

Oracle® Communications Convergent Charging Controller Messaging Manager User's Guide



Release 15.1

April 2025

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

Copyright

Copyright © 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About This Document	vii
Document Conventions	viii
Chapter 1	
System Overview	1
Overview	1
What is Messaging Manager?	1
Messaging Manager Components	4
Configuration Overview	6
Platform Support.....	12
Preconfigured Packages	13
Chapter 2	
Message Routing and Processing	17
Overview	17
Paths and Connections	17
Transaction Types	20
Routing Class	22
SMSCs.....	26
ASP Groups and Parameters.....	26
Screening Rules	27
Address Domains	29
Congestion Control.....	31
Triggering	31
Routing	33
Chapter 3	
Messaging Manager Screens	35
Overview.....	35
Introduction	35
Starting the Messaging Manager Screens	36
Services Menu	38
User Access Control.....	38
Chapter 4	
Messaging Manager Configuration Screen	41
Overview.....	41
Messaging Manager Configuration Screen	41
Nodes	43
Schemes.....	48
Networks.....	54
SMSCs.....	57
ASP Parameters.....	59
ASP Groups.....	64
ASPs.....	67

Chapter 5

Messaging Manager Schemes 75

Overview.....	75
Messaging Manager Scheme Screen.....	75
Adapters.....	77
Interfaces.....	80
Paths.....	82
Path Connections.....	88
IP Connections.....	89
SS7 Connections.....	98
Screening.....	100
Global Title Screening Rules.....	107
SCA Consistency Rules.....	109
Screening Rules.....	111
RLV Prefix Rules.....	114
Addressing.....	117
Throttling.....	122
Triggering.....	125
Routing.....	131

Chapter 6

Messaging Manager Replication Screen..... 137

Overview.....	137
Messaging Manager Replication.....	137
Messaging Manager Replication Screen.....	138
Replication.....	139

Chapter 7

Messaging Manager Action and Error Codes 141

Overview.....	141
Action and Error Codes.....	141
Global Action and Error Codes.....	142
SMPP.....	145
EMI.....	147
MAP.....	148
IS-41.....	150
SIP.....	152
Release Cause Mapping.....	154
Error Mapping.....	159

Chapter 8

Messaging Manager Routing Scheme Edit Control 165

Overview.....	165
Routing Scheme Edit Control.....	165

Chapter 9

Configuration Scenarios 169

Overview.....	169
Mobile to SMSC Messaging.....	169
Application to Mobile Messaging.....	179

Mobile to Application Messaging	194
Mobile to Mobile triggering to ACS	215
Instant Messaging	229
Email	235

About This Document

Scope

The scope of this document includes all functionality a user must know in order to effectively operate the Messaging Manager (MM) application. It does not include detailed design of the service.

Audience

This guide is written primarily for Messaging Manager (MM) administrators. However, the overview sections of the document are useful to anyone requiring an introduction.

Prerequisites

A solid understanding of UNIX and a familiarity with IN concepts are an essential prerequisite for safely using the information contained in this user guide. Attempting to install, remove, configure or otherwise alter the described system without the appropriate background skills, could cause damage to the system; including temporary or permanent incorrect operation, loss of service, and may render your system beyond recovery.

Although it is not a prerequisite to using this guide, familiarity with the target platform would be an advantage.

This manual describes system tasks that should only be carried out by suitably trained operators.

Related Documents

The following documents are related to this document:

- *Advanced Control Services User's Guide*
- *Control Plan Editor User's Guide*
- *Messaging Manager Technical Guide*
- *Messaging Manager Navigator Technical Guide*
- *Service Management System User's Guide*
- *SMS Email Interface Technical Guide*
- *Session Control Agent Technical Guide*

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Convergent Charging Controller documentation.

Formatting Convention	Type of Information
Special Bold	Items you must select, such as names of tabs. Names of database tables and fields.
<i>Italics</i>	Name of a document, chapter, topic or other publication. Emphasis within text.
Button	The name of a button to click or a key to press. Example: To close the window, either click Close , or press Esc .
Key+Key	Key combinations for which the user must press and hold down one key and then press another. Example: Ctrl+P or Alt+F4 .
Monospace	Examples of code or standard output.
Monospace Bold	Text that you must enter.
<i>variable</i>	Used to indicate variables or text that should be replaced with an actual value.
menu option > menu option >	Used to indicate the cascading menu option to be selected. Example: Operator Functions > Report Functions
hypertext link	Used to indicate a hypertext link.

Specialized terms and acronyms are defined in the glossary at the end of this guide.

System Overview

Overview

Introduction

This chapter provides an overview of the Graphical User Interface for Messaging Manager configuration and explains at a high level how Messaging Manager works.

In this chapter

This chapter contains the following topics.

What is Messaging Manager?	1
Messaging Manager Components	4
Configuration Overview	6
Platform Support.....	12
Preconfigured Packages	13

What is Messaging Manager?

Introduction

Messaging Manager (MM) is a messaging system for mobile networks. It acts as a Virtual Message Point (VMP) for a variety of different messaging traffic (for example: SIP, email, and SMS). Depending upon the role that it is performing, the VMP can act as any of the following:

- Message Service Center (MSC)
- Short Message Entity (SME) that terminates and/or originates messaging traffic
- Email host.

Messaging Manager integrates advanced routing and protocol delivery options with extended service control, in order to support all forms of traditional MO SMS and MT SMS services while retaining flexible support for new types of messaging.

Processing model

Messaging Manager's architectural approach as a Virtual Message Point means that all messaging involves transactions that can combine real time charging with direct delivery to the destination. This is the "new messaging model" that is aligned with the Internet age, and replaces the previous "store-and-forward" model with higher value and lower cost infrastructure.

The VMP processes all message services in real time, but it can integrate transparently with an existing SMSC for store-and-forward processing when real time delivery is not possible. It delivers:

- High capacity messaging on low cost infrastructure
- Very flexible switching and routing serving a multiple purposes
- Proven efficiencies using real time charging and delivery
- Enhanced message services using a service creation environment (SCE)
- Performance gains over existing SMSC infrastructure

- An enhanced customer experience

Messaging Manager provides a broad range of message processing capabilities at both the network layer and at the service layer. To the network it presents standard signaling interfaces to act in the role of:

- SMS-IW MSC (SMS Inter-Working MSC)
- SMS-GMSC (SMS Gateway MSC)
- HLR (proxy and emulation services)
- Email host (with SEI)

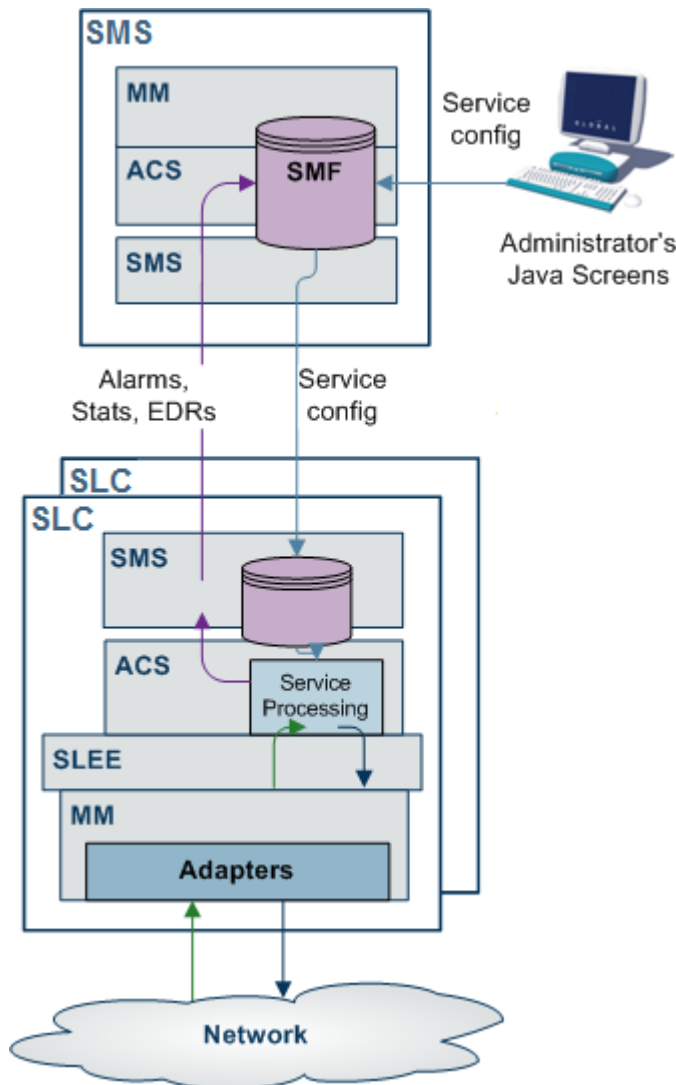
By performing multiple functions in one system, Messaging Manager simplifies the messaging infrastructure and frees up resources.

Messaging Manager components operating at the network layer can route traffic from one communication path to another and will automatically perform protocol translation based on the inbound and outbound communication paths. This can be statically configured through the management UI but can be dynamically overridden during transaction processing by the service control layers. Typically all message traffic arriving at the VMP is processed for charging (if necessary) then immediately directed to the destination. This process of delivering directly to a destination is known as First Delivery Attempt (or FDA).

When huge traffic spikes occur (such as during holiday peaks, or events such as televoting) Messaging Manager can absorb the load and groom traffic to provide smooth processing and near real time delivery.

Deployment diagram

This diagram shows the Messaging Manager deployment architecture.



Messaging Manager features

Messaging Manager provides the following features:

- FDA (First Delivery Attempt). SMS are directly delivered (through SS7) without going through an SMSC.
- Overload protection from SMS traffic peaks, for example, special events (New Year) or application peaks time (televoting). MM, enables you to offload your SMSCs and protect them from traffic peaks. This enables you to extend your capability to handle extreme traffic peaks in an efficient way.
- Value-added SMS services. These include:
 - Flash messaging
 - Auto-reply
 - Anti-spam
 - SMS copy to mobile or email
 - SMS-MT forwarding

- Voting campaigns
- Real-time charging
- The ability to provide SPOC (Single Point of Contact) to ASPs to attract more ASPs on your networks and to differentiate your offering on value-added interactive applications

Messaging Manager Components

Messaging Manager components

The major Messaging Manager components are:

Component	Description
Messaging Manager Multigate	A multi-protocol gateway and multi-function router that can receive and send short messages. Its layered architecture allows all signaling and IP protocols to connect to a common set of service logic, maintaining independence between transport protocols and the user-defined routing scheme that defines the messaging model. For a full description of this component, see <i>Messaging Manager Technical Guide</i> .
Messaging Manager Navigator	A Mobile Station location service that can perform and/or emulate HLR lookups by other components or network elements, caching the results to optimize network signaling and direct SMS transmission toward service logic. For a full description of this component, see <i>Messaging Manager Navigator Technical Guide</i> .
Messaging Manager Director	A set of service control feature nodes that execute as a message control plan and provide enhanced logic for message delivery, routing, and charging and offers extended message attribute controls. For a full description of this component, see <i>Messaging Manager Technical Guide</i> .
Messaging Manager Manager	A central UI for management of routing schemes and message control plans that are used to configure and control all service logic components. This component is fully described in this guide.

Messaging Manager Director

Messaging Manager Director provides complete control over all aspects of the VMP services. Its advanced service control facilities enable extended and customised SMS processing, including real-time billing interaction, by supporting user defined message control plans.

Message control plans can be triggered from Messaging Manager Multigate and include service logic based many properties, such as:

- Incoming path names (that is, protocols and connections)
- Transaction types, such as Submit, Deliver, Notify or Route Info messages
- Originating and/or destination address
- Location of originating and/or destination mobile station
- Message content
- Time of day.

A message can be triggered from Multigate to a specific message control plan to provide extended (customer specific) service logic. For example, Messaging Manager Director may modify any routing options before signalling to Multigate to continue delivery so that Multigate routes the message according to the new options.

Messaging Manager Director can ensure that delivery proceeds only if charging is satisfied, such that delivery and charging proceeds as a single transaction.

