	Hour (24-hour format)

Variable	Description
%S	Seconds
%h	Name of the host on which BAT is running
%1	One-digit sequence number
%2	Two-digit sequence number
%3	Three-digit sequence number
%4	Four-digit sequence number
%5	Five-digit sequence number
%6	Six-digit sequence number
%7	Seven-digit sequence number
%8	Eight-digit sequence number

Note: Logs are not automatically purged.

7. Click **Save**.
The MGR saves the properties and closes the tab.

Chapter 15

Tracing

Topics:

- *Introduction.....358*
- *Application Traffic Trace Filter.....358*
- *SS7 Trace Filters.....359*
- *SIP Tracing.....360*

15.1 Introduction

When your system includes a RTR, IIW or HUB, you can create trace filters to capture data and send it to a configured trace receiver.

The trace receiver is a command-line tool (`tp_trace_receiver`); refer to the Tools Operator Manual for more information about its configuration and usage.

15.2 Application Traffic Trace Filter

When your system includes a HUB, you can create trace filters to capture data and send it to a configured trace receiver.

Refer to the HUB Operator Manual for detailed information about tracing and recommended tracing methods.

15.2.1 Creating Trace Filters

To create a trace filter:

1. In the left navigation bar, select **Tracing** ► **Trace Filter**.
The Trace Filters tab appears.
2. Click **Add New**.
A new Trace Filters tab appears.
3. Enter a unique name for the trace filter in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the trace filter in the **Description** box.
5. In the **Server IP** box, enter the IP address of the server to which to send the traces from this filter.
6. In the **Server Port** box, enter the UDP port of the server to which to send the traces from this filter.
7. Click **Save**.
The MGR creates the filter and closes the tab.
8. Configure conditions for the trace filter.
9. After you have created all desired conditions, activate the trace filter.

15.2.2 Configuring Trace Filter Conditions

Prerequisites:

- Trace filter

You can configure many conditions for each trace filter. To configure a trace condition:

1. In the left navigation bar, select **Tracing** ► **Trace Filter**.
The Trace Filters tab appears.
2. Click the trace filter to which you want to add a condition.

The trace filter opens in a separate Trace Filters tab.

3. Click **Add New** in the lower right corner of the Trace Filters tab.
The Trace Filter Conditions tab appears.
4. Select a trace filter from the **Trace Filter** list.
5. Select a trace condition that needs to be satisfied for the trace filter to match from the **Condition** list:
 - **Application**—A list of applications appears; select the desired application
 - **Short Number**—A box appears; enter the desired short number of the application (sessions that receive a valid UCP60 with this short number as OAdC will be sent to the trace receiver)
 - **IP Address**—A box appears; enter the desired source IPv4/IPv6 address of the application (all sessions that have packets sent to and received from this IP will be sent to the trace receiver). IP Address value can be IPv4 or IPv6 address.
 - **Unauthenticated sessions**— An outside session has not yet been authenticated
 - **All MXP Traffic**—MXP is a NewNet proprietary protocol used for communication between the HUB, RTR, and AMS. With this condition traffic can be traced between HUB and RTR. This condition is only useful in case the NewNet Technical Assistance Centre (TAC) requested to use this option.
6. Click **Save**.
The MGR creates the trace filter condition and closes the tab.

Note: You must activate trace filters for them to begin collecting data, but it is not necessary to activate trace filter conditions (they are always active).

15.3 SS7 Trace Filters

When your system includes a RTR, you can create SS7 trace filters to capture data and send it to a configured trace receiver.

Refer to the RTR Operator Manual for detailed information about SS7 trace filters and guidelines for devising filter expression.

15.3.1 Creating Trace Filters

To create a trace filter:

1. In the left navigation bar, select **Tracing** ► **SS7 Trace Filter**.
The Trace Filters tab appears.
2. Click **Add New**.
A new SS7 Trace Filters tab appears.
3. Enter a unique name for the trace filter in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the trace filter in the **Description** box.
5. In the **Server IP** box, enter the IP address of the server to which to send the traces from this filter.
6. In the **Server Port** box, enter the UDP port of the server to which to send the traces from this filter.

7. In the **Filter Expression** box, enter the Filter Expression for the Trace filter (maximum 2048 character including whitespace). Filter Expression should be understood by `tshark` (Refer to http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html).

Note: Using filter expression would have an effect on memory usage and long running traces with filter expression are not recommended. If filter expression is not configured, then all incoming/outgoing SS7 PDUs will be sent to the trace receiver server unfiltered.

8. In the **Memory Usage** box, enter the Maximum amount of memory in Megabytes allowed to use by filtering application, from 512 to 4096 (4 GB). Default value is 1024 MB. Memory parameter is applicable only if **Filter Expression** is specified. In case `tshark` process memory usage exceeds the configured value then the `tshark` process will get restarted.
9. In the **Linkset** box, enter list of linkset names to trace (maximum 16 linksets). If this field is left blank then all linksets specified in the corresponding RTR node's host configuration file will be traced. Linkset-based tracing capability is supported only for SS7 (MTP3) links, not for SIGTRAN (M3UA) links. Multiple linksets can be specified separated by the new-line character.
10. Click **Save**.

The MGR creates the filter and closes the tab.

11. Activate the trace filter.

Note:

1. You must activate SS7 trace filters for them to begin collecting data.
2. Maximum 10 SS7 trace filters can be configured in a domain on MGR.
3. Only one SS7 trace filter can be active in a domain at a time.
4. You must de-activate SS7 trace filter before deleting any SS7 trace filter.

15.4 SIP Tracing

You can create SIP trace filters to capture SIP data and send it to a configured trace receiver. IIW may use external application `tshark` to apply filters on incoming/outgoing SIP traffic.

The trace receiver is a command-line tool (`tp_trace_receiver`); refer to the Tools Operator Manual for more information about its configuration and usage.

15.4.1 Creating Trace Filters

To create a trace filter:

1. In the left navigation bar, select **Tracing** ► **SIP Trace Filter**. The Trace Filters tab appears.
2. Click **Add New**. A new SIP Trace Filters tab appears.
3. Enter a unique name for the trace filter in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the trace filter in the **Description** box.
5. In the **Trace Server IP** box, enter the IP address of Server (on which `tp_trace_receiver` is running) to send the traces from this filter.
6. In the **Trace Server Port** box, enter the UDP port of Server (on which `tp_trace_receiver` is running) to send the traces from this filter

7. In the Filter Expression box, enter the Filter Expression for the Trace filter (maximum 2048 character including whitespace). Filter Expression should be understood by tshark (Refer to http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html).
Note: Using filter expression would have an effect on memory usage and long running traces with filter expression are not recommended. Special characters like @,!,#,%," need to be escaped using the backslash (\). You can always enclose any character - including special characters - inside a double-quoted string.
 Hence as long as a special character is enclosed within double-quotes, it will not require to be escaped with a backslash. However, in that case each of the enclosing double-quote character will need to be escaped (as shown in the example below). For example, if a filter expression needs to be created on sip.Call-ID then it should be written as:

```
sip.Call-ID == \"1-4715@10.41.128.24\"
```
8. In SIP **Listener** box, enter list of listener names to trace (maximum 50 listeners). If this field is left blank or no listener matches with listeners specified in the corresponding IIW node's host configuration file then all the listeners specified in the corresponding IIW node's host configuration file will be traced. Multiple listeners can be specified separated by the new-line character.
9. In the Memory Usage box, enter the Maximum amount of memory in Megabytes allowed to use by filtering application, from 512 to 4096 (4 GB). Default value is 1024 MB.
Note: Memory parameter is applicable only if Filter Expression is specified. In case tshark process memory usage exceeds the configured value then the tshark process will get restarted.
10. Click Save.
 The MGR creates the filter and closes the tab.
11. Refer section [Configuring SIP Trace Filter Conditions](#) for configuring SIP Trace Filter Conditions.

15.4.2 Configuring SIP Trace Filter Conditions

Following is the prerequisite for configuring the SIP Trace Filter Condition.

- Trace Filter should be existing.

You can configure many conditions for each trace filter. To configure a trace condition:

1. In the left navigation bar, select **Tracing-> SIP Trace Filter**. SIP Trace Filters tab appears.
2. Click the trace filter to which you want to add a condition. The trace filter opens in a separate SIP Trace Filters tab.
3. Click Add New in the lower right corner of the SIP Trace Filters tab. The Trace Filter Conditions tab appears.
4. Select a trace filter from the Trace Filter list.
5. Select a trace condition that needs to be satisfied for the trace filter to match from the Condition list
 - Originator Address - A box appears. Enter ipv4 or ipv6 address of originator.
 - Originator Port - A box appears. Enter port of originator (0 to 65535).
 - Recipient Address - A box appears. Enter ipv4 or ipv6 address of recipient.
 - Recipient Port - A box appears. Enter port of recipient (0 to 65535).
 - Protocol - A box appears. Enter protocol . (tcp , sctp, udp).
 - SIP End Point - A dropdown list appears. Select the SIP End Point.
6. Click Save. The MGR creates the trace filter condition and closes the tab.

Note:

1. You must activate SIP trace filters for them to begin collecting data but it is not necessary to activate trace filter conditions (they are always active).
2. Maximum of 10 SIP trace filters can be configured in a domain on MGR.
3. Multiple trace filter can be active in a domain at a time provided none of the active filter contains filter expression.
4. Only one filter can be active in a domain at a given time when the activated filter contains filter expression.
5. You must de-activate SIP trace filter and delete all its associated conditions before deleting any SIP trace filter.
6. Trace Filter conditions are applied as 'or' i. e. if any of condition matches, trace filter will be applied on the SIP PDU.
7. Maximum of 100 trace conditions can be configured for a given trace filter.
8. If filter expression is not configured, no condition specified and no matching listener configured in trace filter, then all incoming/outgoing SIP PDUs will be sent to the trace receiver server unfiltered.
9. IIW will filter SIP Traffic based on Trace Filter Conditions set in active SIP Trace Filter:
 - a. Origin Address condition. It filters:
 - a. All SIP Requests with source IP equal to Origin address specified in the condition.
 - b. All SIP Responses with destination IP address equal to address specified in condition.
 - b. Origin Port condition. It filters:
 - a. All SIP Requests with source port equal to Origin port specified in the condition.
 - b. All SIP Responses with destination port equal to port specified in condition.
 - c. Recipient Address condition. It filters:
 - a. All SIP Requests with destination IP equal to Recipient address specified in the condition.
 - b. All SIP Responses with source IP address equal to address specified in condition.
 - d. Recipient Port condition. It filters:
 - a. All SIP Requests with destination port equal to Recipient port specified in the condition.
 - b. ii. All SIP Responses with source port equal to port specified in condition.
 - e. Protocol condition filters SIP traffic based on the Transport protocol (UDP, SCTP, TCP)

Chapter 16

Settings

Topics:

- *Introduction.....364*
- *Setting Your Preferences.....364*
- *User Administration.....364*
- *Viewing Error and Change Logs.....368*
- *Adding Domains.....370*
- *Configuring Servers.....371*
- *Configuring Devices.....372*
- *Configuring Global Settings.....378*
- *Pending Transactions.....380*
- *Verifying Device License Information.....382*
- *Customising the Application Password Generator.....382*
- *Configure CCI Properties.....384*

16.1 Introduction

In the MGR settings, you can:

- Set your MGR preferences
- Manage MGR users and user groups
- View the MGR's error log and change logs
- Configure the layout of your network (devices and domains)
- Configure global MGR settings
- Verify device license information
- Customise the MGR's SMS application password generator
- Customise character conversion sets

Note: For information about configuring the Customer Care Interface (CCI) component, refer to the CCI Operator Manual.

16.2 Setting Your Preferences

To change your MGR preferences:

1. In the left navigation bar, select **Settings ► My Preferences**.

The My Preferences tab appears.

2. Change one or more of the following options:

- The number of lines that appear on each page (minimum is 10)
- Your password (you must also confirm it)
- Your default view level (basic, standard, or expert)
- The date and time format

3. Click **Save**.

The MGR saves the changes and closes the tab.

Note: The MGR automatically assigns your user index number, and it cannot be changed. Your name, log-in, and description can only be changed by an administrator. If you are an administrator, you can change your own name, log-in, or description in **User Admin ► User(s)**.

16.3 User Administration

Administrators use the MGR's user administration functions to create user accounts, assign users to groups, and assign rights to user groups.

16.3.1 User Password Policy

Administrators can set different session time-outs, password restrictions, and log-in attempt restrictions for different user groups. For example, the MGR session time-out can be set to 10 minutes for super users and 30 minutes for customer service representatives.

The user password policy is:

- Password patterns are enforced by the system and have the following requirements:
 - Contain at least 2 alphabet letters or underscores
 - Contain at least 1 digit
 - Length is at least 8 alphanumeric characters or underscores.
- Passwords are checked against the previous password history to reject recently used passwords (configurable range 1-10).
- Password expiration is configurable by the administrator (0-99 days). An administrator can define the period of time before the lifetime is reached; the user is automatically requested to change the password. If this request is ignored and the lifetime is reached, the user can not log in until the password is changed. When set to 0 (zero), the password expiration is disabled.

The default lifetime is 60 days.

16.3.2 Add a User

Prerequisites:

- Domain
- User group

To add a user:

1. In the left navigation bar, select **Settings** ► **User Admin** ► **User(s)**.
The Users tab appears.
2. Click **Add New**.
The New User tab appears.
3. Enter the user's name in the **Name** box.
4. Enter a unique log-in ID for the user in the **Login** box.
5. Optionally, enter a description of the device in the **Description** box.
6. In the **Lines Per Page** box, set the number of lines that the user will see on each page (default is 20).
7. In the **User Password** box, enter a password for the user.
8. Retype the password in the **Confirm Password** box.
9. Select a group for the user from the **User Group** list.
10. Select the user's default domain from the **Default Domains** list.
11. Select the user's default view from the **View Level** list.
12. Select a date and time format for the user from the **Date Format** list.
13. Click **Save**.

The MGR creates the user and closes the tab.

16.3.3 Unlock a User Account

When a user exceeds the maximum allowed number of subsequent failed log-in attempts (as set for their group in **Settings > User Admin > Groups**), the MGR locks the user's account. An administrator must unlock the account.

To unlock a user account:

1. In the left navigation bar, select **Settings > User Admin > User(s)**.

The Users tab appears. The icon next to the locked user's name is



2. Select the user by clicking the check box in his or her row.
3. From the **Action** menu, select **Activate**.

The MGR unlocks the user's account and the icon next to his or her name changes to



The user can now attempt to log in again.

16.3.4 Add a User Group

The default user groups are:

Group	Privileges
Administrators	All privileges for all items
Super Users	All privileges for all items
Customer Support	<ul style="list-style-type: none"> • All privileges for My Settings • View privileges for all items except User Admin, Global Settings, Devices and Domains
Counting Management	<ul style="list-style-type: none"> • All privileges for Counting Rules • All privileges for Statistics • View privileges for all items
Firewall Management	<ul style="list-style-type: none"> • All privileges for Routing Rules, Advanced Filters, Logging, and Firewall • View privileges for all items
Application Management	All privileges for Applications, Application Groups, and Application Categories
BAT Server Management	All privileges for Batch Sending

You can modify these user groups and/or add new user groups.