Messaging Manager Multigate

Multigate is the core VMP component that provides multi-protocol message handling. It employs a “message model” abstraction that gives enormous power to the service designer in classifying, filtering and routing message traffic. Multigate provides the message delivery and retry logic driven by the message model and dynamic changes made by Messaging Manager Director. The following features are provided:

- Routing for all types of SMS, including protocol translation
- High speed criteria-based classification/filtering/switching
- First Delivery Attempt (FDA) to a destination handset or ASP
- Alternate delivery options for conditional and/or optimal routing
- Forwarding to a specified SMSC or ASP through a load weighted group
- Service logic triggering for charging and enhanced message services
- Service level OA&M support (statistics and alarms) and EDR management

Messaging Manager Multigate can trigger to a message control plan based on different criteria:

- Incoming path (and hence protocol)
- Originating address (or address "domain"), and/or
- Destination address (or address "domain").

Adapters

Messaging Manager Multigate utilizes a set of adapters to provide support for different messaging protocols. Available adapters include:

Adapter	Used For
MAP Adapter	GSM networks
IS41 Adapter	CDMA and TDMA networks
SMPP Adapter	ASP/SMSC proxy connections
UCP/EMI Adapter	ASP/SMSC proxy connections
SCA Adapter	SIP connections

During inbound processing, adapters identify the arrival path and translate received messages into a common format used by Messaging Manager.

During outbound processing, routing is based on the path and the message's details and drives the adapter for that path. Each path can have a single connection to a specific machine or it can support multiple connections to the same destination and provide weighted load-sharing across several machines.

Messaging Manager Navigator

Messaging Manager Navigator provides location services for Messaging Manager and performs the following roles.

- HLR location query and cache
- HLR location query proxy with caching
- HLR emulation

Navigator can be called by other Messaging Manager components to query the HLR for the destination switch address for real time delivery of SMS. It then caches the results to reduce loads on the HLR when there is a subsequent query for the same information.

Navigator can also accept HLR query traffic, such as from a foreign SMSC attempting to locate a mobile station, and proxy the request to the actual HLR. On the return path it caches the switch address returned, then substitutes its own Messaging Manager node address as the switch address in order that the foreign SMSC will forward any stored SMS to Multigate for processing. This allows "termination services" to be applied to SMS, and, for example, anti-spam checks, to be made.

Stale cache entries are detected on delivery failure, automatically refreshed, allowing the delivery operation to retry.

Messaging Manager Manager

Messaging Manager Manager is the GUI-based design and deployment system that allows all service configuration to be created and updated for execution. This component is the major focus of this user guide.

The two main instruments for configuring Messaging Manager are:

- Routing schemes
- Message control plans

Routing schemes define the message model to Multigate and Navigator, including all message classification, filtering, triggering and routing rules. The key to configuring the full functionality of Messaging Manager is understanding the message model and routing scheme concepts described within this guide.

Message control plans leverage off Advanced Control Services (ACS), which is an underlying platform technology for service control. This is where you can customize services by placing conditional logic for service execution within the message control plan. It is also where the transaction management occurs for locking real-time charging with message delivery. You create control plans in the Control Plan Editor. For more information, see *CPE User's Guide*. For information about the available feature nodes, see *Feature Nodes Reference Guide*.

Configuration Overview

Introduction

Messaging Manager processing falls into three logical parts. Understanding the different parts is important to understand how to configure an MM service. The three parts are:

- 1 *Incoming classification (addressing)* (on page 7)
- 2 *Message processing* (on page 8)
- 3 *Outbound routing* (on page 10)

Routing schemes

Routing schemes provides configuration which is concerned with service design and message control. Routing schemes are managed from Messaging Manager Manager (hosted on the SMS).

Note: The configuration in `eserv.config` provides only the Messaging Manager configuration parameters that are global to the software (or SLC).

Routing schemes define and control the following aspects of SMS processing:

- *Adapters* (on page 77)
- *Interfaces*
- *Paths and Connections* (on page 17)
- *Transaction types* (on page 20)
- *Routing class* (on page 22)

- *Address Domains* (on page 29)
- *Congestion Control* (on page 31)
- *Screening* (on page 100)
- *Triggering* (on page 125, on page 31)
- *Routing* (on page 33)

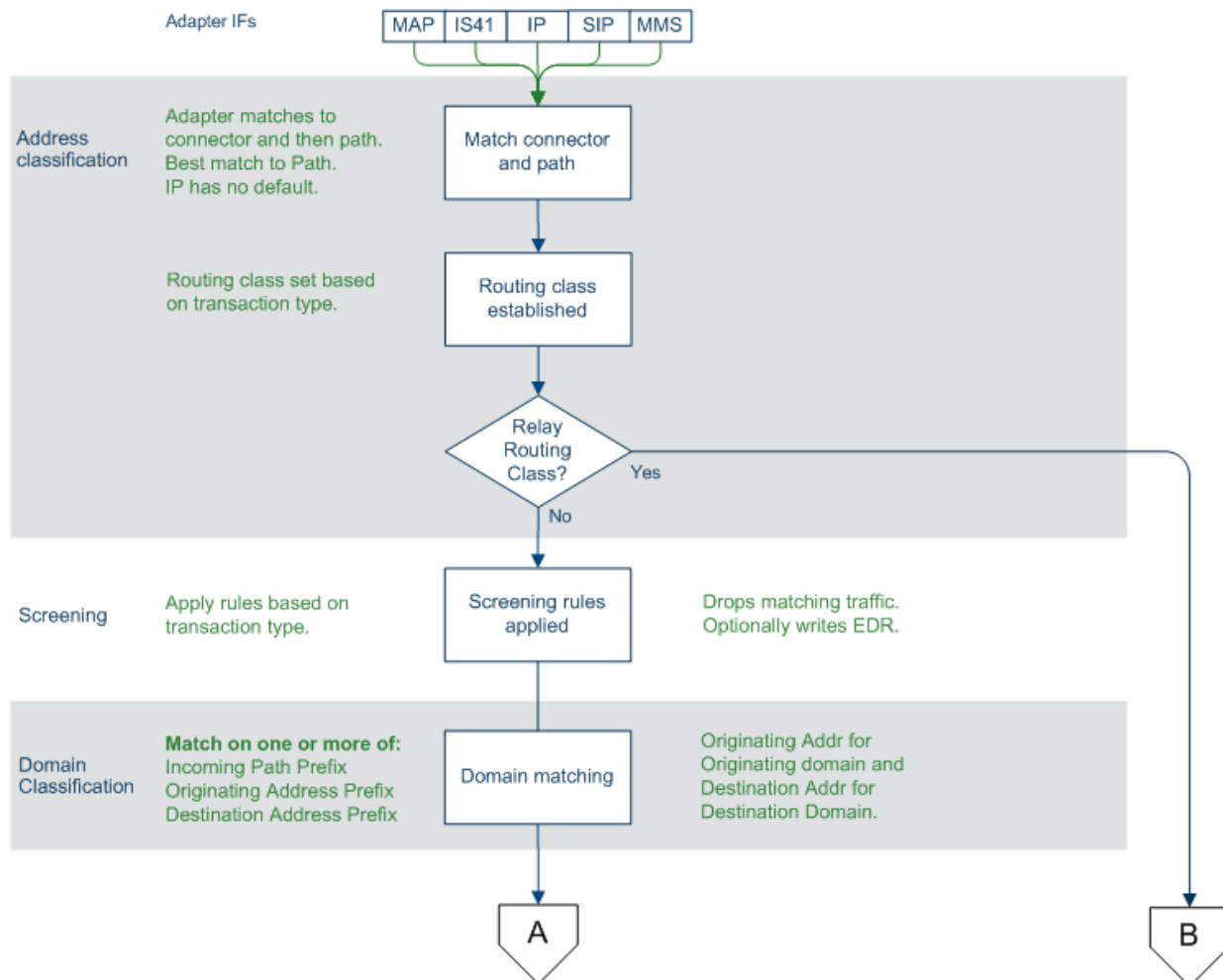
Incoming classification (addressing)

This table describes how Messaging Manager processes inbound messages.

Stage	Description
1	Messages are received over a protocol-specific adapter. The configuration of which adapter will be used is done in eserv.config. For more information about eserv.config, see <i>Messaging Manager Technical Guide</i>. For signaling protocols, the PC, SSN, GT and potentially the setting of the GPRS support parameters, are used to direct the inbound message to the correct adapter.
2	The adapter establishes the inbound connection and path for the message using the configuration in the currently deployed routing scheme. Notes: • The adapter matches against the connections in the paths which have been configured to be available to it. • The best match is used. • IP protocols do not have a default path. For more information about paths and connections, see <i>Paths and Connections</i> (on page 17).
3	A default routing class is assigned to the message, based on its transaction type. Each transaction is classified as one of Submit, Deliver, Notify, Route Info or Command. Exception: If the message has a command routing class, it will be forwarded directly to the configured default path for that protocol. For more information, see <i>Default routing</i> (on page 34). For more information about routing classes, see <i>Routing Class</i> (on page 22).
4	Each message is assigned to a default SMSC. Operations performed by Messaging Manager will take place in a fashion consistent with the assigned SMSC name. For more information, see <i>SMSCs</i> (on page 26).
5	Screening options are applied, which potentially filter out undesired messages. For more information about screening configuration, see <i>Screening Rules</i> (on page 27).
6	The originating address and destination addresses are matched against address rules to determine the originating domain name and the destination domain names. For more information about addressing rules, see <i>Address Domains</i> (on page 29).

Incoming classification diagram

This diagram shows the logic involved in processing incoming messages.



Message processing

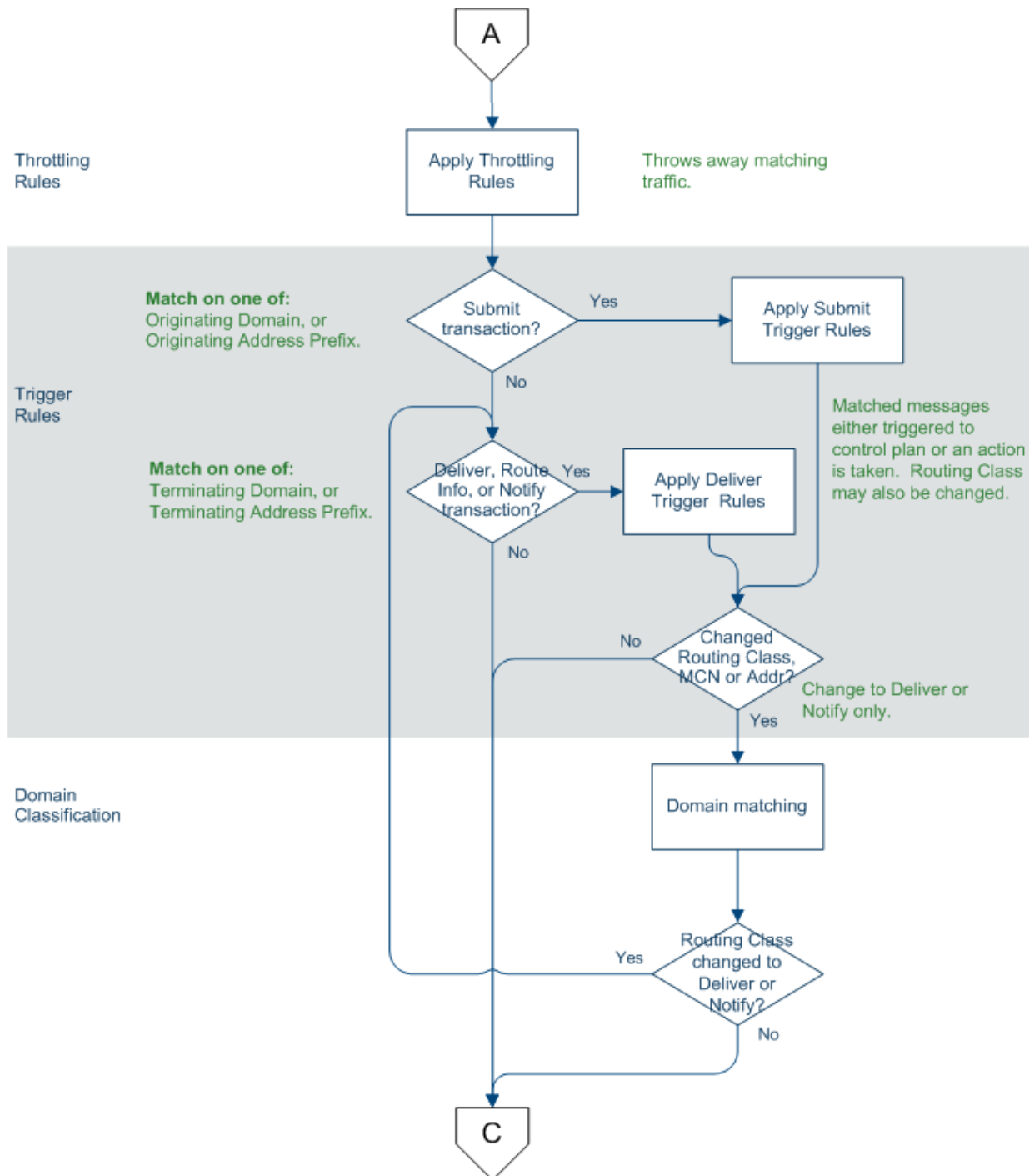
This table describes how Messaging Manager processes messages.

Stage	Description
1	Based on the criteria assigned by the classification rules, the message is checked by congestion control. This may result in transactions being throttled. For more information about throttling, see <i>Congestion Control</i> (on page 31).
2	Based on the transaction type, messages are then directed to one of four sets of trigger rules, for Submit, Deliver, Notify or Route Info transactions. This may result in triggering to ACS to run a message control plan in order to control delivery processing options. Control plans can change message parameters. Having selected a best match trigger rule it is possible to modify the transaction's routing class from its default value (assigned during incoming classification). A matching trigger rule may be one of the following: - Perform an action - Trigger to ACS to run a control plan For more information about triggering, see <i>Triggering</i> (on page 125, on page 31).

Stage	Description
3	If the message was triggered to a control plan, and the control plan returned a release INAP (that is, the control plan exited after a Disconnect node, or an error exit), the ACS release cause is mapped to an action or error code. The action or error code is added to a Nack which is returned to the source of the message. For more information about action and error codes, see <i>Messaging Manager Action and Error Codes</i> (on page 141).

Message processing diagram

This diagram shows the logic involved in processing messages.



Outbound routing

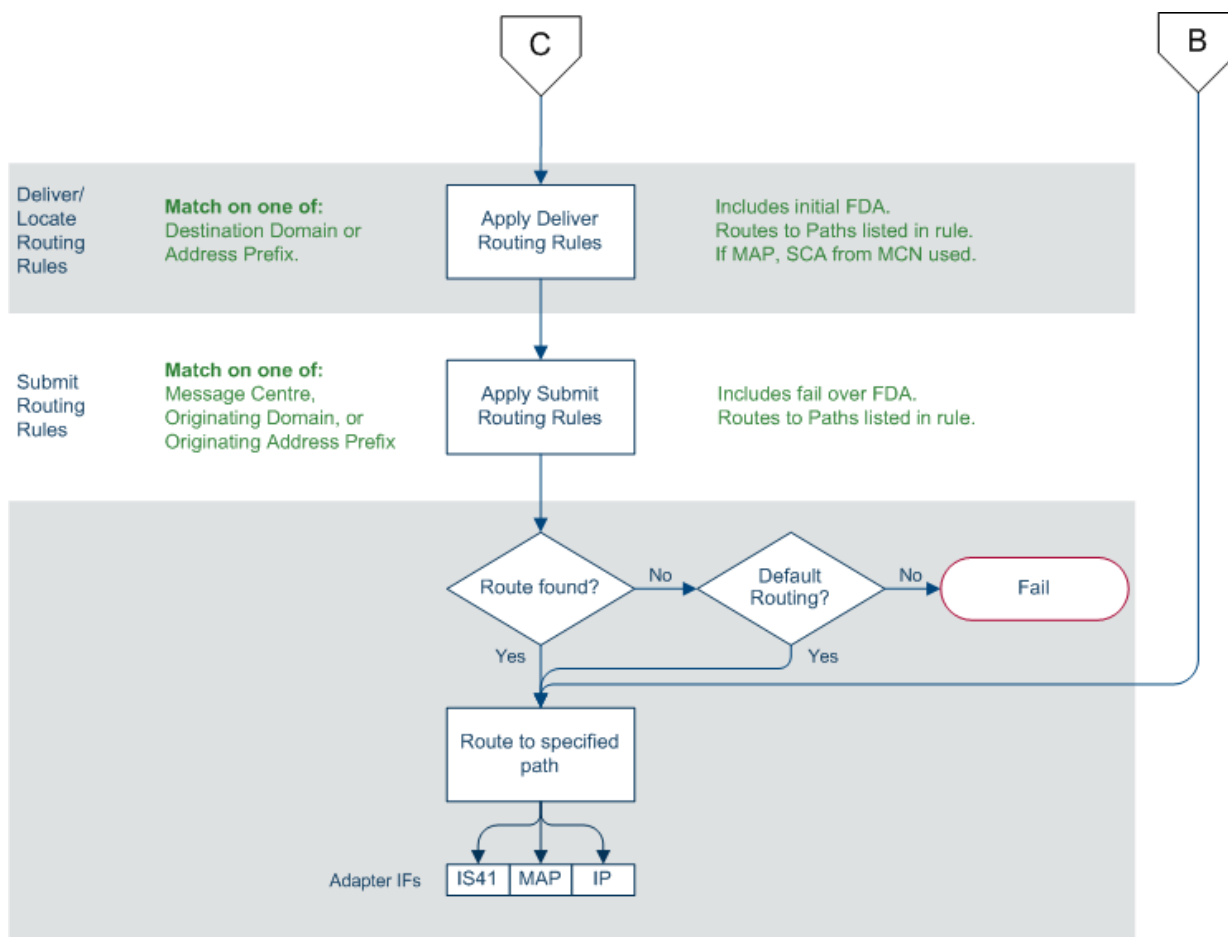
This table describes how Messaging Manager processes outbound message routing.

Stage	Description
1	Outbound routing takes place based on the routing class.

Stage	Description
	When applying: • Submit routing, the key determinant of the outbound path is the message center name and the originating or domain address. • Deliver routing, the key determinant of the outbound path is the destination domain name or prefix, and/ or originating domain name or prefix. • Locate routing, the key determinant of the outbound path is the destination domain name or prefix, and/ or originating domain name or prefix. For more information about routing, see <i>Routing</i> (on page 33).
2	One or more outbound paths may be selected by the routing rule. If there is more than one, then each is tried in turn, until "success" occurs, or a permanent error is encountered.
3	The adapter for each selected path will build the appropriate PDU, based on the path protocol, and select a connection within the path for transmission.
4	If a message control plan is active, it will be notified of the outcome from outbound routing to complete any service logic, such as finalize charging, retry by switching to an alternate route.

Outbound routing diagram

This diagram shows the logic involved in outbound routing of messages.



Interfaces and nodes

Routing nodes can provide connections for one of the following:

- All IP connections of a routing scheme
- Connections only for certain ASPs

This means a connection does not need to support all the capabilities of its associated routing scheme in order to be a valid connection.

Routing schemes can be configured with interface records. An interface record is a virtual IP connection that may be supplied or instantiated by real IP addresses on one or more routing nodes. Each node can assign a different IP address to an interface record.

Routing nodes are configured with a list of real 'IP addresses'. When a routing scheme is assigned to a routing node, you can map any of the routing scheme interfaces to the node's IP addresses. This defines what (if any) contribution that node makes to the scheme's routing interface requirements.

When is a Delivery Report produced?

Delivery Reports are generated and sent as a completely separate transaction (like other SMSs that Messaging Manager handles). That means existing routing and retry functionality can be used to deliver the DR.

Messaging Manager generates a delivery report (DR) in the following conditions:

- An 'early acknowledged' message is subsequently unable to be delivered. Messaging Manager can be configured to generate a delivery report regardless of whether or not the originator requested it (through the `alwaysProduceNonDeliveryReceipt` parameter).
- If Messaging Manager successfully delivers a message by FDA and the originating party requested a delivery receipt, then a delivery report is generated and sent to the originator

Platform Support

ACS description

Advanced Control Services (ACS) provides a call state model and service control platform for the message control plans used by MM Director to provide enhanced services.

ACS is an application support platform that allows many different types of service logic to be implemented in a common fashion. ACS runs on the Service Logic Execution Environment (SLEE). It provides the container for service logic execution in the form of user defined service control plans, as well as providing various mobile and telephony support functions. Hence ACS provides a foundation technology for users to develop and execute customer specific service logic for all forms of voice, messaging, and data services.

Service logic developed by the user is executed as an ACS service control plan. In MM service control plans are referred to as a message control plans. Message control plans are created through the ACS ACS Control Plan Editor.

CPE description

The ACS Control Plan Editor (CPE) is a graphical interface that allows the user to build service control plans. This allows the user to define multiple message control plans to implement the various message services. The CPE provides many tools that allow the user to route messages according to such factors as originating and destination addresses, MNP information, geographic location, time of day, and to collect statistical information from the message during delivery processing.

For information about the features available in the CPE, see *CPE User's Guide*.

For information about the Messaging Manager feature nodes, see *Feature Nodes Reference Guide*.

Message control plan

A message control plan is similar to a flow chart. It defines the decisions and actions made to determine the routing of a message. Exactly the same technology is used in routing voice and data calls.

A message control plan consists of multiple different decision points or actions called feature nodes. Each feature node has one entry point that is invoked after exiting a previous feature node, but may have multiple output paths. Each output path can be connected to different “next” feature node so that a directed graph is created where there are many different paths possible. Based on decisions made at execution time, each message delivery transaction will follow just one path. This means that it is simple to create services for message processing with user defined branches and actions, (that is, conditional service logic).

A message control plan can be as simple or as complex as required.

Preconfigured Packages

Introduction

Upon installation, you can install each of the following pre-configured packages automatically on each target machine. You can use the default services provided as-is, or as examples.

- EDR - Express Delivery Routing
- PME - Personal Message Exchange
- SAF - SMS Anti Fraud
- VAS - Value Added Services

Package structure

This table describes the components configured with each package.

Component	EDR	PME	Home Routing	SAF
SS7	Yes	Yes	Yes	Yes
Inbound MO	Yes			Yes
Outbound MO	Yes			Yes
VAS	Yes			Yes
Inbound MT		Yes	Yes	Yes
Outbound MT	Yes	Yes	Yes	Yes
Internet		Yes		
EDR	Yes			
PME		Yes		
SAF				Yes

Components

This table describes the function of each field.

Component	Description
SS7	MAP/CDMA adapter.
Inbound MO	- MAP/CDMA SME path (already created by SS7 component) - Set local domain if match local network prefix
Inbound MT	- MAP/CDMA MC In path (already created by SS7 component) - Set default routing path to built-in SME - Set destination domain to local.
Outbound MO	MAP/CDMA MC Out path, set as default routing path for corresponding SME path.
Outbound MT	MAP/CDMA SME path (already created by SS7 component).
VAS	- SMPP/EMI adapter - SME path/connection for each ASP. - If IP address specified for SMSC, create MC path/connection and make default - routing path for ASPs.
Internet	Email / IM adapters and paths, configured to match the SCA and SEI applications.
PME	- Trigger all local MT to PME control plan - Trigger MO to (enhanced) direct SMS to email / IM to the corresponding control plan. Maybe needs to be another package or component. - Trigger all other MO to control plan that does direct delivery only, but EDR triggering takes precedence. This isn't necessary as we have to intercept MT from the local SMSC anyway, but is more efficient. - Definition of profile tags. For more information, refer to Personal Message Exchange.
EDR	Trigger all MO to control plan that does FDA.
SAF	- Turn on all screening rules - Default routing of inbound MO messages will apply.

Default control plans

This table describes the function of each default control plan.

Control Plan	Description	More Information
Direct_Delivery	Sets message routing class to 'Deliver' and then attempts to deliver it.	<i>Routing Class</i> (on page 22).
EDR	Sets message routing class to 'FDA' and then attempts to deliver it.	<i>Routing Class</i> (on page 22).