Prerequisites:

- Domain

To add a user group:

1. In the left navigation bar, select **Settings** ► **User Admin** ► **Groups**.
The User Groups tab appears.
2. Click **Add New**.
The New User Group tab appears.
3. Enter a unique name for the group in the **Group Name** box.
4. Optionally, enter a description of the group in the **Description** box.
5. In the **Session Timeout** box, set the number of minutes that a user's session can be idle before it times out (default is 20 minutes).
To allow the user's sessions to never time out, set **Session Timeout** to 0.
6. In the **Password Lifetime** box, set the number of days before a user's password expires (default is 60 days).
To allow the user's password to never expire, set **Password Lifetime** to 0.
7. In the **Password History** box, set the number of previous passwords to keep for users in the group (default is 5 passwords).
A user cannot reuse a password in his or her history.
8. In the **Max. Failed Attempts** box, set the maximum number of subsequent times a user can attempt to log in with an incorrect ID or password before he or she is locked out of his or her account. When a user is locked out, an administrator must reset the account.
Note: The username/password administration of the MGR and CCI are shared, and lockout info as well. The wrong attempt counter increases whenever user tries to login with consecutive wrong passwords in MGR GUI or CCI GUI or combination of both. After a successful login, the wrong attempt counter gets reset. The account never gets disabled for a zero value of **Max. Failed Attempt**. In this case, only the value of the wrong attempt counter increases for each failed log-in attempt.
9. If users in the group should be allowed to view restricted user data (that is, SMS content), select **View Restricted Data** (by default, this option is not selected).
If the user is not allowed to view restricted data, then the MGR will replace SMS content with ' X ' characters when the user uses the Log Search or Customer Care Interface (CCI).
10. If users in the group should be allowed to view encrypted user data (that is, SMS content), select **View Encrypted Data** (by default, this option is not selected). This option cannot be selected if **View Restricted Data** option is not selected.
11. If users in the group should be allowed to view the LGP background query results of all users, select **View All Users Background Query** (by default, this option is not selected).
12. In the **Privilege Assignments** section, select the rights that the users in the group should have for each domain (as defined in **Settings** ► **Network Layout** ► **Domains**).

There are several types of privileges:

- Activate
- Deactivate

- Delete
- Edit
- New
- View

Each type of privilege can be assigned to various items in the MGR menu, at the top (category) level and at the individual menu item level. Click the plus sign to expand a category and view individual menu items. A checkbox with a gray background indicates that there are both enabled and disabled items at the lower level.

To assign a single type of privilege for all items, select the topmost box in that privilege's column; for example, to allow users to view all items in the MGR, select the topmost box under **View**.

To assign all types of privileges for a single item, select **Select All** in that item's row; for example, to allow users to have all privileges for the Firewall, select **Select All** in the **Firewall** row.

Privilege Assignments							
Domain / Name	Select All	Activate	Deactiv..	Delete	Edit	New	View
[-] main	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Routing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Firewall	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] SMS Applications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Environment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] Storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Advanced Filters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 38: MGR privileges

13. Click **Save**.

The MGR creates the user group and closes the tab.

16.3.5 Remove a User Group

For instructions on removing a user group, refer to [Delete](#).

You cannot remove a user group that one or more users are assigned to. Before removing the user group, you must assign all users in the group to a different group in **Settings** > **User Admin** > **User(s)**.

16.4 Viewing Error and Change Logs

The **Errors and Changes** section contains logs of errors and changes that occur in the MGR itself.

16.4.1 Error Log

The error log lists errors that MGR users encounter. To view the MGR error log, select **Settings** > **Errors and Changes** > **Errors**.

To view details about an error in the log, click the error row. A new tab appears with the following information:

- Log-in of the user who encountered the error

- Domain in which the user encountered the error
- The target table in the MGR database (if applicable)
- A description of the error
- The target record in the MGR (if applicable)
- The MGR action
- The date and time when the error occurred

To refresh the error log, click **Refresh** on the Error Log tab.

Note: You can change the location of the error log in **Settings** ► **Global Settings**.

16.4.2 User Change Log

To view the log of MGR user changes, click **User Changes**.

To view details about a change in the log, click the change row. A new tab appears with the following information:

- Log-in of the user who made the change
- Domain in which the user made the change
- Type of configuration item that was changed
- Index of the configuration item that was changed
- Name of the configuration item that was changed
- Operation that the user did
- The date and time when the user made the change

Note: You can change the location of the user change log in **Settings** ► **Global Settings**.

16.4.3 Automatic Change Log

The automatic change log lists changes that the MGR automatically makes. To view the automatic change log, select **Settings** ► **Errors and Changes** ► **Auto Changes**.

To view details about a change in the log, click the change row. A new tab appears with the following information:

- Indication that this was an auto-update
- Domain in which the MGR made the change
- Type of configuration that changed
- Index of the configuration item
- Name of the configuration item
- Change operation
- The date and time when the MGR made the change
- Change details:
 - Attribute name
 - Old value
 - New value

To refresh the automatic change log, click **Refresh** on the Automatic Change Log tab.

16.5 Adding Domains

To add a domain to the MGR:

1. Log in to the main domain.
2. From the left navigation bar, select **Settings** ► **Network Layout** ► **Domains**.
The Domains tab appears.
3. Enter a name for the domain in the **Name** box (maximum 31 characters).
Domain names can only contain a-z, A-Z, and the underscore (_) character.
4. Optionally, enter a description of the domain in the **Description** box.
5. For **Applications**, select a sharing option:
 - **Shared: Use from Main:** The item will be shared between the main domain and the new domain. If you take action on an item in the main domain, the action will be reflected in the new domain. For example, if you delete an item from the main domain, it will be automatically deleted from the new domain.
Restriction: You can only use this option for applications if the following items are also set to **Shared: Use from Main:**
 - Application groups
 - Application categories
 - Service centers
 - Service classes
 - **Not Shared: Make initial copy from Main:** The item will be copied from the main domain and the new domain will be independent of the main domain. If you taken action on an item in the main domain, the action will not be reflected in the new domain. For example, if you add a new item in the main domain, the item will not appear in the new domain.
 - **Not Shared: No initial copy from Main:** The item in the new domain is completely independent of the main domain. The item in the new domain is empty.
 - **Not Shared: Copy all from Main (existing and new):** Initially, all items from the main domain are copied to the new domain at the moment it is created. Subsequently, every new item is copied to the new domain when it is created in the main domain. Only the creation is copied; all other actions are per domain.
Restriction: You can only use this option for applications if the following entries are **Shared: Use from Main:**
 - Application groups
 - Application categories
 - Service centers
 - Service classes
6. For the remaining configuration items, select a sharing option:
 - **Shared: Use from Main:** The item will be shared between the main domain and the new domain. If you take action on an item in the main domain, the action will be reflected in the new domain.

For example, if you delete an item from the main domain, it will be automatically deleted from the new domain.

- **Not Shared: Make initial copy from Main:** The item will be copied from the main domain and the new domain will be independent of the main domain. If you taken action on an item in the main domain, the action will not be reflected in the new domain. For example, if you add a new item in the main domain, the item will not appear in the new domain.
- **Not Shared: No initial copy from Main:** The item in the new domain is completely independent of the main domain. The item in the new domain is empty.

7. Click **Save**.

The MGR creates the domain and closes the tab.

8. In **Settings > User Admin > Groups**, assign rights for the new domain to the appropriate group(s). You can use the `tp_mgr_domain_sharing` command-line tool to change the sharing of an existing domain. Refer to [tp_mgr_domain_sharing](#) for more information.

9. Follow the below steps to create a common semi-static configuration file for each new domain:

- Login into MGR server as user `textpass` and create `common_config_<new domain name>.txt` and place this file in `/usr/TextPass/etc/` path.
- Switch to user `root` and restart the MGR using below commands:

```
# /usr/TextPass/bin/tp_mgr_stop
# /usr/TextPass/bin/tp_mgr_start
```

16.5.1 Domain Database Management

The MGR creates a MySQL database for each domain. By default, there are two MySQL databases:

- `mgr_domain_mgr`
- `mgr_domain_main`

When you add a new domain, the MGR creates a new MySQL database based on the naming pattern `mgr_domain_<domain name>`. Because of this functionality, when adding new domains, you may need to update your MySQL configuration file (normally `/etc/my.cnf`).

If you have started multiple MySQL processes, each with a custom configuration file, you must update the particular configuration file. In particular, if you have configured MySQL replication and you must replicate specific databases, you must update the list of databases to include the database of the new domain.

16.6 Configuring Servers

Prerequisites:

- Domain
- Poller

You must configure servers before you can configure devices. To configure a server in your system:

1. In the left navigation bar, select **Settings** ► **Network Layout** ► **Servers**.
The Servers tab appears.
2. Click **Add New**.
A new Servers tab appears.
3. Enter a name for the server in the **Name** box (maximum 31 characters).
4. Enter the server's IP address in the **IP Address** box.
5. Enter SNMP port number of the server in the **System SNMP Port** box. Default is 11114.
6. Enter the number of CPU cores in the server in the **CPU Cores** box. Default is 1.
The number of CPU cores is as follows for:
 - HP DL380 G6 (Dual Processor with Intel® Hyper-Threading disabled): 8
 - HP DL380 G6 (Dual Processor with Intel® Hyper-Threading enabled): 16
 - HP DL380 G7 (Dual Processor with Intel® Hyper-Threading disabled): 12
 - HP DL380 G7 (Dual Processor with Intel® Hyper-Threading enabled): 24
7. From the **Domain** list, select the domain to which the server belongs (defaults to the main domain).
8. Optionally, from the **Poller** list, select a poller for the server (as configured in **Statistics** ► **Settings** ► **Pollers**).
9. Click **Save**.
The MGR saves the server and closes the tab.

16.7 Configuring Devices

Use the MGR to manage the devices in your system.

16.7.1 Add a Device

Prerequisites:

- Domain
- Server

To add a device:

1. In the left navigation bar, select **Settings** ► **Network Layout** ► **Devices**.
The Devices tab appears.
2. Click **Add New**.
The New Device tab appears.
3. Enter a name for the device in the **Name** field (maximum 31 characters).

Note: It is strongly recommended that you give each device a unique name. Adding a new device with the same name as an existing device will not replace the existing device. However, the presence of two devices with the same name can increase the difficulty of statistics and log analysis.

4. Optionally, enter a description of the device in the **Description** field.
5. Select the type of device from the **Type** field.

Note: PBC R01.04 is referred to as **PBC1**. The PBC R02.00 and later is referred to as **PBC**.

6. If selected device type is : RTR, HUB, AMS, FAF, LGP, PBC or IIW, an additional field **Device Port** is displayed with default value for user `textpass`. Enter the value of the SNMP port used by that device in this field.

Important: SNMP ports for devices of each user can be seen by executing the command `/usr/TextPass/bin/tp_manage_user --info` on the traffic element server.

7. If the device is a HUB, another field for **External IPv4 Address** appears. Enter the IPv4 address or hostname that will be used by the HUB as listen address for application protocols (SMPP, UCP and CIMD2).
8. If the device is a HUB, an additional field **External IPv6 Address** is displayed. Enter the IPv6 address or hostname; this address is used by the HUB as listen address for application protocols (SMPP, UCP and CIMD2).

Note:

HUB External Address must be unique in domain. Both external addresses will support ``empty`` string but at least one must be specified. For validation rules for IPv4/IPv6/Hostname, refer the [Configure Service Centre Nodes](#).

If the hostname is configured on HUB External Address, refer to section: [DNS Query Mechanism](#) for more details.

9. If the device is an IIW, an additional field **Primary External IP Address** is displayed. Enter the IP address or hostname; this address is used by the IIW to listen for outside SIP connections. IPv4, IPv6 and hostname address formats are supported for the IIW **Primary External IP Address** field.
10. If the device is an IIW, an additional optional field **Secondary External IP Address** is displayed. Enter the IP address or hostname; this address is used by the IIW to listen for outside SIP connections in case of SCTP only. IPv4, IPv6 and hostname address formats are supported for the IIW **Secondary External IP Address** field.
11. If the device is an AMS, additional field **QCLI Server Port** is displayed with a default value. You can modify default value if required.

Note: QCLI Server port for AMS of each user can be seen by executing the command `/usr/TextPass/bin/tp_manage_user --info` on the traffic element server.

12. If the device is an LGP, additional field **LGP Query Port** is displayed with a default value. You can modify default value if required.

Note: LGP Query port for LGP of each user can be seen by executing the command `/usr/TextPass/bin/tp_manage_user --info` on the logging element server.

13. If the device is a RTR and it should be the default router, ensure that the **Default Router** check box is selected.

Otherwise, clear the **Default Router** check box.

Note: If the user adds a new RTR device from MGR GUI, the MGR will automatically setup the FTA job for that device, which will enable transferring of list files and output files. Please refer to the DMF Operator Manual for more information about list files and output files.

14. Select the correct device release number from the **<device> Release** field.

Where **<device>** represents the type of the device as selected in the **Type** field.

15. In the **Server Name** field, select the server on which the device resides.

Note: The MGR automatically assigns the device TCP port, based on device type.

16. In the **Domain** field, select the management domain for the device (defaults to the main domain).

17. If you do not want the MGR to connect to the device under any circumstances, clear the **Allow Connection** check box.

Otherwise, ensure that the **Allow Connection** check box is selected.

18. Optionally, in the **Poller** field, select a poller for the device (as configured in **Statistics > Settings > Pollers**).

19. Click **Save**.

The MGR creates the device and closes the tab.

20. Activate the device.

IMPORTANT CONSIDERATIONS:

When adding a new device on a multi-instance setup, following restrictions shall apply.

1. Two devices of the same device type cannot be added if they have exactly the same combination for **Device Port** and **Server IP Address**.
2. Two HUB devices cannot be added on the same server if they have exactly the same combination for **External IP Address** and **Domain**.
3. Two HUB devices can be configured on the same server in a domain if they use different **External IP Address**.
4. Any two AMS devices cannot use exactly the same combination for **QCLI Server Port** and **Server IP Address**.
5. Any two LGP devices cannot use exactly the same combination for **LGP Query Port** and **Server IP Address**.
6. Two IIW devices cannot be added on the same server if they have exactly the same combination for **External IP Address** and **Domain**.
7. Two IIW devices can be configured on the same server in a domain if they use different **External IP Address**.

16.7.1.1 Add a Device That Is Not Available

If you attempt to add a device that is not available, the MGR daemon (`tp_mgrd`) returns an SNMP error to the MGR, indicating that the device is non-operational. The MGR requires that all SNMP errors from devices be resolved before further provisioning can be done.

To prevent this issue, if you know a device is offline, clear the **Allow Connection** option when you add the device. This will add the device to the configuration but prevent the MGR from sending provisioning data to the device. When the device is restarted, the MGR will apply the correct configuration to it.

Once the device is available, the **Allow Connection** option must be selected.

16.7.1.2 Clear an SNMP Error for an Unavailable Device

If a configuration change is made when a device is unavailable, you can clear the resulting SNMP error by:

1. Clearing **Allow Connection** for the device in question
2. Selecting the configuration item that was changed and re-syncing it

16.7.1.3 Device Configured Version and Component Version

Device list GUI page (**Settings** ► **Network Layout** ► **Devices**) displays the **Configured Version** and **Component Version** of the device.

- **Configured Version** => Device release version configured on MGR GUI
- **Component Version** => Component version on the target device.

You must ensure that the **Configured Version** of device is always less than or equal to **Component Version**.

16.7.2 Polling Devices

The Manager's `tp_mgr_poll` service automatically polls the devices at regular intervals to verify their operational state and component version.

16.7.3 Device States

Each device has two types of states:

- Administration state:
 - Active—The device is active (see [Activate](#)).
 - Inactive—The device has not been activated yet or was deactivated (see [Deactivate](#)).
- Operational state:
 - Active—The device is operating.
 - Not active—The device has not been activated yet or was deactivated.
 - Synchronizing—The device is waiting to synchronize with the Manager or is currently synchronizing.
 - Unknown—The MGR cannot communicate with the device.

The Devices tab shows the states of each device: the administration state in the **ST** column and the operational state in the **OS** column. It also shows the device type (**Type**), the server where the device is installed (**Server Name**), and the domain the device belongs to (**Domain**).