Control Plan	Description	More Information
Email_to_SMS	Takes incoming email messages and translates parameters and addresses in order to allow SMS delivery. Included as a sub-control plan in PME_Delivery.	
Enhanced_SMS_to_Email	Looks up the last digit of the destination address (number) and sends the message as an email to the corresponding email address book entry.	MM IM/Email.
Enhanced_SMS_to_IM	Looks up the last digit of the destination address (number) and sends the message as an IM to the corresponding IM address book entry.	MM IM/Email.
IM_to_SMS	Takes incoming IM messages and translates parameters and addresses in order to allow SMS delivery. Included as a sub-control plan in PME_Delivery.	<i>Instant Messaging</i> (on page 229)
PME_Delivery	General delivery control plan with PME functionality.	PME Delivery.
PME_Provisioning	Interprets the SMS and sets PME configuration items for the subscriber.	PME Provisioning.
SMS_Submit	Classifies incoming submit messages by type (SMS, IM or email) and processes IM and email addresses for messages of those types.	
SMS_to_Email	Takes the first word of the message body as an email address, and sends an email to that address with the rest of the SMS message body as the email message body.	<i>SEI Technical Guide</i>
SMS_to_IM	Takes the first word of the message body as an IM address, and sends an IM to that address with the rest of the SMS message body as the IM message body.	<i>Instant Messaging</i> (on page 229)
SMS_to_IM_via_TAN	This control plan will be set to trigger on numbers in the temporary access number range. The destination address (temporary access number) is looked up, and the associated IM address is used to send the message on as an IM. Included as a sub-control plan in SMS_Submit.	

Refer to PME Control Plan Scenarios for examples of these control plans.

Message Routing and Processing

Overview

Introduction

This chapter explains how Messaging Manager routes and processes messages and the key concepts involved in understanding the routing and processing configuration options available in the GUI.

In this chapter

This chapter contains the following topics.

Paths and Connections	17
Transaction Types	20
Routing Class	22
SMSCs	26
ASP Groups and Parameters	26
Screening Rules	27
Address Domains	29
Congestion Control	31
Triggering	31
Routing	33

Paths and Connections

Introduction

All message traffic entering and leaving the VMP does so through a communication channel known as a **path**. A path is a logical entity that contains one or more **connections** of the same type.

Paths

Paths are a simple abstraction concept which is used when configuring the rest of the system. By mapping connections to paths the complexity of each connection is encapsulated and hidden within the path itself. The path then becomes the "communication port" visible to other parts of the messaging processing model.

Each path has a name. Using a naming convention for paths helps to manage the configuration (for example: paths are the means of identifying where traffic is being routed, and paths are also the lowest level at which statistics can be collected).

Inbound paths

All inbound traffic is assigned an inbound path based on the path configuration and the message details (including which adapter the message arrived over). The inbound path enables the user to categorize and manage the message in the Messaging Manager configuration. Inbound paths can be used to treat message services in different ways, even where the messages are almost identical to those arriving on other paths.

Example: Given a specific address (such as the short code "123") it is possible to assign a different address domain name based on the inbound path, effectively providing multiple address spaces.

Outbound paths

All outbound routing functions take through a selected path.

Warning: Since a path may have multiple connections, it is important that each connection within an outbound path can be used to reach the same destination(s), otherwise the configuration may result in frequent routing failures.

Connections

Connections define the details required to connect to another entity on the network which handles short messages. All short message traffic in or out of the VMP will occur through a connection.

Because Messaging Manager supports multiple messaging protocols which require different configuration, connections have complex configuration, which is different depending on the protocol used.

Connections may be:

- Socket-based IP connections, as are used for communication between an ASP and SMSC. Socket-based protocols (such as SMPP and EMI) are straightforward. Each connection corresponds to a TCP connection in the underlying transport layer.
- Signaling-based virtual connections that are used between network elements. Signaling protocols are considered virtual connections because they do not correspond to the underlying (SUA/SIGTRAN) transport layer connections. Instead, they relate to network elements addressed within the SCCP layer (and above) and the ability to use a TCAP transaction as a temporary connection for the purpose of message transmission.

IP paths

Each IP connection is associated with a path, but a path may have many connections that can provide the same service.

For example, an ASP may have several machines that can be used to provide a common set of content-based services. Messaging Manager Multigate can have a separate connection configured to each server so that any load can be shared across these servers. If one server is unavailable, this is transparent to the system as a whole, and hence the service is not impacted. To achieve transparent failover, all IP connections available to an ASP should be configured in a single path. As long as one connection is open, then the path is available and the service is also available. Load distribution is defined by setting a weighting for each server in the path.

To simulate ASP connections to an SMSC, each separate ASP service may need its own path and connection(s) defined between Messaging Manager Multigate and the SMSC. By doing this, Messaging Manager will appear to be a range of ASPs to the SMSC and the administrator can define how the ASP-Multigate paths map to the Multigate-SMSC paths. This may be one of:

- 1:1, to proxy traffic through from a "real" ASP to the SMSC and vice versa
- N:1 to aggregate ASP traffic down to one (or a few) connections to an SMSC

Signalling paths

Because all destinations can be reached through the signaling network, connections and paths can be used to partition communication across all the network elements into separately-manageable streams. These are known as signaling paths.

Outbound

Example: A network has several SMSCs that can be used for store-and-forward processing. To configure them correctly, you need to decide how you want to control the traffic that is sent to each individual SMSC.

- If the SMSCs are to be used as a group of redundant store-and-forward nodes, then they can be represented as connections on a single path. Each SMSC connection can be given a weighting so that the path will be used to distribute traffic according to available capacity. In this manner it is simple to process the "submit" traffic and route it for store-and-forward processing while hiding the complex details about the SMSC cluster from the Messaging Manager system behind a single path.
- To route traffic to SMSCs based on specific transaction properties, each SMSC should be configured on a separate path. This enables routing decisions to be made and traffic to be conditionally directed to the appropriate path.

For other network destinations (predominantly traffic direct to subscriber handsets through an MSC), it is possible to have a single path that can reach all destinations. However, this traffic can also be arbitrarily split into more than one path, to enable other functionality such as collecting statistics for different destinations.

Inbound

Many inbound classification and filtering rules use the inbound path as a discriminator. Consequently inbound paths must be defined with downstream service logic in mind.

Example: Subscribers may be given a Service Center Address (SCA) as part of the subscribed service profile. This is then transmitted in each SMS sent through the VMP. The SCA value can be used to match a signaling connection, and hence an inbound path. Other SCCP parameters, such as the SSN, the Point Code, or the Global Title Address can also be used to match incoming traffic onto virtual connections and inbound paths. So, although all signalling is received over a set of SIGTRAN links, the traffic can be divided into various streams by the administrator and assigned to different inbound paths. So Messaging Manager can implement a "Virtual SMSC" by mapping the incoming SCA onto a path, then treating traffic arriving over that path in a special manner.

Connection and path identification

Each adapter instance receives messages on one of many different connections defined for that adapter instance. Whenever an inbound message is received, the adapter must determine which connection the message arrived on, and map the connection to the associated inbound path.

For IP protocols (SMPP, EMI, and SIP), this is straightforward because the TCP connection on which a message is received correlates directly with a configured logical connection. A relationship between the TCP connection and the logical connection is established when the TCP connection is created.

For SS7 protocols (IS41 and MAP), there is no persistent connection across messages, so instead, Messaging Manager matches a logical connection to a message by comparing the SCCP address of the originating node (contained in the message) with the list of defined connections. Once the best match is established, it is used to identify the inbound path for that message.

A MAP connection is considered a match for an:

- MO-FSM message if its:
 - GT, SSN, PC match the message's SCCP CgPA parameter
 - SCA is an exact match of the message's RP-DA parameter
- MT-FSM message if its:
 - GT, SSN, PC match the message's SCCP CgPA parameter
 - SCA is an exact match of the message's RP-OA parameter

Only one path and connection can be assigned.

SS7 connection matching rules

Since Messaging Manager allows the value "ANY" to be used in a connection's GT, SSN and PC specification, the potential exists for many matches. This table shows the set of rules for identifying the best match on a connection.

Precedence	RP-DA (MO-FSM) RP-OA (MT-FSM)	CgPA PC	CgPA SSN	CgPA GT
1 (best match)	Exact Match	Exact Match	Exact Match	Prefix Match
2	Exact Match	Exact Match	Exact Match	ANY
3	Exact Match	Exact Match	ANY	Prefix Match
4	Exact Match	Exact Match	ANY	ANY
5	Exact Match	ANY	Exact Match	Prefix Match
6	Exact Match	ANY	Exact Match	ANY
7	Exact Match	ANY	ANY	Prefix Match
8	Exact Match	ANY	ANY	ANY
9	ANY	Exact Match	Exact Match	Prefix Match
10	ANY	Exact Match	Exact Match	ANY
11	ANY	Exact Match	ANY	Prefix Match
12	ANY	Exact Match	ANY	ANY
13	ANY	ANY	Exact Match	Prefix Match
14	ANY	ANY	Exact Match	ANY
15	ANY	ANY	ANY	Prefix Match
16 (worst match)	ANY	ANY	ANY	ANY

Transaction Types

Introduction

The Messaging Manager Multigate system handles inbound messages slightly differently based on the transaction type, and assigns a different default routing class to each one. The routing class is the primary control value for determining how the message will be subsequently handled for onward routing.

Regardless of which path is assigned, all inbound messages are classified as being one of the transaction types in this table.

Transaction Type	Description
Submit	MO SMS from a handset or Submit from an ASP.
Deliver	Any of: - MT SMS from a foreign SMSC - local SMSC (including sending to an ASP) - FDA
Notify	All delivery receipts.
Route Info	HLR every request to determine the MSC that is serving a handset.
Command	All other message types.

Note: IP protocols use terms Submit and Deliver, SS7 uses MO and MT.

Submit type

A **Submit** transaction refers to a message that is being introduced into the messaging network (for example: MAP MO_FSM, IS41 SMDPP (Submit), SMPP submit_sm or EMI). These messages originate from a subscriber on the network or from an external ASP connected to the network. Typically these messages need to be authorized and are subject to charging operations.

When the message first passes through the detection point in Messaging Manager Multigate, Submit transactions are assigned a routing class of "Submit".

To provide extended service control for Submit transactions, including charging and/or routing control, the customer may implement one or more message control plans that are triggered through the Submit trigger rules.

Deliver type

A **Deliver** transaction refers to any attempt to deliver a message directly to the destination address (for example: MAP MT_FSM, IS41 SMDPP (Deliver), SMPP deliver_sm or EMI). This may occur during the First Delivery Attempt (FDA) that takes place from within Messaging Manager Multigate during a Submit transaction processing, or due to any subsequent delivery attempt that is intercepted from the network. Messages that are delivery attempts from a foreign SMSC may be redirected to Multigate by Navigator and will enter the system as a Deliver transaction.

When the message first passes through the detection point in Messaging Manager Multigate, Deliver transactions are assigned a routing class of "Deliver".

To provide extended service control for Deliver transactions, the customer may implement one or more message control plans that are triggered through the Deliver trigger rules.

Notify type

A **Notify** transaction refers to a delivery receipt (DR) message. These are typically intercepted by Messaging Manager Multigate after an SMSC completes its final delivery attempt (successful or not) and purges the SMS.

When the message first passes through the Detection Point in Messaging Manager Multigate, Notify transactions are assigned a routing class of "Deliver".

To provide extended service control for Notify transactions (including refunds on non-delivery), the customer may implement one or more SMS Service Plans that are triggered through the Notify trigger rules.

RouteInfo

The **RouteInfo** transaction is a request which is sent to an HLR to determine information regarding a destination handset prior to send SS7 deliver transactions. Information can include:

- The address of the MSC currently serving the handset
- GPRS subscription information
- IMSI
- LMSI
- MIN
- ESN

Command type

All other messages are considered **Command** transactions and are assigned a routing class of "Relay".

Note: These messages do not undergo further processing, but are immediately directed to the default outbound routing path that was configured for the message's inbound path.