Devices











ST	OS	Name	Type	Server Name	Domain
		RTR	RTR	ibiza-zone2	main
		HUB	HUB	ibiza-zone2	main
		AMS	AMS	sardegna	main
		RTR1	RTR	java	AGW_D1
		HUB1	HUB	java	AGW_D1

Figure 39: Device states

Note: The operational state as shown in the MGR is not necessarily the same as the state that is shown when `tp_status` is run on the device itself.

Note: When changing the administration state of the SPFSOAP device, it is only changed on the MGR GUI. The administration state of the SOAP server is actually not changed.

The MGR logs changes to devices' administration state and operational state in **Settings** ► **Errors and Changes** ► **User Changes** and **Auto Changes**.

16.7.3.1 Example State: Active and Connected

When a device is active, connected, and in sync with the Manager, the administration state shows



and the operational state shows



16.7.3.2 Example State: Active and Synchronizing

When a device is active and synchronizing with the Manager, the administration state shows



and the operational state shows



This state can occur after an operator request or when a device missed configuration changes while disconnected. The Manager does not allow changes that affect this device while it is in this state.

16.7.3.3 Example State: Active and Disconnected

When a device is active but not connected to the Manager, the administration state shows



and the operational state shows



This state can occur when the operator sets the device to active or the device was active the last time the Manager polled it; however, the Manager cannot currently communicate with the device. When the Manager can connect to the device again, the Manager will synchronize the device with any changes that were made while communication was not possible (through the `tp_mgr_poll` service).

16.7.3.4 Example State: Inactive and Connected

When a device is inactive and connected to the Manager, the administration state shows



and the operational state shows



Although the device is inactive, the Manager can communicate with it and will keep it synchronized with any configuration changes that impact it.

16.7.4 DNS Query Mechanism

If the hostname is configured, then DNS query will be performed. Following steps explain how DNS query will be performed:

1. DNS lookup is performed for all the configured hostnames.
2. If the specific type of address that is "AAAA (for IPv6)" and "A (for IPv4)" is not found on DNS lookup, then no IP address is set for that parameter. For example:
 - a. The field "**External IPv6 Address**" (in case of HUB) requires an IPv6 address and it won't be set until an IPv6 address is returned through the DNS query
 - b. The IP address of Service center node can accept an IPv4/IPv6 address or a hostname. While doing DNS query, IPV6 address is preferred over IPv4 address.
3. The asynchronous DNS query interval is controlled by the semi-static parameter `dnsfailtimeout`. If the value of this parameter is "0", then no more DNS queries is performed.
4. As long as the DNS query does not get resolved, a log message is printed to indicate that the DNS query is not successful.
5. DNS module maintains a TTL value for the resolved hostnames. Once the TTL value expires for hostname, the DNS lookup is performed again to get the new resolved IP address.
6. If the user configures hostname which does not exist in DNS sever, then in that case there will be infinite number of DNS queries performed. To avoid this situation, a maximum of 50 DNS queries are performed.

16.7.5 Device Limitations

Use the MGR to manage the devices in your system The following table summarizes the maximum number of devices that can be configured in the MGR per domain.

Device Type	Maximum Devices
AMS	250
BAT	100
EMG	250
FAF	250
HUB	250
IIW	250
LGP	250

Device Type	Maximum Devices
PBC	250
PBC1	250
RTR	250
SPFCORE	250
SPFSMS	250
SPFSOAP	250
XSARP	32
XSBWL	32
XSCPY	32
XSDIL	32
XSFWD	32
XSSIG	32
XSINT	32

16.8 Configuring Global Settings

To configure and modify global settings:

1. In the left navigation bar, select **Settings ► Global Settings**.
The Global Settings tab appears. Next to **Master**, the host name of the master MGR appears. Next to **Slave**, the host names of the local MGRs appear.
2. In the **Maximum Open Tabs** box, set the maximum number of MGR tabs that a user can have open at one time (between 2 and 25).
3. In the **Request Timeout** box, set the number of seconds that the MGR should wait for the server to respond to a request before timing out (default is 600 seconds).
4. In the **Change Period** box, set the number of hours that the MGR should keep configuration changes in its database (default is 48 hours).
5. In the **Change File** box, set the location and name of the .txt file in which to store MGR changes (for example, /var/TextPass/tp_mgr_change_log.txt).
6. In the **Error Period** box, set the number of hours that the MGR should keep errors in its database (default is 48 hours).
7. In the **Error File** box, set the location and name of the .txt file in which to store MGR errors (for example, /var/TextPass/tp_mgr_error_log.txt).
8. Set the device polling interval, which controls how often the MGR refreshes the device overview in **Settings ► Network Layout ► Devices** (default is 60 seconds).

9. In the **Max Deactivated Devices (%)** box, set the maximum percentage of devices allowed to deactivate per device type in a domain. If you try to deactivate devices more than configured percentage, then confirmation message will be displayed on GUI.
10. Optionally, configure user-defined fields.
11. Click **Save**.

The MGR saves the settings and closes the tab.

Note: The **Max Shortcode Length** shows the maximum length of short numbers that can be assigned to applications).

16.8.1 Configuring User-Defined Fields

The MGR provides six user-defined fields to contain custom data. The user-defined fields will be added to the parameters that are available for each configuration item.

There are two types of user-defined fields:

- Short fields, which look like:



- Large fields, which look like:



16.8.1.1 Add a User-Defined Field

To add a user-defined field:

1. In the left navigation bar, select **Settings ► Global Settings**.
The Global Settings tab appears.
2. If you want to add a short field, enter its name in **Short User Defined Col. 1 Name**. If you want to define a large field, enter its name in **Large User Defined Col. 1 Name**.
3. Optionally enter help text for the field.
This text will appear when the user moves his or her mouse pointer over the field name.
4. Repeat steps 2 and 3 for each field that you want to add.
5. Click **Save**.

The Manager makes the field(s) available in all configuration items and closes the tab.

16.8.1.2 Modify a User-Defined Field

You can modify an existing user-defined field without affecting the data that has been entered in that field within any configuration item. For example, if you change the name of a field from "Comments"

to "Location Details", any data that was entered in the "Comments" field will be available in the "Location Details" field.

To modify a user-defined field:

1. In the left navigation bar, select **Settings ► Global Settings**.

The Global Settings tab appears.

2. For the field(s) that you want to modify, change the name and/or help text.
3. Click **Save**.

The MGR saves the changes and closes the tab.

16.8.1.3 Remove a User-Defined Field

To remove a user-defined field:

1. In the left navigation bar, select **Settings ► Global Settings**.

The Global Settings tab appears.

2. For the field(s) that you want to remove, completely clear the name and, if provided, the help text.

WARNING: When you remove a user-defined field, any data that has been entered in that field within any configuration item is completely removed and is not recoverable.

3. Click **Save**.

The MGR removes the field(s) and closes the Global Settings tab.

16.9 Pending Transactions

The **Pending Transactions** screen contains details of the configuration updates which are not yet synched with the devices.

The synchronization operations are queued, i.e. when one synchronization operation is already in progress and same/another user initiates another configuration update operation, then the second operation is synchronized only after the earlier synchronization gets completed.

To view the Pending Transaction(s), select **Settings ► Pending Transactions** from the left-hand navigation pane.

Index	Table	Action	IP	Device Name	Table Index
3228	listConditionTable	set	172.16.133.103	RTR2	5.2959
3229	listConditionTable	set	172.16.133.33	RTR_instance1	5.2959
3230	listConditionTable	set	172.16.133.33	RTR	5.2959
3231	listConditionTable	set	172.16.133.103	RTR2	5.2959
3232	listConditionTable	set	172.16.133.33	RTR_instance1	5.2959
3233	listConditionTable	set	172.16.133.33	RTR	5.2959
3234	listTable	set	172.16.133.33	RTR_instance1	5
3235	listTable	set	172.16.133.103	RTR2	5
3236	listTable	set	172.16.133.33	RTR	5

Figure 40: Pending Transactions

Note: In case a single configuration update operation performed on a table results in more than one pending transactions, i.e. for synching the updated configuration with multiple devices, then each such pending transaction will be displayed as a separate row on the **Pending Transactions** screen.

To view details about a particular pending transaction, click on the corresponding row in the **Pending Transactions** screen. A new tab appears with the following information:

- **Table** on which the configuration update was performed.
- Configuration **Action performed** on the corresponding device.
- **IP** on which the device is running.
- **Port** on which the device is running.
- **Device Name**, i.e. name of the device configured with MGR, as indicated on the **Settings ► Network Layout ► Devices** screen.
- **Table Index**, i.e. SNMP index of the table on which the configuration update was performed.

Table	Action performed	IP	Port	Device Name	Table Index
moRtgRuleTable	set	172.16.133.53	11161	RTR	3

Figure 41: Pending Transaction Details

16.10 Verifying Device License Information

The MGR can be used to verify device licenses by comparing them with locally stored license information. You can view local license information for all devices, or you can view specific license information for individual devices.

16.10.1 Verifying Local License Information for All Devices

To view local license information for all devices:

1. In the left navigation bar, select **Settings > Global Settings > License Overview** .
2. The Location column shows the server name (i.e. where the device is installed). The license expiration date (Expires) and the license file name (Filename) are also indicated.

If a device is running, the Hours Left column shows the number of hours left for the license. This information is retrieved from the corresponding device itself.

The status of the license (Status) is also indicated, as follows:

- Expired - the license has already expired and cannot be used any more
- Current - the license is still valid and could be used by one of the devices
- Active - the license is actually being used by one of the devices

16.10.2 Verifying Device-Specific License Information for Each Device

To view the device-specific license information that is read from each device:

1. In the left navigation bar, select **Settings ► Network Layout ► Devices**.

The **Devices** tab appears.

2. Click the device name in the **Devices** tab to select a device.
On the selected device screen, License Expiry indicates the number of hours of operation that a running device license has left (refer to the Hours Left column in the Global License Overview settings). Information in the License Number and License Issue Number fields identify the license file being used by the selected device (refer to the Filename column in the Global License Overview settings).

16.11 Customising the Application Password Generator

The HUB supports password authentication for SMS applications. The MGR's application password generator can generate passwords for SMS applications, based on customisable settings.

Interface Type:	▼	UCP	▼
Session Model:	▶	Use Service Class Model	▼
Outside Authentication Method:	▶	<input checked="" type="checkbox"/> 1 - Password Authentication <input type="checkbox"/> 2 - CLI Authentication <input type="checkbox"/> 3 - One OR the other (not both)	
Outside UCP Password:	▶	<input type="text"/>	← GEN PW
Inside Authentication Method:	▶	<input checked="" type="checkbox"/> 1 - Password Authentication	
Inside UCP Password:	▶	<input type="text"/>	← GEN PW
Inside UCP Window Size:	▶	100	

Figure 42: Password generation buttons

To customise the settings for the application password generator:

- In the left navigation bar, select **Settings ► Application Password**.
The Application Password Generator Settings tab appears.
- Set the following properties:
 - Description**—An optional description of the application password generator.
 - Total Password Minimum**—The minimum length of the passwords that will be generated for applications.
 - Total Password Maximum**—The maximum length of the passwords that will be generated for applications.
 - Character Set 1, 2, and 3**—Up to three sets of characters to use to generate passwords.

For each character set that you create, set the minimum and maximum numbers of characters to use from the set.

Character Set 1:	✓	abcdefghijklmnopqrstuvwxyz
Minimum:	✓	1
Maximum:	✓	20
Character Set 2:	✓	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Minimum:	✓	1
Maximum:	✓	20
Character Set 3:	✓	1234567890
Minimum:	✓	1
Maximum:	✓	5

Figure 43: Customised character sets

- Minimum Application Password Length**—The overall minimum required length for application passwords. Set this property to 0 (zero) to allow empty passwords.

Note: The minimum application password length must be set to 0 (zero) when you are using the HUB's learning mode (which applies to UCP applications). Refer to the HUB Operator Manual for information about learning mode.

3. Click **Save**.

The MGR saves the application password generator changes and closes the tab.

16.12 Configure CCI Properties

1. In the left navigation bar, select **Settings > CCI > Properties**.

The Customer Care Properties tab appears.

Customer Care Properties

Search All Domains:	<input type="checkbox"/>
Max Open Tabs:	16
SMSC IP Address:	127.0.0.1
SMSC Port Number:	2275
Message Type:	SMPP
System ID:	anonymous
System Type:	SMPP
Password:	*****
Source Address:	1234
Message Text:	test message
Last Updated:	2011-Aug-31 11:37:17 CEST

Figure 44: Customer Care Properties

- Normally, the CCI will only search for messages that are in the domain where the user is currently logged in. If the CCI should be allowed to search messages in all domains, select **Search All Domains**.
- In the **Max Open Tabs** box, enter the maximum allowed number of open tabs in the CCI.
Note: If this parameter is changed you must either log-out and log back into the CCI GUI or restart the CCI for the change to take effect.
- In the **SMSC IP Address** box, enter the destination IP address that the CCI should use when sending a test message to a subscriber.
- In the **SMSC Port Number** box, enter the destination port number that the CCI should use when sending a test message to a subscriber.
- From the **Message Type** list, select the protocol that the CCI should use when sending a test message to a subscriber:
 - SMPP
 - UCP
- If the message type is SMPP:

- a) Enter the system ID to use in the SMPP bind message in the **System ID** box.
- b) Enter the system type to use in the SMPP bind message in the **System Type** box.
8. If the message type is UCP, enter the short code to use in the UCP 60 log-in message in the **Short Code** box.
9. In the **Password** box, enter the password that the CCI should use when establishing a session to send a test message to a subscriber.
10. In the **Source Address** box, enter the address that should appear as the originator address when the CCI sends a test message to a subscriber.
11. In the **Message Text** box, enter the text that the CCI should use in test messages sent to subscribers.

Chapter 17

Statistics

Topics:

- *Introduction.....388*
- *Types of Statistics.....388*
- *Configuring Statistics Settings.....391*

17.1 Introduction

When your system includes the Statistics Viewer (STV), you can view detailed, real-time statistics about the traffic in the system.

17.2 Types of Statistics

The following types of statistics are available:

Type	Statistics
System	<ul style="list-style-type: none"> • Overview • Processes • Storage <p>Double-click a system to view additional information about it.</p>
Incoming traffic	<ul style="list-style-type: none"> • Total MO • Country MO • Network MO • Application AO/MT
Outgoing traffic	<ul style="list-style-type: none"> • Total MT • Country MT • Network MT • Application MO/AT • SMSC • Country SMSC • Network SMSC • HLR • SRISM
Through traffic	<ul style="list-style-type: none"> • Total AO/AO • Total AT/AT • Application AO/AO • Application AT/AT
Inside traffic	<ul style="list-style-type: none"> • Application sessions • Application AO • Application AT • Recipient country AT • Recipient network AT

Type	Statistics
	<ul style="list-style-type: none"> Termination point AO Termination point AT Node AO Node AT Service centre AO Service centre AT
Outside traffic	<ul style="list-style-type: none"> Application sessions Application AO Application AT Recipient country AT Recipient network AT
Detected violations	<ul style="list-style-type: none"> Detected MO violations Detected MT violations Detected SRI violations
Unexpected traffic	<ul style="list-style-type: none"> Total TCAP Country TCAP Network TCAP
Rules	<ul style="list-style-type: none"> Routing rules (MOR, MTIR, MTOR, AOR, ATIR, ATOR) Counting rules (MOC, MTIC, MTOC, AOC, ATIC, ATOC) External condition rules (MOX, MTIX, MTOX, AOX, ATIX, ATOX)
Performance	<ul style="list-style-type: none"> License Usage SS7 Usage <p>Double-click a device in the SS7 usage table to view the SS7 linkset usage for the device. Double-click a linkset to view the SS7 link usage for the combination of that device and linkset.</p>
Advanced Filters (if FAF is installed and licensed)	<ul style="list-style-type: none"> ECI connections Filters Conditions <p>Double-click a filter to view the conditions of the filter.</p>
AMS (if installed and licensed)	<ul style="list-style-type: none"> Queues Message store Transaction store

Type	Statistics
IPSMGW (if IIW is installed and licensed)	<ul style="list-style-type: none"> • Total SIP MO • Total SIP MT • HSS Sh Interface • SIP Register • Subscribe • Notify • Sip Application <ul style="list-style-type: none"> • Incoming <ul style="list-style-type: none"> • Message • Info • Outgoing <ul style="list-style-type: none"> • Message • Info • Sip Listener <ul style="list-style-type: none"> • Incoming <ul style="list-style-type: none"> • Message • Info • Register • Notify • Outgoing <ul style="list-style-type: none"> • Message • Info • Subscribe
PBC R01 (if installed and licensed)	<ul style="list-style-type: none"> • ECI connections • Attribute filters • Diameter (requests and results)
PBC R02 (if installed and licensed)	<ul style="list-style-type: none"> • ECI connections • Scripts • Diameter • Database
EMG (if installed and licensed)	<ul style="list-style-type: none"> • Session management • Incoming SMS • SMS2Email

Type	Statistics
	<ul style="list-style-type: none"> • Outgoing email • SMS response
Other	<ul style="list-style-type: none"> • Status reports • External condition (EC) failures

Refer to the STV Operator Manual for detailed information about available statistics.