Summary

To summarize, when a message passes through a detection point it is assigned, each transaction is assigned the following default routing class.

Transaction	Routing Class
Submit	Submit
Deliver	Deliver
Notify	Deliver
Route Info	Locate
Command	Relay

Routing Class

Introduction

Routing classes are the message attribute which has the greatest impact on outbound routing control. The routing class is first assigned a default value based on the transaction type (for more information, see *Transaction Types* (on page 20)). The default routing class can be overridden by subsequent service logic and set to a new value. Assigning new routing classes enables dynamic control over routing.

Although outbound routing is one of the last events in the message model, it is useful to understand routing classes when setting up inbound configuration because a lot of the inbound configuration is used to set up the transaction for its eventual outbound routing treatment.

Routing class overview

There are five defined routing classes, and each class has its own method of determining “how” and “where” to send a message. All routing classes ultimately result in external operations.

Routing Class	Method Description
Default routing	Uses the default routing path attached to the inbound path.
Submit	Applies almost exclusively to Submit transactions and indicates to Multigate that it should attempt to "submit" (or forward) the message to an SMSC. From the SMSC viewpoint the message arrives in exactly the same manner as if it came directly from the network switch, or a connected ASP. Hence Messaging Manager stands in the submission path to apply enhanced services and acts as an SMS Proxy between the originating party and the SMSC.
Deliver	Can be applied to Submit, Deliver and Notify transactions and indicates to Multigate that it should attempt to "deliver" (or forward) the message directly to the destination. From the destination viewpoint the message arrives in exactly the same manner as if it were being forwarded by the SMSC. Hence Messaging Manager provides enhanced services and acts as an SMSC.
FDA	Applies mainly to Submit transactions and indicates to Multigate that it should perform First Delivery Attempt routing. This means a new Deliver transaction is created and this will drive the Deliver method as described above. However, in the event the Deliver does not succeed, the Submit method is driven for the transaction. Hence the FDA routing class makes use of the Deliver and Submit routing classes in order to drive service logic and external operations.

Routing Class	Method Description
Locate	Causes the RouteInfo (MAP SRI4SM or IS41 SMSRequest) message to be sent to an HLR, using the configured Locate routing rules.

Behaviour

When performing routing, Messaging Manager behaves in the manner appropriate for that routing class and as expected by the destination. For:

- Signaling paths, where the destination is an:
 - SMSC, Messaging Manager appears to be an MSC
 - MSC, Messaging Manager appears to be an SMSC.
- IP connections, where the destination is an:
 - SMSC, Messaging Manager appears to be an ASP
 - ASP, Messaging Manager appears to be an SMSC.

Default routing

Messages with the Default routing class are routed directly to the default outbound path configured for the inbound path they arrived on. The outbound path will have the same protocol, but must be a different path.

Default routing rules are configured in the path definition. Any given path may have a "Default routing path" assigned, and (to support aggregation) more than one inbound path can use the same outbound Default routing path.

If outbound routing is called upon to perform "Default routing" routing and no outbound Default routing path is defined for the inbound path, then the transaction is failed.

Default routing routing is used for Command transaction types. When the message arrives, the outbound routing is actioned immediately. Such transactions do not pass through the upper layers of the message model, but are simply transferred from the inbound to the outbound path. Messaging Manager does not process these messages.

It is possible for an inbound path to have no associated outbound "Default routing" path (that is, Default routing routing is disabled for this path). Transactions attempting a Default routing operation from such an inbound path will fail with a Permanent Error and a message is logged to Intensive Logging.

Submit

For the Submit routing class, Multigate expects to send a "submit" PDU to a message center. The type of PDU will depend on the outbound path selected, and hence the actual protocol to be used. It does not depend on the inbound protocol.

For example, if it is a:

- MAP path, then a MAP MO_FORWARD_SHORT_MESSAGE will be constructed
- SMPP, a submit_sm PDU will be constructed

The PDU is then sent over one of the connections available for that path.

In either case, an SMSC is expected as the end-point. The path(s) to be used are configured as Submit rules in the Routing table. These rules mean that a "best match" is made to select the routing entry. More than one path can be defined for a routing entry, and each will be tried until one of the following occurs:

- "submit" is successful
- A permanent error occurs

- The path list is exhausted

If there is no "best match" Submit rule in the Routing table rule, Multigate will attempt a Default routing operation.

Note that Submit routing really only makes sense for Submit transactions.

Deliver

For the Deliver routing class, Multigate expects to send a "deliver" PDU to the final destination. The type of PDU will depend on the path selected, and hence the actual protocol to be used.

For example, if it is a:

- MAP path, then a MAP MT_FORWARD_SHORT_MESSAGE (MAP v3), or FORWARD_SHORT_MESSAGE (MAP v1 or v2) will be constructed
- SMPP, a deliver_sm PDU will be constructed

The PDU is then sent over one of the connections available for that path.

In either case, an SME (that is, either an MSC or ASP) is expected as the end-point. The path(s) to be used are configured as Deliver rules in the Routing table. These rules mean that a "best match" is made to select the routing entry. More than one path can be defined for each given routing entry, and each will be tried until one of the following occurs:

- "deliver" is successful
- A permanent error occurs
- The path list is exhausted

If there is no matching Deliver rule in the Routing table, Multigate will attempt a Default routing operation.

Note: The Deliver routing class can be used from a Submit, Deliver or Notify transaction.

Submit transactions

When used from a Submit transaction, the Deliver routing class requests what is sometimes referred to as a "single shot" delivery. In this case the current transaction is suspended and a new transaction is invoked with:

- The same Inbound Path
- The same Originating and Destination Address domains
- A routing class of Deliver

This new Deliver transaction proceeds through inbound processing to trigger control and may trigger Deliver service logic.

If the Deliver transaction:

- Succeeds, the original Submit transaction is deemed successful
- Fails, the original Submit transaction fails as well

This is why it is referred to as single shot delivery.

Deliver and Notify transactions

The Deliver routing class is the standard mode of delivery for a Deliver or Notify transaction. The transaction is synchronous with the delivery of the message to its final destination. If the Deliver processing is successful, the Deliver transaction is deemed successful, otherwise the Deliver transaction fails. The originating party is then notified of the outcome through a protocol level acknowledgment.

Locate

For the Locate routing class, Multigate expects to send a "RouteInfo" to the HLR. The type of message will depend on the path selected, and hence the actual protocol to be used.

For example, if it is a:

- MAP path, then a SEND_ROUTING_INFO_FOR_SM will be constructed
- CDMA, a SMSRequest will be constructed

The message is then sent over one of the connections available for that path.

In either case, an SME (that is, an HLR) is expected as the end-point. The path(s) to be used are configured as Locate rules in the Routing table. These rules mean that a "best match" is made to select the routing entry. More than one path can be defined for each given routing entry, and each will be tried until one of the following occurs:

- "RouteInfo" is successful
- A permanent error occurs
- The path list is exhausted

If there is no matching Locate rule in the Routing table, Multigate will attempt a Default routing operation.

FDA

For the FDA routing class, Multigate expects to perform a first delivery attempt of a "deliver" style protocol unit over a path that has an SME (ASP) as the end-point.

Note: The FDA routing class can be set for a Submit, Deliver or Notify transaction.

Submit transactions

When used from a Submit transaction the FDA routing class requests what is commonly referred to as a "first delivery attempt". In this case the current transaction is suspended and a new Deliver transaction is invoked with:

- The same Inbound Path
- The same Originating and Destination Address domains
- A routing class of Deliver

This new Deliver transaction proceeds through inbound processing to trigger control and may trigger Deliver service logic.

If the Deliver transaction:

- Succeeds, the original Submit transaction is deemed successful and completes normally without further external operations.
- Fails, then the original Submit transaction resumes by invoking the Submit routing class. If this is successful then the Submit transaction completes normally.

Only in very rare cases will both the Deliver and Submit routing classes fail and result in Submit transaction failure.

Deliver and Notify transactions

The Deliver routing class is the standard mode of delivery for a Deliver or Notify transaction. The transaction is synchronous with the delivery of the message to its final destination. If the Deliver processing succeeds, the Deliver transaction is deemed successful, otherwise the Deliver transaction fails. The originating party is then notified of the outcome through a protocol level acknowledgment.

SMSCs

Introduction

Based on the incoming path, all messages arriving at the VMP are assigned to an **SMSC**. This is a key aspect of Messaging Manager as it acts as a Virtual Message Point (VMP). For each Submit transaction it can attempt to deliver messages as though they came from the SMSC assigned to the transaction and will use this SMSC to store undelivered messages, if necessary.

Defining SMSCs

Within a routing scheme the administrator may define as many SMSCs as required. Each SMSC record should correspond to an actual SMSC, or a group of network elements (each may be a separate SMSC) that together implement an SMSC.

The main consideration is that an SMSC has a Global Title Address that is used as the Service Center Address (SCA) in various network transactions. For example, when Messaging Manager attempts delivery to a handset, it will perform an HLR lookup. This is a MAP `SEND_ROUTING_INFORMATION_FOR_SM` in GSM networks and carries the SCA. If the device is not available then the SCA is placed in the MWD (Message Waiting Data) in the HLR and when later the device becomes available the HLR sends an alert to the SCA. Hence this same SMSC is also where the message will be stored by the Submit method.

The SMSC is assigned based on the incoming path, but more than one path (even all paths) can be assigned to a single SMSC. During message control and processing it is possible to change the assigned SMSC, but this is then preserved throughout a Delivery routing and (if required) the Submit routing process.

ASP Groups and Parameters

ASP accounts

An ASP account contains information about an Application Service Provider (ASP). It records the services it provides and the limits which restrict how it can use the system. ASP accounts are a type of ACS customer, and use the ACS customer profile. For more information about ACS customers, see *ACS User's Guide*.

ASP groups and templates

Every ASP account belongs to an ASP group. ASP groups define the default information for all the ASP accounts within that group. This can be used to streamline configuration by allowing a common parameter to be changed at one point, and automatically propagate that change to all appropriate ASP accounts.

Similarly, ASP accounts can be constructed as a templates. Templates are incomplete ASPs which can be cloned into one or more fully-functional ASP accounts. An ASP account template cannot be used as an ASP account (that is, it cannot be used to create paths and connections in a routing scheme). An ASP account cannot be used as a template for creating other ASP accounts, only templates can be used for this purpose.

ASP groups and parameter defaults

Any ASP account parameter that is editable at group level can be defaulted to group level (that is, a value is not required for it at the ASP account level). All parameter widgets which can be edited at the group level will be displayed with a **Default to group level** check box. If the parameter cannot be edited at group level, the check box will not be displayed. If the Default to group level check box is selected, the parameter at the ASP account level will be defaulted to the value set at the ASP group level. This value is not saved in the ASP account profile, and any value already there will be removed if and when the dialog is saved.

Tip: The value stored at the ASP group level is displayed in a tool tip when the mouse is hovered over the default check box.

Screening Rules

Screening rule list

The set of screening rules available is different for each transaction type as shown in the following table.

Rule Type	Submit	Deliver	Notify	RouteInfo
<i>Calling Party Filter</i> (on page 27)	Y	Y	Y	Y
<i>Delivery Sequence Correlation</i> (on page 28)		Y	Y	
<i>Destination Address Screening</i> (on page 28)	Y	Y	Y	Y
<i>Isolated Delivery</i> (on page 28)		Y	Y	
<i>Layer Address Correlation</i> (on page 28) (GSM only)	Y	Y	Y	Y
<i>Originating Address Screening</i> (on page 29)	Y	Y	Y	
<i>Roaming Location Validation</i> (on page 29)	Y			

Notes:

- Screening rules are not applied to traffic from any path which has the **This is a trusted path** check box selected. For more information about this check box, see *Path screen fields* (on page 84).
- To use the full screening capabilities, a valid screening license must be purchased. Unlicensed users will only have access to the originating address screening and destination address screening rules.

Monitoring screening rules

If a screening rule is in monitoring state, the rule is not applied. Instead an EDR is written recording the SMS/call details, and the screening rule ID for the rule which would have blocked the SMS/call.

Note: If a rule is in monitoring state, an EDR will be written regardless of whether the **Write EDR** check box is selected for that rule.