17.3 Configuring Statistics Settings

You can configure polling and data retention intervals, create pollers for devices, and adjust what data is collected from each type of device.

17.3.1 Set Polling Intervals

By setting the polling intervals you set the sample rate. There are three types of polling intervals:

- Very fast
- Fast
- Normal

When you adjust the data that is collected from each device in **Polling Groups**, you can select one of these intervals for each polling group.

To customise the polling intervals:

1. In the left navigation bar, select **Statistics** ► **Settings** ► **Polling Intervals**.
The Polling Intervals tab appears.
2. Set the following polling intervals:
 - **Very Fast PI**—1 (default) or 5 minutes
 - **Fast PI**—5 (default) or 15 minutes
 - **Normal PI**—15 minutes or 1 hour (default)
3. Click **Save**.
The MGR saves the changes and closes the tab.

17.3.2 Set Data Retention Intervals

To set the data retention intervals:

1. In the left navigation bar, select **Statistics** ► **Settings** ► **Data Retention**.
The Data Retention Intervals tab appears.
2. Set the following data retention intervals:

- **Full Resolution Data**—Number of days to retain the data from all counters
 - **15 Minutes Aggregates**—Number of days to retain the data from the 15-minute aggregate counters
 - **Hourly Aggregates**—Number of days to retain the data from the hourly aggregate counters
3. Click **Save**.
The MGR saves the changes and closes the tab.

17.3.3 Create Pollers

Prerequisites:

- Domain

Pollers collect data from the devices. To create a poller:

1. In the left navigation bar, select **Statistics** ► **Settings** ► **Pollers**.
The Pollers tab appears.
2. Click **Add New**.
3. Enter a unique name for the poller in the **Name** box.
4. Enter the host name of the device from which this poller will collect data in the **Hostname** box.
5. Select the domain in which the device resides from the **Domain** list.
6. Click **Save**.
The MGR creates the poller and closes the tab.
7. Activate the poller.

17.3.4 Filter System Processes

To filter the system processes that appear in the system health statistics:

1. In the left navigation bar, select **Statistics** ► **Settings** ► **Process Filters**.
The Process Filter tab appears.
Note: By default, the MGR includes processes that are commonly of interest.
2. Click **Add New**.
A new Process Filter tab appears.
3. Enter the name of the process in the **Name** box.
Note: You can add names that are not valid processes, but they will not appear in the system health statistics.
4. Click **Save**.
The MGR adds the process and closes the tab.

17.3.5 Customise Polling Groups

You can set different polling intervals (sample rates) for different polling groups within each device. You can also disable polling for certain polling groups.

17.3.5.1 AMS Polling Groups

For each of the following AMS polling groups, select **Do not poll** or select a polling interval:

- Storage per Application
- Storage Duration
- Queues
- Throughput
- Queue Storage
- Queue Throughput
- Transaction Storage

17.3.5.2 EMG Polling Groups

For each of the following EMG polling groups, select **Do not poll** or select a polling interval:

- Session Management
- Incoming SMS
- Sms2Email Conversion
- Outgoing Email
- SMS Response

17.3.5.3 FAF Polling Groups

For each of the following FAF polling groups, select **Do not poll** or select a polling interval:

- ECI Connections
- Filters
- Conditions

17.3.5.4 HUB Polling Groups

For each of the following HUB polling groups, select **Do not poll** or select a polling interval:

- Inside AO Application Traffic
- Inside AT Application Traffic
- Outside AO Application Traffic
- Outside AT Application Traffic
- Application Inside Sessions
- Application Outside Sessions
- Inside SC Termination Point Traffic
- Combined Application Traffic

17.3.5.5 IIW Polling Groups

For each of the following IIW polling groups, select **Do not poll** or select a polling interval:

- Sip Transaction Received from CSCF
- Sip Transaction Sent to CSCF
- HSS Sh Interface
- Register Request from IMS Network
- Subscribe
- Notify
- Sip Application
- Sip Listener

17.3.5.6 PBC1 Polling Groups

For each of the following PBC R01.xx polling groups, select **Do not poll** or select a polling interval:

- ECI Connections
- Attribute Filters
- Diameter Requests
- Diameter Results

17.3.5.7 PBC Polling Groups

For each of the following PBC R02.xx polling groups, select **Do not poll** or select a polling interval:

- ECI Connections
- Scripts
- External Variables
- Diameter Queries
- Diameter Result Codes
- Database

17.3.5.8 RTR Polling Groups

For each of the following RTR polling groups, select **Do not poll** or select a polling interval:

<ul style="list-style-type: none"> • Total MO Traffic • Total MT Traffic • Total MT-AT Traffic • Total AO-AO Traffic • Total AT-AT Traffic • Total AT-AO Traffic • Total AT-Store-AO • Total AT-AO-Store • Combined SM Traffic • MO Routing Rules • MTI Routing Rules 	<ul style="list-style-type: none"> • Application AO-AO Traffic • Application AT-AT Traffic • Application AT-AO Traffic • Application AT-Store-AO Traffic • Application AT-AO-Store Traffic • Country MO Traffic • Country MT Traffic • Country MT-AT Traffic • Network MO Traffic • Network MT Traffic • Network MT-AT Traffic
--	---

<ul style="list-style-type: none"> • MTO Routing Rules • AO Routing Rules • ATO Routing Rules • ATI Routing Rules • IGM Routing Rules • MO Counting Rules • MTI Counting Rules • MTO Counting Rules • AO Counting Rules • ATO Counting Rules • ATI Counting Rules • IGM Counting Rules • MO External Rules • MTI External Rules • MTO External Rules • AO External Rules • ATO External Rules • ATI External Rules • IGM External Rules • Application AO-MT Traffic • Application MO-AT Traffic • Network SRISM Traffic 	<ul style="list-style-type: none"> • MO Violations • MT Violations • SRI Violations • SMSC Traffic • Country SMSC Traffic • Network SMSC Traffic • Unknown SMSC Traffic • HLR Traffic • Status Reports • License Usage • SS7 Usage • M3UA Usage • Recipient Country/App AT Traffic • Recipient Network/App AT Traffic • External Condition Messages • SSI Requests • Unexpected TCAP Traffic • Unexpected Country TCAP Traffic • Unexpected Network TCAP Traffic • Home Routing • Signature • Country SRISM Traffic
---	---

Note:

1. All unexpected TCAP polling groups must be polled at the same interval.
2. The polling group "Home Routing" is obsolete. The counters of this polling group have been replaced by SRISM rules. Set this polling group to "Do not poll", to avoid the below error(s) in the stv_poller process:

```
SNMP error: StatView::Error::SNMP: get(mtScramblingCountSuspect.1): (noSuchName)
There is no such variable name in this MIB.
```

17.3.5.9 SPFCORE Polling Groups

For each of the following SPF Core polling groups, select **Do not poll** or select a polling interval:

- Subscribers Per SPF Profile
- Subscribers Per SPF Service
- Contacts
- Contact Groups
- Rules Per Service

17.3.5.10 SYS Polling Groups

For each of the following system health (SYS) polling groups, select **Do not poll** or select a polling interval:

- System Processes

- System Storage
- System Memory
- System Networks

Note: All system health polling groups must be polled at the same interval.

17.3.6 Configuring Export Streams

Export Streams enables you to generate statistical data reports for use with third-party analysis tools.

17.3.6.1 Create Export Streams

To create export streams:

1. In the left navigation bar, select **Statistics** ► **Settings** ► **Export Streams**. The **Export Streams** tab appears.
2. Click **Add New**.
A new **Export Stream** tab appears.
3. Enter a unique name for the profile in the **Name** box (maximum 31 characters).
4. Select the **Transfer Protocol** that the **Export Stream** will use to transfer the generated report.
Allowed Values:
 - RSync/SSH
 - FTP
 - SFTP

The default is RSync/SSH.

Note: To be able to use SSH or SFTP, you will need to exchange ssh keys with the other systems. Use the `/usr/TextPass/bin/fta_copy_keys` tool to do this. If this has already been done for STV poller usage, this step may be skipped. For FTP usage, an FTP server, and corresponding users need to be set up beforehand.

Note: Unsecured protocols such as FTP and telnet may introduce security risk to your network. The customers are at their own risks if the unsecured protocols are enabled and used on their systems.

5. In the **Username** box, enter the username to use when connecting via FTP or SFTP.
This field will appear only if Transfer Protocol is FTP or SFTP.
6. In the **Password** box, enter the password to use while connecting via FTP.
This field will appear only if Transfer Protocol is FTP.
7. In the **Timestamp Format** box, enter the timestamp format to use in report files (defaults to `%y%m%d %H:%M`).

Use the following case-sensitive variables to construct the **Timestamp Format**:

Variable	Description
%Y	Year formatted with four digits (for example, 2012)
%y	Year formatted with two digits (for example, 12)

Variable	Description
%m	Month formatted with two digits (for example, 01 for January and 10 for October)
%d	Day formatted with two digits (for example, 01 for the first day of May and 31 for the last day of May)
%H	Hour in 24-hour time format
%M	Minutes
%S	Seconds

8. In the **Header 1** through **Header 5** boxes, specify text that will be added as extra headers in each file.
9. In **Quote Space** field, specify whether spaces should be quoted if the export tool finds white space in a field. The default value is 'yes'.
10. In **Column Separator** field, specify which character to use as delimiter between columns.

Allowed values:

- Tab
- Space
- Other character

The default is tab.

11. In **End Of Line** field, specify which character to use as end of line in report file.

Allowed values:

- Unix Style: \n
- Windows Style: \r\n
- Apple Style: \r
- Other character

Default is \n

12. In the **Filename Template** box, enter the template to use to name the report files (defaults to %Y%m%d_%H%M%S_%3.dsv).

Use the following case-sensitive variables to construct the report file name format:

Variable	Description
%Y	Year formatted with four digits (for example, 2012)
%y	Year formatted with two digits (for example, 12)
%m	Month formatted with two digits (for example, 01 for January and 10 for October)

Variable	Description
%d	Day formatted with two digits (for example, 01 for the first day of May and 31 for the last day of May)
%H	Hour in 24-hour time format
%M	Minutes
%S	Seconds
%h	Host name
%1	One-digit sequence number
%2	Two-digit sequence number
%3	Three-digit sequence number
%4	Four-digit sequence number
%5	Five-digit sequence number
%6	Six-digit sequence number
%7	Seven-digit sequence number
%8	Eight-digit sequence number

13. In the **Export to IP** box, enter the IP address of the destination server to transfer the generated reports.
14. In the **Finished Directory** box, enter the full path in which to store the report files on destination server (defaults to `/var/TextPass/STV/export/reports/`).
15. In the **Period** box, select the period for which to combine the data in one file.
Allowed values:
- Hour
 - Day
 - Week
 - Month
 - Year
- The default is Hour.
16. In the **Granularity** box, select the interval to be presented in the Export File.
Allowed values:
- 1m : One minute
 - 5 m : Five minutes
 - 10 m : Ten minutes
 - 15 m : Fifteen minutes
 - 1 h: One hour
 - 4 h : Four hours
 - 12 h: Twelve Hours

- 1 D : One day
- 7 D (week) : One calendar week
- 28 D (calendar month) : One calendar month
- 90 D (quarter): One quarter
- 365 D (year): One year

The default is 5 minutes.

Note: The **Granularity** value should not be higher than **Period** value.

17. In **Static Column Content** field, enter the value to fill in on each row of the Static Column. **Static Column Content** will be added in report only if Static Column is selected in Polling Group counters.
18. In **Polling Group** field, select a group of Counters to export in report. On selection of **Polling Group** from list, a list of **Counter Columns** that are supported for selected polling group will be displayed.

This is a sample of counter groups for **AO Counting Rules** Polling Group.

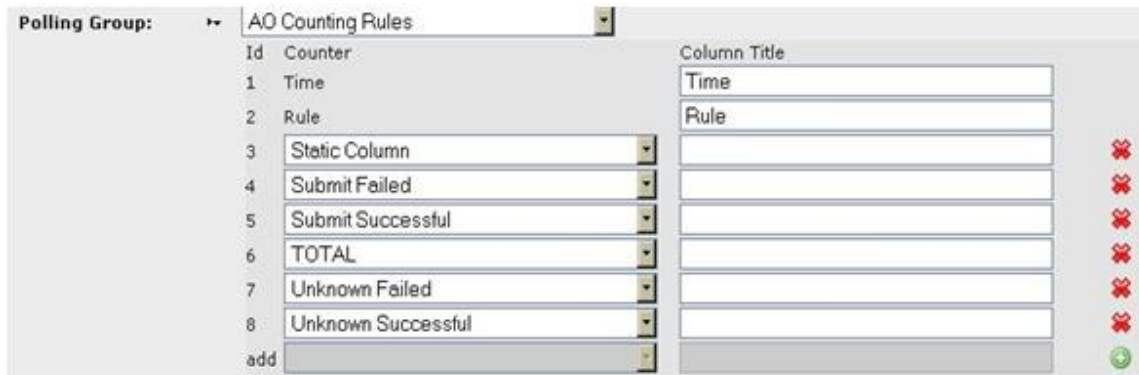


Figure 45: Sample add/remove counter from Polling Group

To remove a counter from list, click



button in counter row.

To add a counter from the list,



in last row of polling group counters.

Note: The list of **Polling Groups** is populated from the currently installed STV build. To know the complete list of supported **Polling Groups** and **Column Counters**, please refer to the STV Operator Manual.

17.3.6.2 Export Stream States

Each Export Stream has two types of states:

- Administration state
 - Active : The export stream is active

- Inactive: The Export Stream has not been activated yet or was deactivated
- Operational State
 - Active: The export stream is operational.
 - Inactive: The Export Stream has not been activated yet or was stopped due to error in transferring reports.
 - Pending: The Export Stream report transfer to destination server is in progress.
 - Unknown: The MGR cannot get the operational state of Export Stream.

The Export Stream tab shows the states of each Export Stream: the administration state in the **ST** column and the operational state in the **OS** column. It also shows the Polling Group and Last updated time.