For more information about EDR post-processing, see *EDR Reference Guide*.

Calling Party Filter

This check is used to:

- Screen out (blacklist) known rogue entities on the network (pirates)

- Allow (white list) known safe entities

A message will be screened if all of the following apply:

- It is received on a path that does not have the **This is a trusted path** check box selected
- The “Calling Party Filter” rule is configured for the message's transaction type
- The message's SCCP calling party global title is matched by the screened global title list

When this rule is selected the *Global Title Screening Rules* (on page 107) panel is displayed on the screen.

Delivery Sequence Correlation

If an inbound deliver or notify message is received on a path that is not flagged as trusted and the “Delivery Sequence Correlation” rule is specified, Messaging Manager will compare the message parameters with the corresponding RouteInfo that was previously received. Message parameters are matched as follows, and the message is screened out if any of the comparisons fail:

MT SMS Field	Expected Value
SCCP Calling Party	SCCP calling party of the RouteInfo
SCCP Called Party	GT returned by Messaging Manager in response to the RouteInfo
SCA	SCCP calling party of the RouteInfo

Destination Address Screening

Destination address screening rules check the digits of the destination address against a configured list of prefixes. For each address prefix, an address rule will specify that the message has either passed or failed screening.

If the address rule is a:

- 'pass' rule, it will assign a destination domain for subsequent processing.
- 'fail' rule, it will specify the action to take.

When this rule is selected the *Destination Screening Rules* (on page 111) panel is displayed in the bottom part of the screen.

Isolated Delivery

When a mobile-terminated SMS (MAP MT-ForwardSM and IS41 SMDPP) is received, the isolated delivery rule checks that a RouteInfo message (HLR lookup) was received before the SMS. If a delivery sequence correlation rule (described above) is also used, Messaging Manager will check that the details in the two requests match up.

If MSID masking is on, or an Accept action is used, MM responds to incoming RouteInfo messages with a temporary IMSI (or MIN). This means that when a subsequent deliver or notify message is received, it will use the MM-generated IMSI, so can be linked with the previous RouteInfo.

If an inbound deliver or notify message is received on a path that is not flagged as trusted, the “Isolated Delivery” rule will check that the IMSI corresponds to one that was previously generated in response to a RouteInfo. The message will be screened out if this is not the case.

Layer Address Correlation

When a message is received, MM can do a basic check to ensure that the parameters provided in the SCCP layer and MAP layer are consistent.

If this rule is used and a MAP message is received on a path that is not flagged as trusted, MM will verify that the prefixes of the following MAP and SCCP address match:

Message Type	SCCP Field	MAP Field
RouteInfo	CallingParty	Service Centre Address
Deliver / Notify	CallingParty	SM-RP-OA
Submit	CalledParty	SM-RP-DA

The number of digits to compare for the SCA Consistency check is determined by finding the longest country prefix matching the address, in the *SCA Consistency Rules* (on page 109) panel displayed in the bottom part of the screen.

Originating Address Screening

This rule checks the digits of the originating address against a configured list of prefixes. For each address prefix, an address rule will specify that the message has either passed or failed screening.

If the address rule is a:

- 'Pass' rule, it will assign an originating domain for subsequent processing
- 'Fail' rule, it will specify the action to take

When this rule is selected the *Originating Screening Rules* (on page 111) panel is displayed in the bottom part of the screen.

Roaming Location Validation

An additional correlation check can be applied to mobile-originated SMSs (MAP MO-ForwardSM and IS41 SMDPP) to validate that when a message comes from a local subscriber via a foreign network, that subscriber is actually known to be roaming.

If a mobile-originated SMS is received on a path that is not flagged as trusted, this rule will force Navigator to query the HLR to determine the MSC serving the originating subscriber. A message will pass if the Calling Party SCCP Address and MSC address from the HLR match, to the determined number of digits.

When this rule is selected the *RLV Prefix Rules* (on page 114) panel is displayed in the bottom part of the screen.

Address Domains

Introduction

Each message transaction involves an originating address as the message sender, and a destination address as the message receiver. These are generally E.164 or Short Dial Code (SDC) digit strings.

Messaging Manager enables you to assign an originating domain and a destination domain for each message based on the originating and destination address and/or incoming path. Messaging Manager uses domains as one of the criteria for matching when performing throttling, triggering and routing.

Note: If no domain is configured, the message will use the default domain.

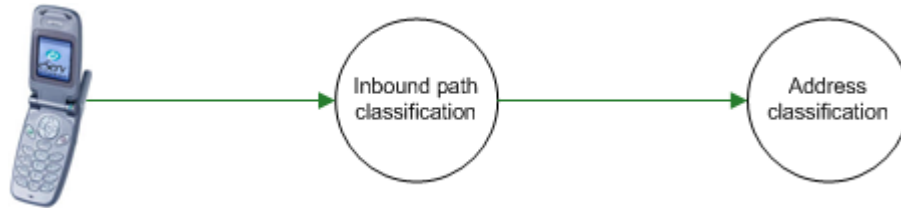
By setting up domains to group addresses subsequent message processing and routing configuration can be simplified.

Examples:

- By using one or more address or path prefix matches you may group together all the numbers that belong to a specific operator into a single domain, and then name the domain so the ownership of the numbers is obvious.
- A domain can be defined to contain all "foreign international" numbers.
- For an ASP the same approach can be used to group any SDC numbers into a domain that is named to reflect the service provider.

Domain classification

Here is a simple diagram showing an inbound message going through the domain classification process.



Example: If a message arrives with an Originating address of 021 185 3821, Messaging Manager looks up originating address screening and destination address screening rules to find a match.

Example address classification

This table shows a typical address classification table.

Path Prefix	Address Prefix	Address Domain
Foreign	1	USA
Foreign	61	Australia
*	031	Telefony
*	035	Teleco 3
Test	0219	Test

Using the above table, Messaging Manager uses the path and originating address to find a match on the listed prefixes. When a match is found, the originating domain will be assigned from the Address domain for the rule. In this example, the path name of "any" and prefix of 035 results in an originating domain of Teleco 3 being selected.

By using the inbound path name as a qualifier there can actually be many "address spaces" set up for the same numbering scheme. For example, even where the originating address is the same for two messages, depending upon which path the message takes into Messaging Manager it can be placed into a different domain.

As another example, based on the SCA, an inbound path can be assigned (described as "virtual SMSC" support above) and then the terminating address (say 333) can be assigned to a different terminating domain name - one may be "Sport" and another "Weather". This means that the same destination number (333) can be routed to a different application as they "appeared" to be sent to a different SCA and hence Messaging Manager can implement behavior associated with the different SMSCs.

The originating domain name is significant in Submit processing rules and the terminating domain name is used for Deliver processing rules.

Congestion Control

Throttling rules

Throttling rules match on domain and transaction type. A "best match" throttling rule is selected by the transaction and this rule will specify the congestion point for such a transaction.

For a matched domain, it starts to drop traffic when the total traffic is above the specified limit. Matching on domain enables Messaging Manager to throttle different services at different congestion points.

Applying throttling

The throttling congestion point is simply a percentage value and indicates the point at which this type of transaction is considered to reach a point of congestion in the system and be throttled. The value relates to the overall concurrent transaction limit for the system.

Example: By setting a value of 75%, for a given domain (like Televoting) then, in effect, the administrator is ensuring there is a 25% headroom for other types of transactions. Televoting transactions will be throttled when the system has reached 75% capacity and hence a Televoting event cannot cause disruption to all other types of messaging.

Triggering

Introduction

Triggering rules provide the core message processing functionality. Messages which match transaction type and domain and/or address prefix are processed in one of the following ways:

- By using a specified control plan.
- By performing a specified action. Available actions are: route, route unchanged, relay, accept, reject, or discard.

Matching messages can also have their routing class changed.

By triggering to a message control plan, extended service logic can be applied to perform more detailed checks and processing on the message; for example, to filter out unwanted transactions (anti-spam function), or to apply charging or alternate routing controls.

The trigger rule also provides the first opportunity to select a transaction in order to apply a new action or routing class, thus changing the default value.

Example: If you require all Submit messages to undergo a First Delivery Attempt (FDA), then it makes sense to set the routing class to FDA on the appropriate Submit trigger rules. This means that the message control plan does not need to set the routing class, and if a control plan is not used the processing will continue with the routing class changed to FDA.

Trigger rules

Messaging Manager triggers based on the best match against domain name and address prefix.

- **Submit** transactions match on originating domain name and address prefix.
- **Deliver**, **Notify** and **RouteInfo** transactions match on destination domain name and address prefix.

Message Control Plan options

Trigger rules which specify that the message is triggered to ACS, nominate or guide the selection of the message control plan to execute. When the control plan returns signaling to Multigate, it can indicate which transaction processing action to take.

Signal	Description
Release	Perform one of: - Accept (reason code 127) - Reject (reason code 1 to 118) - Discard (reason code 126)
Continue (or no control plan matched)	Progress to outbound routing with parameters unchanged. Will be one of: - Route action for Submit, Deliver or Notify transaction types - Relay action for RouteInfo transaction type
Connect	Progress to outbound routing with modified parameters. Will be one of: - Relay, Route, or Route Unchanged action from the Attempt Delivery Pending node - Route action from the Attempt Delivery Pending with Billing node

Note: Actions can be specified directly without the need to invoke a control plan.

Accept action

The Accept action sends the release cause code 127 to Messaging Manager.

The Accept action does nothing with the message, but tells the caller that it was accepted.

For control plan configuration details see Accept feature node.

Discard action

The Discard action sends the release cause code 126 to Messaging Manager.

The Discard action drops the message without sending any response to the caller.

For control plan configuration details see Discard feature node.

Reject action

The Reject action sends a specified (default configured value, or feature node configured value, see Reject feature node.) Release cause code to Messaging Manager. The Reject action sends an error back to the caller.

If this is a:

- Submit transaction, the subscriber will see a "Message not sent" indication on their handset.
- Deliver, Notify, or RouteInfo transaction, then the caller (an SMSC) will keep the message for a subsequent retry unless a permanent error is signaled.

Route action

For the Route action, various parameters may have been changed by the service logic within the message control plan. By dynamically modifying parameters in the message control, Messaging Manager provides flexible control over transaction processing. The parameters that may be changed and the effects of changing the value are described in this table.

Parameter	Effects of modification
Originating address	Used to mask or alter the identity of the sender.
Originating domain	Used to modify any routing rules that are based on the originating domain name.
Destination address	Used to alter the destination service address.
Destination domain	Used to modify any routing rules that are based on the destination domain name (perform alternate routing)
Routing class	The routing class can be changed under service logic. This is most effective for Submit transactions to attempt as “single shot” by assigning the routing class to “Deliver”, or for performing a First Delivery Attempt by assigning the routing class to FDA.
Message Centre	Used to modify the SMSC name that is used for Submit processing to an SMSC.

Route Unchanged action

The Route Unchanged action passes messages back to the originating network without modification, for delivery to the subscriber by the originating network. The Route Unchanged action applies only to RouteInfo transactions only. It differs from Route actions only in the following ways:

- When analysing the result of a RouteInfo transaction request, the identity of the sender stays the same, it is not altered or masked.
- Mobile Switching Center (MSC) information is not set in the RouteInfo transaction response.

Relay action

The Relay action is the same as for the Route action, with the Originating SCCP address modified so that the response is sent directly to the caller. This action applies to RouteInfo transactions only.

Routing

Introduction

Outbound routing is based on:

- Routing class
- Domain and/address prefix (destination and/or originating depending on routing class)
- (for Submit routing class only) SMSC

In general, outbound routing of messages proceeds according to the assigned routing class for the transaction.

Note: Failure either due to delivery failure or due to no path being specified does not necessarily mean that the message will not be delivered. If a control plan has been triggered, and has an active NoAnswer trigger, then we will return to the control plan and it may determine to re-attempt delivery using an other mechanism, or even to retry using the same mechanism.

Default routing

When Messaging Manager needs to force relay a message, it routes it down the default routing path. For more information, see *Default routing* (on page 23).

Default routing paths are used when Messaging Manager has determined that the message can only be delivered through the same protocol it was received on. For example, if a message utilizes protocol-specific features, Messaging Manager ignores the allocated routing class and default routing is performed. Default routing paths always use the same protocol as the inbound path.

Submit routing

Each routing rule is defined in terms of an originating domain (or address prefix), destination domain (or prefix), and routing class (for example: Submit, Deliver).

Deliver routing

This table describes the criteria Messaging Manager uses to determine the best match for routing which doesn't follow the default routing rules.

Best Match	Routing Class	Originating	Destination
1 (Best)	Deliver	Longest Prefix	Longest Prefix
2	Deliver	Exact Domain	Longest Prefix
3	Deliver	"ANY" Domain	Longest Prefix
4	Deliver	Longest Prefix	Exact Domain
5	Deliver	Longest Prefix	"ANY" Domain
6	Deliver	Exact Domain	Exact Domain
7	Deliver	"ANY" Domain	Exact Domain
8	Deliver	Exact Domain	"ANY" Domain
9 (Worst)	Deliver	"ANY" Domain	"ANY" Domain

Determining the best match submit routing rule

This table shows the criteria Messaging Manager uses to determine the best match for Submit message which don't use the default routing rules.

Best Match	Routing Class	Message Center name	Originating
1 (Best)	Submit	Exact Match	Longest Prefix
2	Submit	Exact Match	Exact Domain
3 (Worst)	Submit	Exact Match	"ANY" Domain

Messaging Manager Screens

Overview

Introduction

This chapter explains how to use the Messaging Manager (MM) screens. The screens are used to maintain the Messaging Manager configuration database.

Because database data related to any screen can be changed at any time, no attempt is made to explain how the various screens and database content work together. For information about how everything works together, see the chapter on *Configuration Scenarios* (on page 169).

In this chapter

This chapter contains the following topics.

Introduction	35
Starting the Messaging Manager Screens	36
Services Menu	38
User Access Control	38

Introduction

Database configuration

Parts of the Messaging Manager configuration are located in a database. The database is maintained through the Messaging Manager screens.

Configuration sequence

While the Messaging Manager screens can generally be used in any sequence, some screens depend on information configured by other screens. Consequently, the following sequence is recommended:

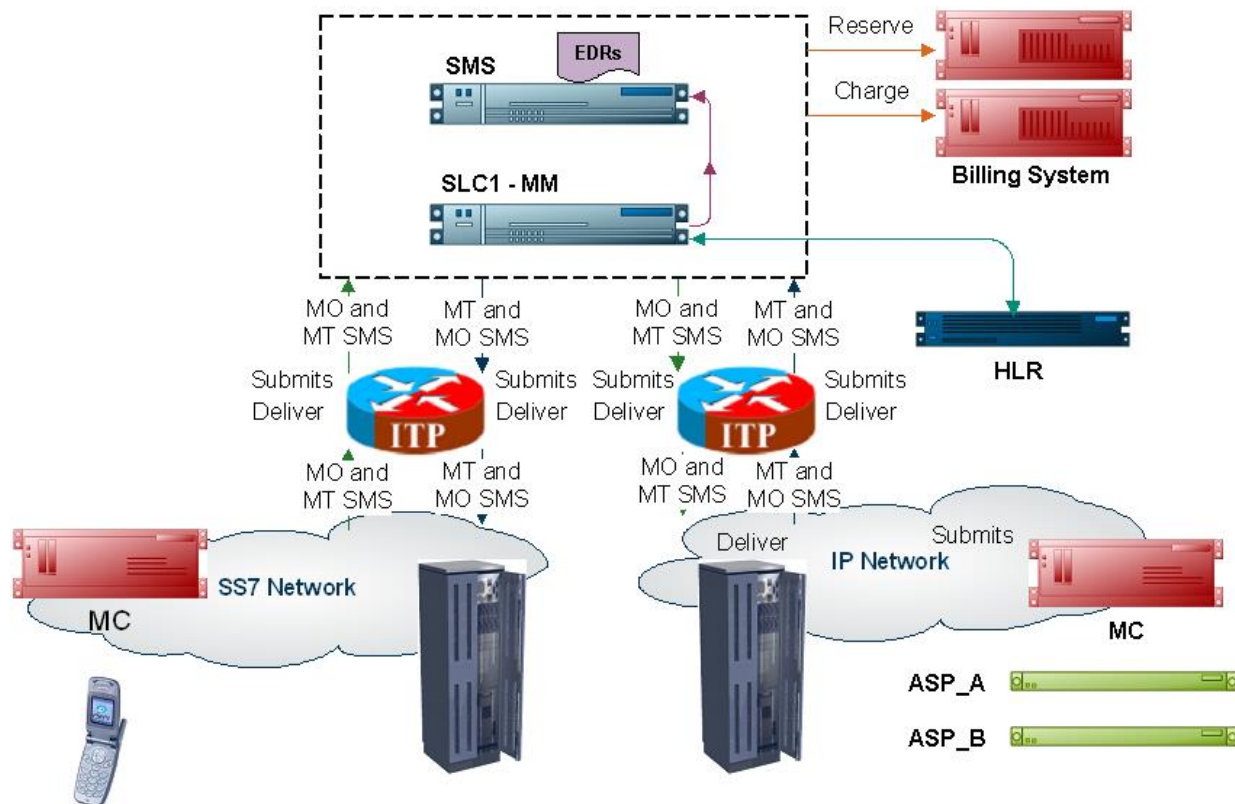
- 1 Add all required adapters.
- 2 Add all required schemes.
- 3 For each scheme, add all required domains
- 4 For each scheme, add all path requirements.
- 5 For each scheme path, add all path connection requirements..
- 6 For each scheme domain, add all address screening rule requirements.
- 7 For each scheme, add all routing requirements.
- 8 For each scheme, add all triggering requirements.
- 9 Add all node requirements.

Note: Originating/ destination address screening rules depend on path prefix, therefore advisable to create paths first, although there is no hard dependency.

The screen detail information below is presented in this sequence.

Example network

For the purposes of this document let us pretend that the network entities that are to be configured to use Messaging Manager are as follows:



These details will be used throughout the document as we work through examples of setting up and configuring Messaging Manager to perform standard services.

Starting the Messaging Manager Screens

Accessing the application

Before you can open any of the Messaging Manager screens, you must log into Service Management System.

For more information about logging into SMS, see *SMS User's Guide*.

SMS Login screen

Here is an example of the SMS Login screen.

Logging into SMS

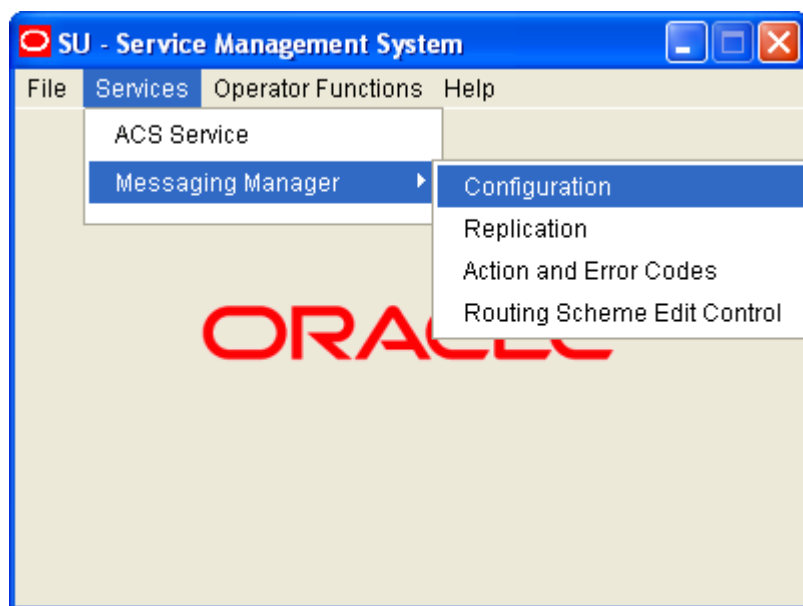
Follow these steps to log into SMS.

Step	Action
1	In the User Name field, type your username.
2	In the Password field, type your password.
	Notes: • Passwords are case sensitive. • You have three attempts to enter a correct username and password before the User ID is locked. If this happens, you must see your System Administrator to re-activate it.
3	Click OK .
	Result: You see the Service Management System main screen.

Services Menu

SMS main screen

Here is an example of the Service Management System main menu showing the Messaging Manager menu options.



Messaging Manager menu options

This table describes the menu options accessible from the Messaging Manager menu option.

Menu	Description
Configuration	Provides access to the creation and maintenance screens for triggering, paths, domains, screening, throttling and routing rule configuration. See <i>Messaging Manager Configuration Screen</i> (on page 41) for details.
Replication	Provides access to the creation and maintenance screens for MM node replication configuration. See <i>Messaging Manager Replication Screen</i> (on page 137) for details.
Action and Error Codes	Provides access to the creation and maintenance screens for MM release cause codes. See <i>Messaging Manager Action and Error Codes</i> (on page 141) for details.
Routing Scheme Controls	Provides access to the enabling screen for MM routing scheme components. See <i>Messaging Manager Routing Scheme Edit Control</i> (on page 165) for details.

User Access Control

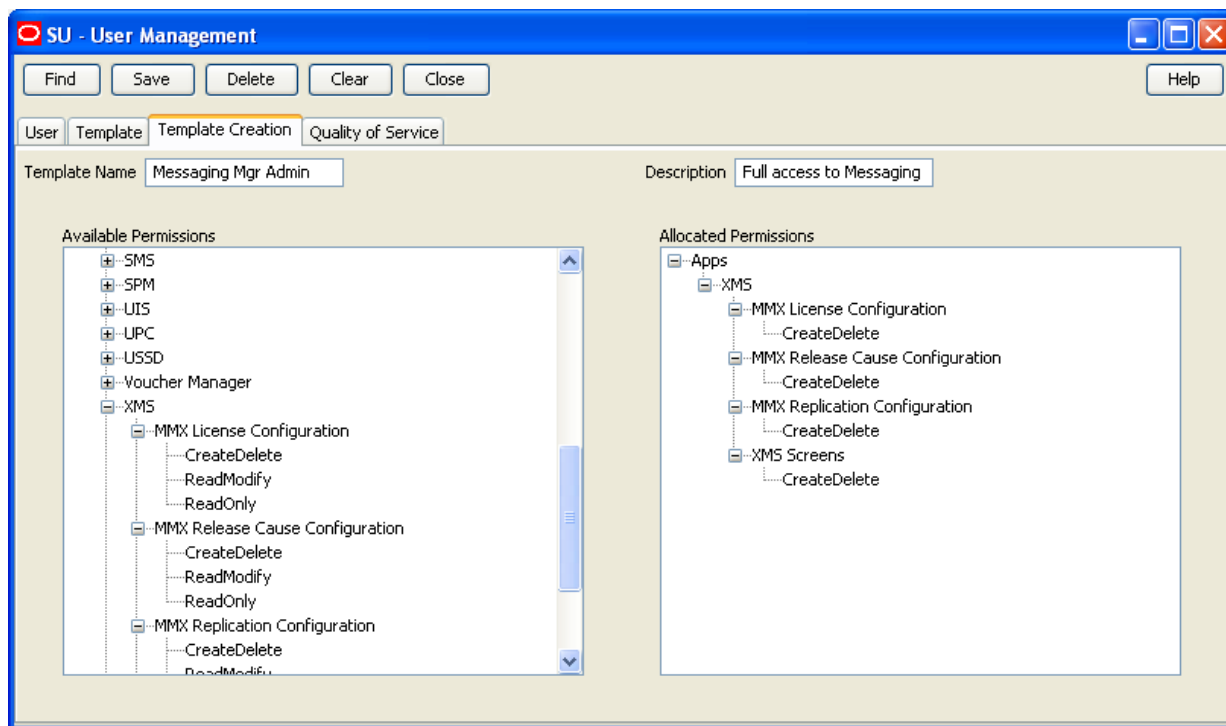
Access templates

To prevent unauthorized access, an additional security template for Messaging Manager replication can be found in the SMS application.