Statistics Export Streams						
ID	ST	OS	Name	Polling Group	Last Updated	
1			RSync	HubApplicationTrafficTable	2012-06-14 06:56:11	
2			FTP	HubApplicationTrafficTable	2012-06-14 06:56:50	
3			SFTP	RtrApplicationsAtAoTable	2012-06-14 06:57:16	

Figure 46: Example Export Stream State

17.3.6.2.1 Example State: Active and Operating

When the Export Stream is active, generating reports and successfully transferring reports to the destination server, the administration state shows and



the operational state shows



17.3.6.2.2 Example State: Active and Pending

When the Export Stream is active, generating reports and report file transfer is in progress, the administration state shows



the operational state shows



17.3.6.2.3 Example State: Active and Inactive

When the Export Stream is active, generating reports but not able to transfer the reports to the destination server due to errors, the administration state shows



and the operational state shows



Note: Operating state is changed to Inactive after the number of retries to transfer reports to the destination server exceeds the value of the "max_retries" value in /usr/TextPass/etc/mgr.cnf on the MGR server. If the "max_retries" value in /usr/TextPass/etc/mgr.cnf is set to -1 then the Export Stream status is never changed to Inactive by the export process.

17.3.6.2.4 Example State: Inactive and Inactive

When the Export Stream is inactive the administration state shows

—

and the operational state shows

X

. No reports are generated or transferred in this state.

17.3.6.3 Viewing Export Stream Status

To view the operational state of each Export Stream, go to **Statistics** ► **Settings** ► **Export Status** in the MGR Web interface. The view shows the operational status of Export Stream.

STV Export Stream Status

Status	Job Name	Last Updated	Next Scheduled Time
✓	RSync	2012-06-18 12:48:32	2012-06-18 12:53:32
▶	FTP	2012-06-18 12:52:27	2012-06-18 12:52:26
X	SFTP	2012-06-14 07:03:41	2012-06-14 07:03:41

Figure 47: Example Export Stream Status

To see the detailed view of Export Stream, double click on Export Status table row. STV Export Stream Status Detail Web interface will display the status of last 50 cycles.

STV Export Stream Status Detail

Source Filename	Destination Filename	Job Status	Job Error
FTP_hatteras-vm1_201...	FTP_hatteras-vm1_201...	✓	
FTP_hatteras-vm1_201...	FTP_hatteras-vm1_201...	✓	
FTP_hatteras-vm1_201...	FTP_hatteras-vm1_201...	✓	
FTP_hatteras-vm1_201...	FTP_hatteras-vm1_201...	!	Could not setup FTP connection to 127.0...
FTP_hatteras-vm1_201...	FTP_hatteras-vm1_201...	!	Could not setup FTP connection to 127.0...

Figure 48: Example detailed Export Stream Status

To see the complete Source filename, Destination filename or Job Error of a particular record, hover the mouse pointer over the row.

Chapter 18

Command-Line Tools and Scripts

Topics:

- *Introduction*.....404
- *tp_app_throughput*.....404
- *clean_mgr_error_logs*.....405
- *tp_auth*.....405
- *tp_configure_dmf*.....407
- *tp_install_mgr*.....408
- *tp_master*.....411
- *tp_mgr_backup*.....412
- *tp_mgr_domain_sharing*.....413
- *tp_mgr_ecmessage_import*.....414
- *tp_mgr_poll*.....415
- *tp_mgr_restore*.....416
- *tp_mgr_start*.....417
- *tp_mgr_stop*.....417
- *tp_mgr_table_migration*418
- *tp_role*.....420
- *tp_shell*.....421
- *tp_slave*.....427
- *tp_update_mgr_device*.....427

18.1 Introduction

This chapter describes the command-line tools and scripts that work with the MGR.

All tools and scripts return 0 on success and 1 on failure, unless otherwise stated in the description of the tool or script.

For information about other Mobile Messaging tools, refer to the Tools Operator Manual.

Note: Many of these tools require an in-depth knowledge of NewNet Mobile Messaging components. They should therefore be used with care, and only when required.

18.2 tp_app_throughput

The `tp_app_throughput` command-line tool shows the throughput of different applications in the MGR (total number of messages since the last HUB restart). In continuous mode (`-c` option), each additional report shows the average number of messages per second since the last report.

Note: If, while in continuous mode, data collection takes longer than the configured interval (`-t` option), the results may not be accurate. This condition can occur if the system is slow and/or if there are several thousand applications configured.

18.2.1 Synopsis

```
tp_app_throughput [ options ]
```

```
tp_app_throughput -d=<domain> -t=<interval> -a=<applications> -c
```

18.2.2 Options

Option	Description
-t	Interval time (optional); default is 10 seconds.
-d	Domain indication (optional); default is 0 (indicates all domains).
-a	Comma-separated list of short codes of applications to monitor (optional); default is "all".
-c	Indicates continuous mode.
-h	Displays the help message.
-?	
--help	

18.2.3 Operands

Operand	Description
domain	Domain to monitor.
interval	Interval to monitor.
applications	Short code(s) of applications to monitor.

18.3 clean_mgr_error_logs

The MGR creates log files via Apache which are rotated daily. A script and a crontab entry to clean up these log files (10 log files are preserved) are available.

The log files to clean up are:

- /var/TextPass/MGR/logs/mgr_error_log.*
- /var/TextPass/MGR/logs/mgr_ssl_request_log.*

The clean up script is: /usr/bin/clean_mgr_error_logs.pl.

The scheduling is done by /etc/cron.daily/clean_mgr_error_logs.

18.4 tp_auth

The tp_auth command-line tool allows for management of users. tp_auth can be used on the command line or as a shell.

18.4.1 Synopsis

```
tp_auth show
```

```
tp_auth add -n=<name> -g=<group> [ -p=<password> -d=<desc> -D=<domain> ]
```

```
tp_auth set -n=<name> -g=<group> [ -p=<password> -d=<desc> ]
```

```
tp_auth reset -n=<name> -g=<group>
```

```
tp_auth activate -n=<name>
```

```
tp_auth deactivate -n=<name>
```

```
tp_auth delete -n=<name>
```

18.4.2 Commands

Option	Description
show	Shows an overview of all active and inactive users.

Option	Description
add	<p>Adds a new user. The name and group are mandatory. If the password is not specified, the user can log in to the Manager by leaving the password box empty.</p> <p>The user can only be assigned to a log-in domain if a password is specified. If a password is not specified, the user is assigned to domain 1, the main domain.</p>
set	Changes a user's group, description, or password. The log-in name is mandatory.
activate	Activates the indicated account.
deactivate	Deactivates the indicated account.
delete	Deletes the indicated account.
reset	<p>Resets a group or a single user account.</p> <p>Resetting a single user will:</p> <ul style="list-style-type: none"> • Replace the password with an empty password • Activate the user account <p>Resetting a group will:</p> <ul style="list-style-type: none"> • Change the privileges of the group • Allow all user management privileges for the main domain • Allows the My Preferences functionality <p>If the group does not exist, it will be created. Any account that is part of that group can modify all user privileges in the interface.</p>

18.4.3 Options

Option	Description
--name -n	Sets the log-in name of the user (mandatory except for the show command).
--group -g	Sets the user group (mandatory for the add command).
--password -p	Sets the user password (mandatory for the add command).
--description -d	Sets the user description (optional).

Option	Description
--domain -D	Sets the default log-in domain for the user.
-h -? -m --help --man	Displays the help message.

18.4.4 Operands

Operand	Description
name	Log-in name of the user.
group	Name of the user group.
password	User's new password in plain text.
desc	Description for the user.
domain	Log-in domain for the user.

18.4.5 Sample Usage

The following command creates a new user with an ID of newadmin and a password of admin123, in the Administrators user group, with a default log-in domain of 2:

```
tp_auth add -n="newadmin" -p="admin123" -g="Administrators" -D=2
```

The following command changes the description for the existing account for the user with the ID tester:

```
tp_auth set --name="tester" --description="Account is blocked"
```

The following command removes the account of the user with the ID john:

```
tp_auth delete -n="john"
```

The following command activates the account of the user with the ID john:

```
tp_auth activate -n="john"
```

18.5 tp_configure_dmf

This utility configures FTA jobs for file transfer. Script adds the FTA jobs for the transfer of the list and the output files between the Traffic Element and the OAM Element. Please refer to the DMF Operator Manual for more information about list files and output files.

On deletion of the RTR device from the MGR, the FTA configuration associated to that device gets removed automatically.

18.5.1 Synopsis

```
tp_configure_dmf --help
tp_configure_dmf --verbose
tp_configure_dmf --re_configure
tp_configure_dmf --reset_scheduling
```

18.5.2 Options

Option	Description
--verbose -v	Prints more detailed status messages.
--re_configure -r	Reconfigures all the FTA jobs for DMF.
--reset_scheduling -s	Resets the next schedule interval for all the FTA jobs for DMF.
--help -h -?	Displays the help message.

Note: Before running `tp_configure_dmf`, it is necessary to create SSH-less connections from the user `textpassdmf` on the OAM Element to the user `textpassdmf` on the Traffic Element.

18.6 tp_install_mgr

The `tp_install_mgr` command-line tool allows you to install new devices or to upgrade existing ones.

18.6.1 Options

Option	Description
--check -c	Displays the current configuration.

Option	Description
--export -e	Exports the current device version to a file (requires -f).
--filename -f	File name to use for importing or exporting device configuration. ¹
-h -? --help	Displays the help message.
--role -r	The Manager role (master or slave). ²
--shortcodelength -s	The maximum short code length (default is 5). ²
--username -u	The user name to access the database. ²
--password -p	The password to access the database. ²
-hostname -H	The host name of the database server. ²
--portnumber -P	The port number of the database. ²
--all -A	The MGR will upgrade and install all components. ¹ Note: The version is limited to the configured devices. Those must be upgraded first.
--upgrade_all -U	The MGR will upgrade all installed components. ¹ Note: The version is limited to the configured devices. Those must be upgraded first.

1. The options --filename, --all, and --upgrade_all are mutually exclusive.
2. If you do not provide these options, the Manager attempts to use previously configured data.

18.6.2 Upgrade Process

The general upgrade procedure for a working network is:

1. Upgrade the devices, one by one.

The Manager will manage the devices, but new features will not be available yet.

2. Use `tp_install_mgr` to upgrade the Manager.

This step will enable new features, reapply the license, and updates the database. The tool will create backups of the configuration files and database. In case of failure, the old configuration file and database can be restored.

18.6.3 Usage

18.6.3.1 Verifying Current Configuration

To verify the current configuration, use the `--check` option. The tool will list the available devices with their current version number (or "not installed"). The tool will then exit without making modifications to the running system.

18.6.3.2 Exporting Current Configuration

To export the current configuration, use the `--export` option. You must specify a file name using the `-f` option. The tool will write the current device configuration to the file, which can be used in other installations. The tool will then exit without making modifications to the running system.

18.6.3.3 Manual Installation

If you do not specify the `-f` option, the tool will work in manual mode. The installer will display the installed device types and versions and a selection of available device types. Select a device by pressing the number corresponding to the type. Then, select a version to install or to upgrade to. Press 0 to return to the previous selection. After you have selected the desired version(s), press 0.

No changes are done without confirmation.

Note: `tp_install_mgr` does not check available nodes. You must ensure that the selected versions match the devices. If an exact device is not available, select the closest version (but never a higher version).

18.6.3.4 Non-Interactive Installation

If you specify the `-f` option to perform an installation, the tool will work in non-interactive mode. This mode requires that:

1. The specified file contains valid installation data
2. All information (such as database settings, short code length, and Manager role) must be provided at the command prompt

18.6.4 File Format

When you use the tool in non-interactive mode, the file containing the installation data should be formatted with the device abbreviation, a colon, and a version number. For example:

```
AMS:R01.02.00.00
STV:R04.03.02
FAF:R02.01.00.01
HUB:R04.01.11.01
LGP:R01.03.00.00
RTR:R04.01.14.07
```

`tp_install_mgr` will check the devices for validity and compatibility. If a matching version is not found, the tool will select the next best match. If the version specified is `R00.00.00.00`, `tp_install_mgr` will remove the device from the database.

18.7 `tp_master`

`tp_master` is an internal command to start the Manager in master mode. It returns 0 upon success.

18.7.1 Synopsis

```
tp_master --clean
```

```
tp_master --noclean
```

```
tp_master -?
```

18.7.2 Options

Option	Description
--clean -c	This option will remove all pre-created files from the MGR cache directory. This somewhat slows down MGR startup, but ensures fresh copies are created after actions like license changes. This is the default option.
--noclean -n	This option will skip the cleaning of the MGR cache directory. This may speed up the MGR start but the MGR will not accept changes in licenses or device versions.
--help -h -?	Print this help message and exits.

18.8 tp_mgr_backup

The `tp_mgr_backup` command-line tool creates a backup of the Manager configuration using `mysqldump`. `tp_mgr_backup` creates the backup file and compresses it.

Use `tp_mgr_restore` to restore a Manager configuration. Refer to [tp_mgr_restore](#) for more information.

18.8.1 Synopsis

```
tp_mgr_backup -mysql_path=<path to binaries> -name=<backup file name>
```

```
tp_mgr_backup -name=<backup file name> -verbose
```

18.8.2 Options

Option	Description
<code>-verbose</code>	Provides progress statements during the backup procedure (optional).
<code>-mysql_path</code>	Specifies the path to the MySQL binaries (optional). <code>tp_mgr_backup</code> assumes that the MySQL binaries <code>mysql</code> and <code>mysqldump</code> are in the path. This option allows you to specify the specific path.
<code>-name</code>	Specifies the path to and name of the backup file (optional). <code>tp_mgr_backup</code> creates a single backup file. The name is taken from the optional <code>-name</code> option. The default name is <code>/var/TextPass/MGR/backup/mgr_databases.sql</code> . To guarantee uniqueness a date string is appended. If the file is compressed, the full name will be <code>.gz</code> .
<code>-help</code> <code>-?</code> <code>-man</code>	Displays the help message.

18.8.3 Operands

Option	Description
<code>path to binaries</code>	Path to the MySQL binaries (defaults to the current path).
<code>backup file name</code>	Name of the backup file (defaults to <code>/var/TextPass/MGR/backup/mgr_databases.sql</code>). To guarantee uniqueness, <code>tp_mgr_backup</code> appends a date string to the file name.

18.8.4 Example

The following example command:

```
tp_mgr_backup -name=/tmp/
```

Creates the file `/tmp/mgr_databases.sql_2007_12_13_15_41_00.gz`.

18.9 tp_mgr_domain_sharing

The MGR can control multiple Mobile Messaging networks, which are called domains. Some configuration items can be shared from the MGR's default domain, which is called main. You configure sharing when you add a new domain. The `tp_mgr_domain_sharing` command-line tool enables you to change the sharing configuration so that the setting for applications is **Not Shared: Copy all from Main (existing and new)**.

Changes that are made using `tp_mgr_domain_sharing` do not take effect until the MGR has been restarted.

CAUTION: Changing the sharing configuration has a severe impact on the configuration of devices.

18.9.1 Synopsis

```
tp_mgr_domain_sharing
```

```
tp_mgr_domain_sharing --help
```

```
tp_mgr_domain_sharing --version
```

```
tp_mgr_domain_sharing [-v] [-q] -c --domain=<domainname> --table=<table>
```

18.9.2 Options

Option	Description
--help -h -?	Prints a help message and exits.
--version -V	Prints version info and exits.
--verbose -v	Prints more detailed status messages.
--quiet -q	Suppresses normal output.

Option	Description
--domain -d	The name of the domain for which to change the sharing.
--table -t	Name of the table for which the sharing will be changed. Currently only applicationTable is supported.
--copy -c	From now on, copy every new element from the specified table into the specified domain.

18.9.3 Example

The following example will make sure that from now on, all the applications that are added to the main domain, are copied to the domain called agw_domain:

```
tp_mgr_domain_sharing -c -d agw_domain -t applicationTable
```

18.10 tp_mgr_ecmessage_import

The `tp_mgr_ecmessage_import` command-line tool imports old external condition (EC) message definitions from a host-specific configuration file, into the Manager database. The messages are then editable in **Routing** > **EC Applications** > **Messages**.

18.10.1 Synopsis

```
tp_mgr_ecmessage_import --help
```

```
tp_mgr_ecmessage_import --version
```

```
tp_mgr_ecmessage_import [-v] [-q] [--domain=<domain name>] --tp_config=<file name>
```

18.10.2 Options

Option	Description
--version -v	Displays the version information and exits.
--verbose -v	Provides progress statements during the backup procedure (optional).
--quiet -q	Suppresses normal output.

Option	Description
--domain -d	Specifies the domain to which to import the messages (defaults to main).
--tp_config -t	Specifies the name of the host-specific configuration file to parse. All items marked <code>externalconditionfailuremessage</code> or <code>defaultexternalconditionfailuremessage</code> will be parsed and imported.
-h --help -?	Displays the help message.

18.11 tp_mgr_poll

The `tp_mgr_poll` script keeps track of configuration changes in the Manager, keeps the MGRdata configuration files up to date, checks device states, gets component version and synchronizes the configuration.

18.11.1 Synopsis

```
tp_mgr_poll -start
tp_mgr_poll -stop
tp_mgr_poll -?
```

18.11.2 Options

Option	Description
-start	Starts the poller.
-stop	Stops the poller.
-? -help -man	Displays the help message.

18.12 tp_mgr_restore

The `tp_mgr_restore` command-line tool restores a backup of the Manager configuration that was created by `tp_mgr_backup`, replacing any existing Manager configuration. All existing databases will be dropped.

Refer to [tp_mgr_backup](#) for more information about `tp_mgr_backup`.

18.12.1 Synopsis

```
tp_mgr_restore -mysql_path=<path to binaries> -name=<backup file name>
```

```
tp_mgr_restore -name=<backup file name> -verbose
```

18.12.2 Options

Option	Description
<code>-verbose</code>	Provides progress statements during the backup procedure (optional).
<code>-latest</code>	Will search for and use the last made backup in <code>-name</code> .
<code>-name</code>	Specifies the path to and name of the backup file. <code>tp_mgr_restore</code> loads a single backup file. The name is taken from the <code>-name</code> option. It can be a gzipped file (extension <code>.gz</code>). If option <code>-latest</code> is used, the name is assumed to be a directory, where the last made backup is searched and used.
<code>-force</code>	No questions asked. All databases will be dropped without confirmation.
<code>-mysql_path</code>	Specifies the path to the MySQL binaries (optional). <code>tp_mgr_restore</code> assumes that the MySQL binaries are in the path. This option allows you to specify the specific path.
<code>-help</code> <code>-?</code> <code>-man</code>	Displays the help message.

18.12.3 Operands

Operand	Description
path to binaries	Path to the MySQL binaries (defaults to the current path).
backup file name	Name of the backup file (can be a GZ file).

18.12.4 Example

The following is an example command:

```
tp_mgr_restore -name=/tmp/mgr_databases.sql_2007_12_13_15_41_00.gz
```

18.13 tp_mgr_start

`tp_mgr_start` starts the MGR environment in the configured role (master or slave). It does not accept options and returns 0 upon success.

After starting the MGR with `tp_mgr_start`, all MGRdata files will be recreated. To ensure all the updates are done, wait until the time stamps of those files are later than `tp_mgr_start` was called. This can be verified with the following command:

```
ls -la /usr/TextPass/MGRdata*
```

18.13.1 Synopsis

```
tp_mgr_start
```

```
tp_mgr_start --clean
```

```
tp_mgr_start -c
```

18.13.2 Options

Option	Description
--clean	Removes all pre-created files from the Manager cache directory. This option may slow the MGR's start-up, but it ensures that new files are created after actions such as license changes
-c	

18.14 tp_mgr_stop

`tp_mgr_stop` stops the Manager environment by stopping the following components (the process times out after three minutes):

- `tp_fclient`
- `tp_fserver`
- `tp_mgr_poll`
- `httpd`

18.15 tp_mgr_table_migration

The `tp_mgr_table_migration` is a command-line tool that allows you to transfer the data of the **Environment ► Countries** (countryTable) and the **Environment ► Networks** (mobNetworkTable) from an active MGR instance to a fresh and inactive MGR instance.

Note: There should be no configuration performed (e.g. Add New, Save etc.) on **Countries** and **Network Table** screens on fresh and active MGR GUI while using this tool.

18.15.1 Synopsis

```
tp_mgr_table_migration [arguments]
```

If no arguments are specified, the `tp_mgr_table_migration` tool will run on the fresh MGR with the default values for all the arguments as mentioned in the next section below.

Examples:

```
tp_mgr_table_migration --activehost=<value> --activeusername=<value>
--activepassword=<value>
  --activedomainname=<value> --freshhost=<value> --freshusername=<value>
--freshpassword=<value>
  --freshdomainname=<value> --mgrtype=<value>
tp_mgr_table_migration --dbdumpfile=<value> --mgrtype=<active>
tp_mgr_table_migration --dbdumpfile=<value>
tp_mgr_table_migration --help
```

18.15.2 Options

Options	Description
-h --help	Displays the help message.
-d --debug	Runs the script in debug mode showing detailed information on console.
-v --verbose	Enables the verbose mode.
-dd --dbdumpfile	Specifies the full path of the database table dump file.
-mt --mgrtype	Specifies the MGR's type.
-ahost	Specifies the IP-Address/hostname of the active MGR.

Options	Description
--activehost	
-aport --activeport	Specifies the port number that is used for connecting to the active MGR database.
-auser --activeusername	Specifies the username that is used to log on to the active MGR database.
-apwd --activepassword	Specifies the password that is used to log on to the active manager database.
-adn --activedomainname	Specifies the domain name of the active MGR from where table data is to be migrated.
-fhost --freshhost	Specifies the IP-Address/hostname of the fresh MGR.
-fport --freshport	Specifies the port number that is used for connecting to the fresh MGR database.
-fuser --freshusername	Specifies the username that is used to log on to the fresh MGR database.
-fpwd --freshpassword	Specifies the password that is used to log on to the fresh MGR database.
-fdn --freshdomainname	Specifies the domain name of the fresh MGR where table data is to be transferred.

Note:

1. If you do not provide the 'username', 'password', 'hostname' and 'domainname' for the active or the fresh MGR, then the tool will use the corresponding default values:

Fresh MGR:

freshusername: root

freshpassword: lokal\$

freshhost: localhost

freshport: 3306

freshdomainname: main

Active MGR:

```

activeusername: root
activepassword: lokal$
activehost: localhost
activeport: 3306
activedomainname: main
mgrtype: fresh

```

2. In order to execute the `tp_mgr_table_migration` tool, the component versions of the active and fresh MGR must be the same.
3. The tool should be executed with 'root' privileges only.
4. All logs generate at `/var/TextPass/MGR/logs/unification/` path
5. There are two different ways in which the table data can be migrated using the tool:

a) Direct data transfer:

In case of direct connectivity between both MGRs, you can directly transfer the table data from the active MGR to the fresh (inactive) MGR. To do so you need to execute below command on either the fresh or the active MGR:

```

tp_mgr_table_migration --activehost=<value>
--activeusername=<value> --activepassword=<value>
--activedomainname=<value> --freshhost=<value>
--freshusername=<value> --freshpassword=<value>
--freshdomainname=<value> --mgrtype=<value>

```

b) Dump transfer:

In case there is no direct connectivity between the MGRs, you need to follow the below steps:

1. Export the mysqldump from the active MGR tables.
2. Transfer the dump file offline to fresh MGR.
3. Import the dump file into the fresh MGR tables.

Execute the below command for exporting the mysqldump from the active MGR tables:

```

tp_mgr_table_migration --dbdumpfile=<value> --mgrtype=<active>

```

Execute the below command for importing the mysqldump into the fresh MGR tables:

```

tp_mgr_table_migration --dbdumpfile=<value>

```

There is no need to mention the mgrtype; it is by default set to fresh.

18.16 tp_role

`tp_role` provides the current role (master or slave) of the Manager environment.

18.17 tp_shell

The `tp_shell` command-line tool allows you to change the Mobile Messaging dynamic configuration from the command-line instead of in the MGR Web interface. It can be used on the command line, or as a shell.

18.17.1 Synopsis

```
tp_shell [authentication] [tp_shell commands] [command options]
```

If no arguments are specified, `tp_shell` is used as a shell. When inside the shell, execute `help` for a list of possible commands.

Examples:

```
tp_shell --user=<value> --password=<value> --domain=<value>
```

```
tp_shell --user=<value> --password=<value> --domain=<value> --add <entity> \
--fields <field>=<value>,(<field>=<value>)*
```

```
tp_shell --user=<value> --password=<value> --domain=<value> --delete <entity> \
--index=<value>
```

```
tp_shell --user=<value> --password=<value> --domain=<value> --activate <entity> \
--index=<value>
```

```
tp_shell --user=<value> --password=<value> --domain=<value> --deactivate <entity> \
--index=<value>
```

```
tp_shell --user=<value> --password=<value> --domain=<value> --show <entity> \
[--index=<value>] [--format=(console|csv)]
```

```
tp_shell --user=<value> --password=<value> --domain=<value> --update <entity> \
--index=<value> -f <field>=<value> (-f <field>=<value>)*
```

```
tp_shell -u <value> -p <value> -d <value> -c /path/to/commandfile
```

```
tp_shell -u <value> -p <value> -d <value> --hostname <remote mgr hostname> \
-S applicationTable
```

18.17.2 Authentication Options

Option	Description
-u --user	Identifies the user (this must be an existing user in the MGR).
-p --password	Authenticates the user.
-d --domain	Number of the domain in which the command should be executed (the "main" domain is usually 1).

Option	Description
--hostname	The host name where the MGR you wish to control is running. Note: Port 80 must be reachable on that host.

18.17.3 tp_shell Commands

Command	Description
-A --add	Adds a new entry to the configuration.
-D --delete	Deletes an entry (identified by name or by index) from the configuration.
-U --update	Updates the fields listed after the <code>fields</code> keyword. Note: Use <code>--activate</code> or <code>--deactivate</code> to change the <code>admin_state</code> of a table entry. The option <code>--update</code> shall not be used in such situations.
--activate	Activates the entity identified by index.
--deactivate	Deactivates the entity identified by index.
-S --show	Shows the details of the entity (identified by name or by index), in the format specified by <code>format</code> . If no entity is specified, all are shown.
-v --version	Shows the version of <code>tp_shell</code> .
-v --verbose	Provides verbose output on the console.
-c --command_file	Enables you to provide a file containing one command per line. <code>tp_shell</code> will read the file and execute each command, in order. For the command file format, refer to Command File Format . CAUTION: <code>tp_shell</code> does not verify whether executing the command file will result in an unusable configuration. Use this command with caution!
-n --numbering	Adds a number for each command performed in the output. This can be useful for determining which commands succeeded and which failed when executing a large command file.

Command	Description
-? -h --help	Displays the help message.

18.17.4 Options

Option	Description
<entity>	Any item from the MGR database or MIB files. For example: applicationTable or aoRtgRuleTable
-f --fields	Indicates that the information that follows consists of <field="value"> combinations. You can provide one combination per --field command or a comma-separated list of combinations.
-i --index	Index of the entity that should be changed.
--format	Specifies how the returned information should be formatted. Current options are console or csv. The value provided in the command line option will overwrite the value provided in the interactive mode.
<field="value">	Name the entity field that should be changed and its value (in quotation marks).

18.17.5 Command File Format

The file that can be passed on the command line containing commands to be executed, should have a single command per line as follows:

```
<COMMAND> <ENTITY> [<INDEX="NUMBER">] [FIELDS <FIELD="VALUE"> <FIELD="VALUE"> <FIELD="VALUE">]
```

18.17.5.1 Sample Usage

The following examples illustrate adding a country to the configuration, updating an application, and deleting an application:

```
add countryTable fields countryCountryCode="382" countryMobileCountryCode="297" \
countryAdminState="1" countryDescription="Montenegro" countryCountry="me"
```

```
update applicationTable index="32" fields applicationThroughputAoMaximum="500" \
applicationOutsideSmppWindowSize="10"
```

```
delete applicationTable index="32"
```

The following example illustrates the handling of multiple entries.

A <textfile> can be created with multiple inputs as follows:

```
add fafListTable fields fafListIndex1="1" fafListIndex2="1" fafListChunk="ListValue33"
add fafListTable fields fafListIndex1="1" fafListIndex2="2" fafListChunk="ListValue34"
add fafListTable fields fafListIndex1="1" fafListIndex2="3" fafListChunk="ListValue35"
```

Command line inputs and results:

```
tp_shell --user=<user name> --password=<password> -c <textfile>
Add fafListTable successful!
Add fafListTable successful!
Add fafListTable successful!
```

18.17.6 Example Use Cases

Due to the complexity of Mobile Messaging in general, and the validation process of the MGR in specific, there are some use cases that at first glance seem unusual.

This section outlines some use cases to show that *anything* that is possible with the MGR, is also possible with `tp_shell`.

Adding or Updating a List

The following examples are executed from the interactive `tp_shell` prompt.

First, understand that a 'list' is not an entity on its own, but actually a container for various 'listConditions', which need to be added to the list separately.

1. First, a container is needed, a `listTable` entry, where the types are as defined in the MIB (see the entry for `listTypeBits`, but 1 is for a list of MSISDN conditions)

```
add listTable fields listName="MyExampleList" listType="1" \
listConditionBlob="M1111111"
```

Note: Note that a `listConditionBlob` is inserted here, as in some versions of the MGR there is a known issue that updating a 'NULL' field in the database (which is what would happen if nothing is filled in) does not work. So inserting a value just serves to initialize the field which will eventually hold all the list entries.

2. Then add the conditions to the list, which are identified with the "show" command:

```
show listTable
```

For this example, it is assumed that there was an index of "3" in the ID column.

The specific modifier (M in this case) needs to match the `listType`. Setting non valid types could cause SNMP errors when provisioning the RTR. The modifiers and valid values can be found in the Condition Spec section of the MIB file.

```
add listConditionTable fields listConditionIndex1="3" \ listCondition="M3112345678"
listConditionIndex2="1"
```

```
add listConditionTable fields listConditionIndex1="3" \
listCondition="M3145600000-3145699999" listConditionIndex2="2"
```

```
add listConditionTable fields listConditionIndex1="3" listCondition="M316*" \
listConditionIndex2="3"
```

3. Now, navigate to the MGR and see that under **Routing ► Lists** at ID 3, there is a new entry 'MyExampleList' with list entries consisting of:

```
M3112345678
M3145600000-3145699999
M316*
```


Note: The **IPAddress-Port** list condition is also sync with IIW using `iiwListConditionTable`. If you are creating or modifying an **IPAddress-Port** list condition, then execute the `listConditionTable` command for `iiwListConditionTable` as well, as shown in example below:

```
update listConditionTable index="6.1" fields listConditionIndex1="6"
listConditionIndex2="1" listCondition="i192.16.1.5"
update iiwListConditionTable index="6.1" fields iiwListConditionIndex1="6"
iiwListConditionIndex2="1" iiwListCondition="i192.16.1.5"
```

Note: To automatically do this from a CSV file is beyond the scope of this manual, but from the example it should be possible to script something that splits the CSV file into entries, which each get added to the proper `listCondition` in the `listConditionTable`.

Country and Network Information Provisioning

The following examples are executed from the interactive `tp_shell` prompt.

1. To add a country:

```
add countryTable fields countryCountryCode="382" countryMobileCountryCode="297"
\ countryAdminState="1" countryDescription="Montenegro" countryCountry="me"
```

2. If you also want to add a network number range for this country, you need to identify the index of the newly added country (in this example 92) and add the Mobile Network entry (again already adding a container for the Number Range in `'mobNetworkNumberRangeBlob'`):

```
add mobNetworkTable fields mobNetworkCountry="me" \
mobNetworkDescription="ProMonte" mobNetworkMapPhase="3" \
mobNetworkMobileCountryCode="297" mobNetworkMobileNetworkCode="01" \
mobNetworkOperator="ProMonte" mobNetworkNumberRangeBlob=""
```

3. Add the number range to the index of the Mobile Network just created (for this example, an index of "2" is assumed).

```
add mobNetworkNumberRangeTable fields mobNetworkNumberRangeIndex1="2" \
mobNetworkNumberRange="3826900000000-3826999999999" \
mobNetworkNumberRangeIndex2="1"
```

4. In the MGR, now there will be a valid entry under **Environment ► Networks** at index 2.

Activating a Trace Filter

The following examples are directly executed from the command line.

1. First, identify the Trace Filter server to add your rule to (this is obviously easier through the MGR GUI):

```
tp_shell --username admin --password Secret --show traceFilterTable
```

2. For example, you decide to enable tracing on Short Number 1234. Add your condition to the Trace Filter you will be using (filter 2 in this example):

```
tp_shell -uadmin -pSecret --add traceFilterConditionTable --fields \
traceFilterConditionIndex1="2",traceFilterConditionSpec="S1234"
```

To make this easier, you could wrap this line in a shell function, with the short number as a variable. Note that this differs per shell, so no examples are added on how to do that.

In this case the `'S1234'` refers to a short number, the full list of currently supported values are:

- S - Short Number (for example, S4444)
- I - IP Address (for example, I10.0.0.1)
- A - Application (uses the index from `applicationTable`, for example, A12)

- U - All Unauthenticated Sessions
 - X - All MXP Traffic.
3. To activate an already existing Trace Filter with its conditions:

```
tp_shell -uadmin -pSecret --activate traceFilterTable --index 2
```

Scheduled Activation of Rules

A scheduled activation of provisioning data or parameters is possible and can be triggered from the operating system's 'cron' functionality.

For example, to disable the MO Routing rule with ID 141:

1. Create a script containing a line like:

```
tp_shell -uadmin -pSecret --deactivate moRtgRuleTable --index 141
```

(or --deactivate to enable it)

2. If you want to disable the rule every weekday at 7:30 AM, in cron this would then, for example, be:

```
30 7 * * 1-5 /opt/scripts/disableRule141.sh
```

Scheduled Activation of an Application

To enable an application with ID 141 at a certain time:

1. Create a script with:

```
tp_shell -uadmin -pSecret --activate applicationTable --index 141
```

2. Add the script to a crontab.

Scheduled Deactivation of an Application

To enable an application with ID 141 at a certain time:

1. Create a script with:

```
tp_shell -uadmin -pSecret --deactivate applicationTable --index 141
```

2. Add the script to a crontab.

Scheduled Updates of Application Throughput

To change the throughput and window size of application 32 and 47 in domain 2:

1. Create a script containing:

```
tp_shell -u admin -p Secret -U applicationTable -d 2 -i 32 -f \
applicationThroughputAoMaximum="500",applicationOutsideSmppWindowSize="50"
```

```
tp_shell -u admin -p Secret -U applicationTable -d 2 -i 47 -f \
applicationThroughputAtMaximum="250",applicationInsideUcpWindowSize="100"
```

2. Add the script to a crontab.

Activation and deactivation of the admin state of a table entry

1. To activate:

```
tp_shell --user=<value> --password=<value> --domain=<value> --activate <entity>
--index=<value>
```

- To deactivate:

```
tp_shell --user=<value> --password=<value> --domain=<value> --deactivate <entity>
--index=<value>
```

18.18 tp_slave

tp_slave is an internal command to start the Manager in slave mode. It does not accept options and returns 0 upon success.

18.19 tp_update_mgr_device

The tp_update_mgr_device command-line tool allows you to update the device version on MGR during NMM upgrade.

18.19.1 Synopsis

```
tp_update_mgr_device [--username=<value>] [--password=<value>]
[--hostname=<value>] --index=<value> --type=<value> [--version=<value>]
```

```
tp_update_mgr_device [--username=<value>] [--password=<value>]
[--hostname=<value>] --config=<value>
```

```
tp_update_mgr_device --help
```

18.19.2 Options

Option	Description
-u --username	Identifies the user. This must be an existing login in the MGR. Default value: admin
-p --password --passwd	Authenticates the user. Default value: admin123
--hostname	The host where the MGR you wish to control is running. Note that you need to be able to reach port 80 on that host. Default value: localhost
-i --index	The index of the record whose version is to be updated.

Option	Description
-t --type	The type of device to be updated. For example : RTR, HUB, IIW, FAF, AMS, PBC, PBC1, LGP, BAT, EMG, SPFCORE, SPFSMS, SPFSOAP, XSCPY, XSFWD, XSARP, XSSIG, XSDIL, XSBWL, XSINT.
-v --version	The maximum version to which the device has to be updated. Must be greater than currently configured version on MGR. If version is not specified then device shall be updated to highest version available on MGR.
-conf --config	The path of the configuration file where all the device details are present in the xml file. <code>tp_update_mgr_device</code> reads the configuration file and update devices provided in configuration file. Sample Configuration file: <pre><?xml version="1.0" encoding="UTF-8"?> <tp_update_mgr_device> <device index="1" type="faf" version="R02.03.00.01"/> <device index="2" type="RTR" version="R02.04.00.01"/> <device index="5" type="pbc"/> </tp_update_mgr_device></pre>
--debug	Runs the script in debug mode showing detailed information on console.
-h --help	Displays the help message.

1. The options "config" and "index, type, version" are mutually exclusive.
2. If you do not provide "username", "password", "hostname", then the Manager attempts to use the default values.
3. If you do not provide "version", then device version is updated to the highest device version available on MGR.
4. If you execute the script without a configuration file, then "index" and "type" are mandatory parameters.

Appendix

A

Logging Elements

Topics:

- [Message Logging.....430](#)
- [Event Logging.....435](#)

A.1 Message Logging

This section lists the filter elements that are available for message log filters. To create a message log filter, go to **Logging > Messages > Filters**.

```

* applicationName
* applicationShortNumber
* destEmailAddr
* event
* ignoredRejectCauses
* isNotificationMessage
* mapLmsi
* messageIdentifier
* moreMessagesToSend
* mtRoutingRuleSkipped
* numberOfPreviousAttempts
* recipientRoutingNumber
* routingAction
* serviceCentreTimestamp
* timestamp
* unconditionalForward
* userData_normalizedText
* correlatedSriSm
  o mapLmsi
  o mapImsi
    + country
    + imsi
    + network
  o mapMsc
    + country
    + gsmAddress
    + network
  o mapMsisdn
    + country
    + gsmAddress
    + network
  o mapSgsn
    + country
    + gsmAddress
    + network
  o mapSmsc
    + country
    + gsmAddress
    + network
  o sccpCgPa
    + country
    + network
    + sccpAddress
* ecResponseData
  o applicationName
  o attributesReset
  o attributesSet
  o clientIpAddress
  o diameterStatus
  o evaluationResult
  o extConditionRule
  o textInEvaluationResponse
* infoFromHlr
  o mapImsi
    + country
    + imsi

```

```
        + network
    o mapMsc
        + country
        + gsmAddress
        + network
    o mapSgsn
        + country
        + gsmAddress
        + network
* insideRejectInfo
    o atiExtConditionRule
    o atiRoutingRule
    o rejectCause
* insideResponseInfo
    o atiRoutingRule
    o deliveryResult
    o routingErrorCode
* mapImsi
    o country
    o imsi
    o network
* mapMsisdn
    o country
    o gsmAddress
    o network
* mapSmsc
    o country
    o gsmAddress
    o network
* messageFields
    o alertOnMessageDelivery
    o alphanumericOriginator
    o alphanumericRecipient
    o billingIdentifier
    o dataCodingScheme
    o deferredDeliveryTime
    o deliveryStatus
    o destBearerType
    o destNetworkType
    o destSubAddress
    o destinationPort
    o displayTime
    o endToEndAckRequest
    o endToEndMessageType
    o errorCode
    o gsmMessageReference
    o gsmStatusReportType
    o language
    o messageReference
    o moreMessagesToSend
    o msValidityIndicator
    o notificationType
    o numberOfMessages
    o originatingPointCode
    o payloadType
    o portNumber
    o priority
    o privacy
    o protocol
    o protocolIdentifier
    o replyPathIndicator
    o serviceDescription
    o singleShotIndicator
    o smDefaultMsgId
    o smsSignal
```

```
o sourceBearerType
o sourceNetworkType
o sourcePort
o sourceSubAddress
o tariffClass
o userData
o userDataHeader
o userResponseCode
o validityPeriod
o xsMessageType
o callbackNumbers
  + alphaTag
  + presentation
  + number
    # address
    # digitMode
o msValidityPeriod
  + multiplier
  + unit
o originatedImsi
  + country
  + imsi
  + network
o originatedMscAddress
  + country
  + gsmAddress
  + network
o originatorAddress
  + country
  + gsmAddress
  + network
o recipientAddress
  + country
  + gsmAddress
  + network
o serviceCentreAddress
  + country
  + gsmAddress
  + network
* originalMessageFields
  o originatorAddress
    + country
    + gsmAddress
    + network
  o recipientAddress
    + country
    + gsmAddress
    + network
* outboundAo
  o applicationName
  o applicationShortNumber
  o routingErrorCode
  o scNodeName
  o scTerminationPointName
  o serviceCentreName
  o serviceCentreTimestamp
  o smppMessageId
  o submissionResult
* outboundAt
  o applicationName
  o applicationShortNumber
  o routingAction
  o ecResponseData
    + applicationName
    + attributesReset
```



```

    + attributesSet
    + clientIpAddress
    + diameterStatus
    + evaluationResult
    + extConditionRule
    + textInEvaluationResponse
  o rejectInfo
    + atExtConditionRule
    + atRoutingRule
    + rejectCause
  o responseInfo
    + atRoutingRule
    + deliveryResult
    + routingErrorCode
* outboundMo
  o rejectCause
  o smscName
  o submissionResult
* outboundMt
  o mtFwdSmToMscRoutingAction
  o mtFwdSmToSgsnRoutingAction
  o sriSmRoutingAction
  o ecResponseData
    + applicationName
    + attributesReset
    + attributesSet
    + clientIpAddress
    + diameterStatus
    + evaluationResult
    + extConditionRule
    + textInEvaluationResponse
  o mtFwdSmToMscRejectInfo
    + mtExtConditionRule
    + mtRoutingRule
    + rejectCause
  o mtFwdSmToMscResponseInfo
    + deliveryResult
    + mtRoutingRule
  o mtFwdSmToSgsnRejectInfo
    + mtExtConditionRule
    + mtRoutingRule
    + rejectCause
  o mtFwdSmToSgsnResponseInfo
    + deliveryResult
    + mtRoutingRule
  o sriSmRejectInfo
    + mtExtConditionRule
    + mtRoutingRule
    + rejectCause
  o sriSmResponseInfo
    + mapLmsi
    + mtRoutingRule
    + queryResult
    + mapImsi
      # country
      # imsi
      # network
    + mapMsc
      # country
      # gsmAddress
      # network
    + mapSgsn
      # country
      # gsmAddress
      # network

```

```
* rejectInfo
  o atExtConditionRule
  o atRoutingRule
  o rejectCause
* responseInfo
  o atRoutingRule
  o deliveryResult
  o routingErrorCode
* sccpCdPa
  o country
  o network
  o sccpAddress
* sccpCdPaOfFirstSegment
  o country
  o network
  o sccpAddress
* sccpCgPa
  o country
  o network
  o sccpAddress
* sccpCgPaOfFirstSegment
  o country
  o network
  o sccpAddress
* smsCommand
  o smsCommandData
  o smsCommandType
  o smsMessageNumber
  o smsMessageReference
  o smsProtocolId
  o smsServices
  o smsRecipient
    + country
    + gsmAddress
    + network
* smsDeliver
  o smsDataCodingScheme
  o smsProtocolId
  o smsScTimestamp
  o smsServices
  o smsUserData
  o smsUserDataHeader
  o smsOriginator
    + country
    + gsmAddress
    + network
* smsSubmit
  o smsDataCodingScheme
  o smsMessageReference
  o smsProtocolId
  o smsServices
  o smsUserData
  o smsUserDataHeader
  o smsValidityPeriod
  o smsRecipient
    + country
    + gsmAddress
    + network
* ssiInfo
  o originatorServices
  o recipientServices
* statusReport
  o smsDischargeTime
  o smsMessageReference
  o smsScTimestamp
```

```

    o smsServices
    o smsStatus
    o smsRecipient
      + country
      + gsmAddress
      + network
* storage
  o applicationName
  o applicationShortNumber
  o queue
  o routingErrorCode
  o storageResult

```

A.2 Event Logging

This section lists the filter elements that are available for event log filters. To create an event log filter, go to **Logging > Events > Filters**.

```

* mtp
  o mtp3OrigPointCode
* sccp
  o cgPa
    + sccpAddress
      # pointCode
      # subSystemNumber
      # globalTitle
      * numberingPlan
      * number
      * natureOfAddressIndicator
    + country
    + network
  o cdPa
    + sccpAddress
      # pointCode
      # subSystemNumber
      # globalTitle
      * numberingPlan
      * number
      * natureOfAddressIndicator
    + country
    + network
* tcap
  o tcapMessageType
  o tcapOrigTransId
  o tcapDestTransId
  o protoVersionTag
  o dialogTag
  o appContext

```


Appendix B

References

Topics:

- [References.....438](#)

B.1 References

1. NewNet Mobile Messaging Full Element Installation Manual
2. NewNet Mobile Messaging RTR Operator Manual
3. NewNet Mobile Messaging RTR Billing Manual
4. NewNet Mobile Messaging HUB Operator Manual
5. NewNet Mobile Messaging AMS Operator Manual
6. NewNet Mobile Messaging FAF Operator Manual
7. NewNet Mobile Messaging LGP Operator Manual
8. NewNet Mobile Messaging CCI Operator Manual
9. NewNet Mobile Messaging STV Operator Manual
10. NewNet Mobile Messaging ECI Specification

Glossary

#

3GPP 3rd Generation Partnership Project

A

ABL Automatic Blacklisting
An enhanced anti-spam and anti-fraud functionality, wherein the FAF filters screen incoming MO/MT messages received from the RTR and, if a message is detected as `spam` or `fraudulent` based on the appropriately configured filter conditions, sends an automatic provisioning request to the SPF to blacklist the corresponding originator or recipient subscriber for either a specified duration of time or permanently.

ACK Data Acknowledgement

AGW Application Gateway
A gateway between SMS applications and service centres provided by the Router, HUB, and AMS components.

AMS Active Message Store
Provides store-and-forward functionality for SMS messages.

AO Application Originated
Short message traffic that is originated by an application.

AOR Application-Originated Routing

A

	<p>Routing rule that operates on application-originated (AO) messages.</p> <p>Address of Record</p>
AOX	<p>Application-Originated eXternal condition</p> <p>External condition rule that operates on application-originated (AO) messages.</p>
ARP	<p>Address Resolution Protocol</p> <p>ARP monitoring uses the Address Resolution Protocol to determine whether a remote interface is reachable.</p> <p>Auto Reply service</p> <p>Personalized SMS auto reply service. This service is provided by the Mobile Messaging XS-ARP component.</p>
ASCII	<p>American Standard Code for Information Interchange</p>
ASN.1	<p>Abstract Syntax Notation One</p>
AT	<p>Application Terminated</p> <p>Short message traffic that terminates at an application.</p>
ATI	<p>Any Time Interrogation</p> <p>An ATI message allows an external server to interrogate an HLR and obtain information about the location and/or state of a GSM subscriber.</p> <p>Incoming application-terminated</p>

A

ATIC	Incoming application-terminated counting Counting rule that operates on incoming application-terminated (AT) messages.
ATIR	Incoming application-terminated routing Routing rule that operates on incoming application-terminated (AT) messages.
ATIX	Incoming application-terminated eXternal condition External condition rule that operates on incoming application-originated (AO) messages.
ATO	Outgoing application-terminated
ATOC	Outgoing application-terminated counting Counting rule that operates on outgoing application-terminated (AT) messages.
ATOR	Outgoing application-terminated routing Routing rule that operates on outgoing application-terminated (AT) messages.
ATOX	Outgoing application-terminated eXternal condition External condition rule that operates on outgoing application-originated (AO) messages.

B

B

BAT	<p>Batch Server</p> <p>Message distribution application that can send the same short message to multiple recipients.</p>
BOBO	<p>Billing On Behalf Of</p> <p>The Billing On Behalf Of ServiceClass condition is used by SMS Applications to send messages charged as if the were submitted as MO messages.</p>
BWL	<p>Black and Whitelist service</p> <p>Personalized short message black and whitelist service. This service is provided by the Mobile Messaging XS-BWL component.</p>

C

CCDR	<p>Comverse SMSC-compatible CDR format</p>
CCI	<p>Customer Care Interface</p> <p>A Web-based interface that allows customer care agents to assist SMS subscribers.</p>
CdPA	<p>Called Party Address</p> <p>The field in the SCCP portion of the MSU that contains the additional addressing information of the destination of the MSU. Gateway screening uses this additional information to determine if MSUs that contain the DPC in the routing label and the subsystem number in the called party address portion of the MSU are allowed in the network where the EAGLE 5 ISS is located.</p>

C

CDR	<p>Call Detail Record</p> <p>This refers to the recording of all connections in a database to permit activities such as billing connection charges or network analysis. CDR files are used in public switched networks, IP networks, for IP telephony, and mobile communications networks.</p> <p>Charging Data Record</p> <p>Used for user billing; a telecom provider transfers them from time to time in order to send bills to their users.</p>
CIMD	<p>Computer Interface for Message Distribution</p> <p>Proprietary SMSC protocol developed by Nokia.</p>
CLI	<p>Custom LSMS Interface</p> <p>Command-line interface</p> <p>Calling Line Identification</p>
CPU	<p>Central Processing Unit</p>
CPY	<p>Copy to Phone service</p> <p>Personalized short message copy service that provides MO and MT copy to phone functionality. This service is provided by the Mobile Messaging XS-CPY component.</p>
CSV	<p>Comma-separated values</p> <p>The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline</p>

C

is a special character or sequence of characters signifying the end of a line of text).

CTA

Copy to Application service

Personalized short message copy to application service that provides originator copy to application ("Sent Items") and/or recipient copy to application ("Inbox") functionality. This service is provided by the Mobile Messaging XS-CPY component.

CTE

Copy to Email service

Personalized short message copy to email service, which allows MT short messages to be copied to one or more e-mail addresses provisioned by a subscriber. This service is provided by the Mobile Messaging XS-CPY component.

D

daemon

A process that runs in the background (rather than under the direct control of a user) and performs a specified operation at predefined times or in response to certain events. Generally speaking, daemons are assigned names that end with the letter "d." For example, sentryd is the daemon that runs the Sentry utility.

DCS

Data Coding Scheme

Diameter

Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in

D

both local and roaming AAA situations.

Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

DIL

Distribution List service

Personalized short message distribution list service. This service is provided by the Mobile Messaging XS-DIL component.

DMF

Direct Message Filter

Application component that consumes Intercept files generated by RTR, so it must run with RTR on the same Traffic Element. This component will regularly monitor for new Intercept Files generated by the RTR.

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

E

E.164

The international public telecommunication numbering plan developed by the International Telecommunication Union.

EC

External Condition

Condition that is passed on the external condition interface.

E

ECDR	Ericsson MSC-compatible CDR format
ECI	External condition interface Interface for communicating with external condition applications.
ECM	External condition message Message that is passed on the external condition interface.
EMG	SMS-to-E-mail Gateway Provides SMS-to-e-mail conversion for mobile subscribers.
EMS	Element Management System The EMS feature consolidates real-time element management at a single point in the signaling network to reduce ongoing operational expenses and network downtime and provide a higher quality of customer service.
ESME	External Short Message Entity The remote-destination entities on the IP network that is connected to using SMPP protocol.

F

FAF	Firewall Advanced Filter Works in combination with the Firewall to filter messages, modify message content, and alert network operators of increases in SMS-related traffic.
-----	---

F

FCDR	SMSC-compatible ASN.1 CDR format
FDA	<p>First Delivery Attempt</p> <p>Approximately 85 to 90 percent of SMS traffic gets through on first delivery attempt (FDA). That means that all of the initial processing that the SMSC does to store, query and forward messages is to a certain extent a waste of processing power — it would be much more cost-effective for an operator if a less expensive piece of equipment could first attempt to deliver the message.</p>
FTE	<p>Personalized short message forward to email service, which allows MT short messages to be forwarded (unconditionally) to one or more e-mail addresses provisioned by a subscriber.</p> <p>This service is provided by the Mobile Messaging XS-FWD component.</p>
FTP	<p>File Transfer Protocol</p> <p>A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.</p>
FWD	<p>Forward service</p> <p>Personalized short message forward service. This service is provided by the Mobile Messaging XS-FWD component.</p>
FWL	Firewall

F

Helps protect subscribers from receiving unwanted messages and provides statistical information and message details about inbound suspect messages.

G

GB	Gigabyte — 1,073,741,824 bytes
GMT	Greenwich Mean Time
GPRS	General Packet Radio Service A mobile data service for users of GSM mobile phones.
GSM	Global System for Mobile Communications
GSM 7-bit	GSM 7-bit default alphabet The GSM 7-bit default alphabet is a character set used for SMS as specified in 3GPP TS 23.038.
GT	Global Title Routing Indicator

H

HCDR	Huawei comma-separated values CDR format
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server A central database for subscriber information.

H

HUB Works in combination with the Router to manage traffic to and from SMS applications.

I

Icache Intermediate Cache
Enables the Mobile Messaging system to store the state and certain parameters of a short message while it is being processed by an external SMSC.

IGM See IS41 GSM Migration

IGMC Internally generated message counting
Counting rule that operates on internally generated messages (IGM).

IGMR Internally generated message routing
Routing rule that operates on internally generated messages (IGM).

IGMX Internally generated message external condition
External condition (EC) rule that operates on internally generated messages (IGM).

IIW IMS InterWorking
Works in combination with the router to provide gateway functionality between IMS domain and SS7 domain.

IMEI International Mobile Equipment Identifier

I

IMSI	International Mobile Subscriber Identity
IP	Internet Protocol IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network Integrates a number of services to form a transmission network. For example, the ISDN network integrates, telephony, facsimile, teletext, Datex-J, video telephony and data transfer services, providing users with various digital service over a single interface: voice, text, images, and other data.

L

LAC	Location Area Code
LCDR	Logica-compatible CDR format
LGP	Log Processor

L

Collects and processes data for the Log Viewer to display.

M

M3UA	<p>SS7 MTP3-User Adaptation Layer</p> <p>M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.</p>
MAP	Mobile Application Part
MB	Megabyte — A unit of computer information storage capacity equal to 1,048, 576 bytes.
MCC	<p>Mobile Country Code</p> <p>A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.</p>
MGR	A Web-based interface for managing NewNet Mobile Messaging components. Prior to Suite 6, the Configuration Manager (CM) provided this functionality.
MIB	Management Information Database
MNC	<p>Mobile Network Code</p> <p>A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.</p>

M

MNP	Mobile Number Portability
MO	Mobile Originated Refers to a connection established by a mobile communication subscriber. Everything initiated by the mobile station is known as mobile originated.
MOR	Mobile-Originated Routing Routing rule that operates on mobile-originated (MO) messages.
MOX	Mobile-Originated eXternal condition External condition rule that operates on mobile-originated (MO) messages.
MS	Mobile Station The equipment required for communication with a wireless telephone network.
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.
MT	Mobile Terminated All transmissions that reach the mobile station and are accepted by it, such as calls or short messages.

M

MTI	Incoming mobile-terminated
MTIC	Incoming mobile-terminated counting Counting rule that operates on incoming mobile-terminated (MT) messages.
MTIR	Incoming mobile-terminated routing Routing rule that operates on incoming mobile-terminated (MT) messages.
MTIX	Incoming mobile-terminated external condition External condition (EC) rule that operates on incoming mobile-terminated (MT) messages.
MTO	Outgoing mobile-terminated
MTOC	Outgoing mobile-terminated counting Counting rule that operates on outgoing mobile-terminated (MT) messages.
MTOR	Outgoing mobile-terminated routing Routing rule that operates on outgoing mobile-terminated (MT) messages.
MTOX	Outgoing mobile-terminated external condition External condition (EC) rule that operates on outgoing mobile-terminated (MT) messages.

M

MTP3 Message Transfer Part, Level 3

MXP Message eXchange Protocol
NewNet proprietary protocol used for communication between the Mobile Messaging HUB, RTR, and AMS components.

N

NAI Nature of Address Indicator
Standard method of identifying users who request access to a network.

Network Access Identifier
The user identity submitted by the client during network authentication.

NCDR Nokia SMSC-compatible CDR format

NPI Number Plan Indicator

NPS Non-Provisionable Service
A service that cannot be provisioned by the subscriber. For example, the subscriber is not able to switch the service ON/OFF or provision the service with service specific settings.

O

OAM Operations, Administration, and Maintenance
The application that operates the Maintenance and Administration Subsystem which controls the operation of many NewNet products.

O

OPT

Opt-in/Opt-out. An enhanced service provisioning functionality that provides an ON/OFF switch to the subscriber for existing NPS (like XS-TIE) or any third party service defined in SPF.

P

PBC

Prepaid Billing Controller

Performs prepaid charging using the Diameter, CAMEL, or SMPP+ interface.

PC

Point Code

The identifier of a signaling point or service control point in a network. The format of the point code can be one of the following types:

- ANSI point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Non-ANSI domestic point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Cluster point codes in the format network indicator-network cluster-* or network indicator-*-*.
- ITU international point codes in the format **zone-area-id**.
- ITU national point codes in the format of a 5-digit number (**nnnnn**), or 2, 3, or 4 numbers (members) separated by dashes (**m1-m2-m3-m4**) as defined by the Flexible Point Code system option. A group code is required (**m1-m2-m3-m4-gc**) when the ITUDUPPC feature is turned on.
- 24-bit ITU national point codes in the format main signaling

P

area-subsignaling area-service point (**msa-ssa-sp**).

- 16-bit Japanese SS7 international point codes in the format of a 5-digit decimal number (nnnnn), or 3 numbers separated by dashes, i.e. Main number area - Sub number area - Unit number (M-S-U).

PDU	Protocol Data Unit
PID	Password ID Process ID Protocol ID
PSTN	Public Switched Telephone Network.

R

RFC	Request for Comment RFCs are standards-track documents, which are official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group the IESG.
-----	--

RN	Routing Number
----	----------------

RTR	Router Routes all types of SMS traffic.
-----	--

S

SAC	Service Access Code
-----	---------------------

SAR	Segmentation and Reassembly
-----	-----------------------------

S

SC	Site Collector System Controller
SCCP	Signaling Connection Control Part
SCDR	SS.8 CDR format
SFTP	SSH File Transfer Protocol (sometimes also called Secure File Transfer Protocol) A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network over any reliable data stream. It is typically used over typically used with version two of the SSH protocol.
SGSN	Serving GPRS Support Node
short code	A number that has meaning only within a particular phone company's network.
SIG	Signature service Personalized SMS signature service. This service is provided by the Mobile Messaging XS-SIG component.
SIGTRAN	The name given to an IETF working group that produced specifications for a family of protocols that provide reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols. The most significant protocol defined by the SIGTRAN group was the Stream Control Transmission Protocol

S

(SCTP), which is used to carry PSTN signalling over IP.

The SIGTRAN group was significantly influenced by telecommunications engineers intent on using the new protocols for adapting VoIP networks to the PSTN with special regard to signaling applications. Recently, SCTP is finding applications beyond its original purpose wherever reliable datagram service is desired.

SM

Short Message

SMPP

Short Message Peer-to-Peer Protocol

An open, industry standard protocol that provides a flexible data communications interface for transfer of short message data.

SMS

Short Message Service

SMSC

Short Message Service Center

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

SOAP

Simple Object Access Protocol

S

SPF	<p>Subscriber Provisioning Framework</p> <p>The Mobile Messaging solution to enable the configuration, control and application of subscriber-specific services. The SPF provides a framework to store and retrieve service-specific data through a variety of provisioning interfaces.</p>
SRI	<p>Send_Route_Information Message</p>
SS7	<p>Signaling System #7</p>
SSH	<p>Secure Shell</p> <p>A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.</p>
SSI	<p>Service Subscription Information</p> <p>The Mobile Messaging SSI can be queried to determine the applicable personalized subscriber services of the originator and recipient of the message.</p>
SSN	<p>SS7 Subsystem Number</p> <p>The subsystem number of a given point code. The subsystem number identifies the SCP application that should receive the message, or the subsystem number of the destination point code to be assigned to the LNP subsystem of the EAGLE 5 ISS.</p> <p>Subsystem Number</p>

S

A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry.

Subsystem Number

Used to update the CdPA.

STV

Statistics Viewer

Collects statistical data about NewNet Mobile Messaging components and displays it in the Manager.

T

TCAP

Transaction Capabilities Application Part

TCP

Transfer Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

TLV

Type/Length/Value

TON

Type of Number

TS

Test Strategy

Traffic Server

Technical Specification

Teleservices

TT

Translation Type

Resides in the Called Party Address (CdPA) field of the MSU and determines which service database is to receive query messages. The

T

translation type indicates which Global Title Translation table determines the routing to a particular service database.

U

UCP	Universal Computer Protocol Protocol used to connect to SMSCs.
UCS-2	2-byte Universal Character Set UCS-2 coded SMS contains a maximum of 70 characters. It is in use in countries that needs more than the standard 7/8 bit to code their character set. Each character is represented by 2 bytes.
UDH	User Data Header
UDP	User Datagram Protocol

V

VSMSC	Virtual SMSC Virtual SMSC is a feature of an Acision SMSC to have separate SMS Application routing and different billing file content for MO messages with a different SMSC Address.
-------	---

X

XS	eXternal Service Value-adding component that communicates with the Router to provide a service.
XS-ARP	eXternal Service Auto Reply component

X

	eXternal Service component that provides SMS auto reply functionality.
XS-BWL	Black- and Whitelist component eXternal Service component that provides personalized blacklist and whitelist services for home network subscribers.
XS-CPY	Short Message Copy component eXternal Service component that can send a copy of MO, MT, and AT short messages to MSISDNs.
XS-DIL	Distribution List component eXternal Service component that provides distribution list functionality.
XS-FWD	Short Message Forward component eXternal Service component that can forward short messages to MSISDNs.
XS-INT	eXternal Service Intercept component eXternal Service component that can intercept successful deliveries from and to subscribers. The intercepted messages are copied towards a specified APP.
XS-SIG	eXternal Service Signature component eXternal Service component that provides SMS signature functionality.

X

XS-TIE

Text Insertion Engine component
eXternal Service component that can
insert additional text in a short
message that is bound for home
network subscriber.