For details on creating user access templates and general access authorization, see *SMS User's Guide* chapter on configuring users.

Messaging Manager User access template

Here is an example showing the Messaging Manager system administrator template for restricting user access to Messaging Manager activities.



Messaging Manager Configuration Screen

Overview

Introduction

This chapter explains the tabs that are available on the Messaging Manager Configuration screen and the configuration that is achieved using these screens.

In this chapter

This chapter contains the following topics.

Messaging Manager Configuration Screen	41
Nodes	43
Schemes.....	48
Networks.....	54
SMSCs	57
ASP Parameters.....	59
ASP Groups.....	64
ASPs.....	67

Messaging Manager Configuration Screen

Introduction

The Messaging Manager Configuration screen enables you to configure resources used by MM. It contains these tabs:

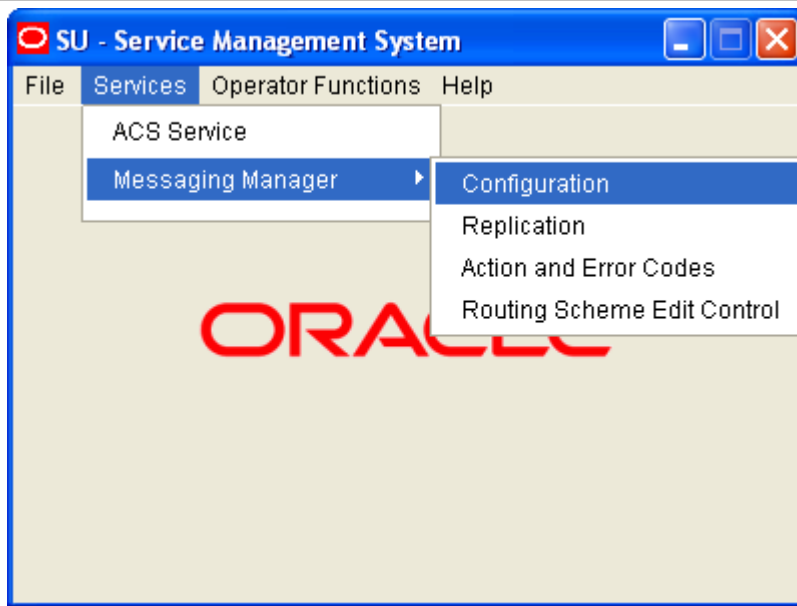
- *Schemes* (on page 48)
- *Nodes* (on page 43)
- *Networks* (on page 54)
- *SMSCs* (on page 57)
- *ASP Parameters* (on page 59)
- *ASP Groups* (on page 64)
- *ASPs* (on page 67)

Accessing the Configuration screen

Follow these steps to open the Configuration screen.

Step	Action
1	Select the Services menu from the SMS main screen.

Step	Action
------	--------



2 Select **Messaging Manager**.

3 Select **Configuration**.

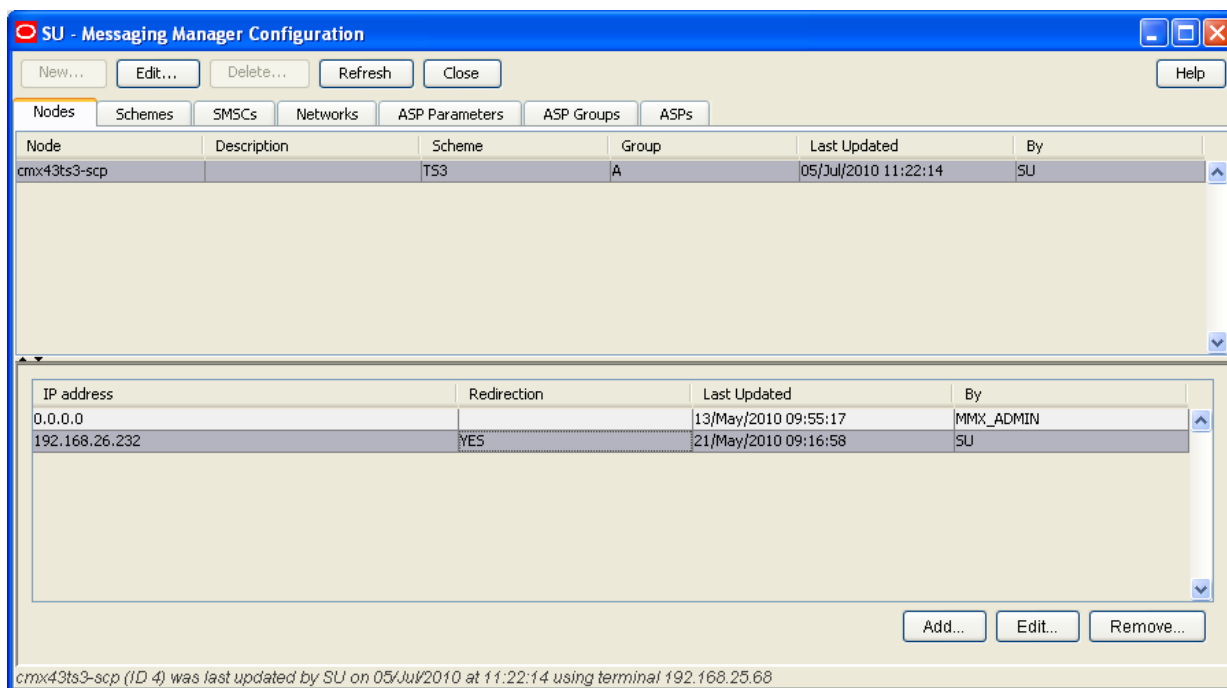
Result: You see the Messaging Manager Configuration screen.

For more information about:

- The screen's content and how to enter configuration information, see the other topics in this chapter.
- How all the information works together to create the Messaging Manager configuration, see *Configuration Scenarios* (on page 169).
- Logging into the Service Management System screen, see *SMS User's Guide*.

Messaging Manager Configuration screen

Here is an example Messaging Manager Configuration screen.



Naming conventions

As part of the configuration process, names for items such as paths and connections are required.

To make maintaining a large number of configuration items easier, a naming convention should be used, such as basing path names on the destination.

Example: For incoming MAP protocol based messages, paths are automatically generated using path names similar to:

- MAP_MC_Adapter_Name
- MAP_SME_Adapter_Name

Nodes

Introduction

The **Nodes** tab allows you to add and change the values for the nodes. The nodes for Messaging Manager to load are established at installation time, and can be the SLC name (default) or any other name entered at that time. The node definition is created with default values that may then be changed through the node configuration screens.

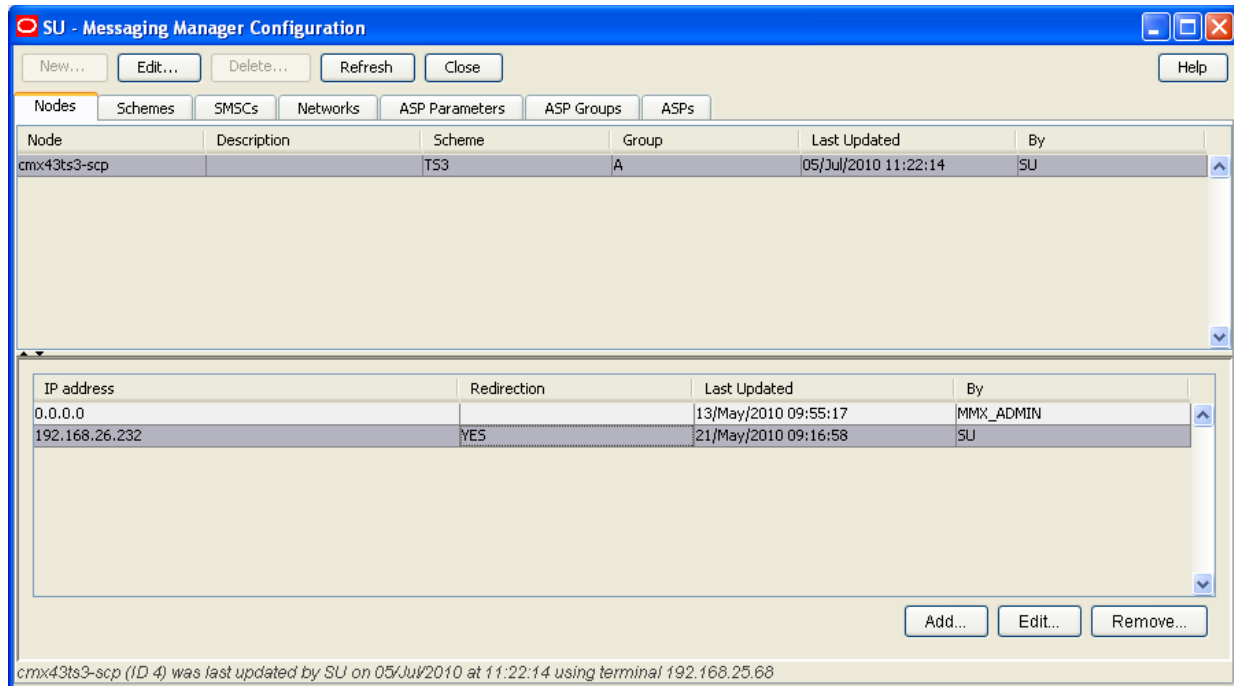
To concatenate user messages, MM needs to be able to process all network packets that are part of a user message on a single MM node. This node is selected based on the B-party address, which will be the same for all message segments.

This is achieved by using a directory function that can map each destination number to a particular processing node.

This makes it necessary for all the MM nodes to be aware of each other and be able to pass a message on to any other node. This is done with a minimum amount of configuration required by the user by putting node data into the existing replicated node table as part of the install of each SLC instance.

Nodes tab

Here is an example of the **Nodes** tab.



Nodes fields

This table describes the function of each field.

Field	Description
Name	A unique identifier of the MM instance. Set during the SLC node installation.
Redirection Port	The listening port on the node being configured. Other nodes will connect to it using this as the destination port. Note: Default value requested by the install process. The IP address used by the MM instance for communicating with other MM instances. Note: Default value requested by the install process.
Concat Group	Defines a set of processing nodes that work together to join concatenated messages. This node does not redirect concatenated messages to other SLCs if the group is NULL. Note: Default value is NULL.
Routing Scheme	The scheme name to associate with this node. This can be any of the configured Scheme names. See <i>Schemes</i> (on page 48). Note: Default value is (Unspecified).
Interface	Interface record used by this node.

Field	Description
	These values are configured in the scheme which is assigned in the Routing Scheme field.
IP Address	IP address of network adapter used for the interface in the corresponding Interface column. Note: This field can be changed by clicking in the cell.
Description	An optional description of the node.

IP address fields

This table describes the function of each field.

Field	Description
IP Address	IP addresses which either are or are not available to be assigned to an interface in this node.
Used for redirection	Whether or not this IP address can be used for redirection. Only one of a node's IP addresses can be used for redirection.

Adding IP addresses

Follow these steps to add a new IP address.

Step	Action
------	--------

1 In the **Nodes** tab, select the node to add an IP address to.

2 Click **Add...**.

Result: The Add IP Address to 'node' screen appears.

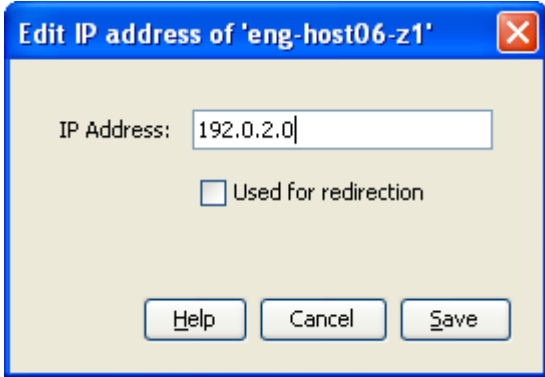
3 Enter data in the fields to configure this record.

For more information about the fields on this screen, see *IP address fields* (on page 45).

4 Click **Save**.

Editing IP addresses

Follow these steps to edit the details of ip address records.

Step	Action
1	On the Nodes tab, select the node which is associated with the IP address to edit. Result: The IP addresses available to the selected node will appear in the bottom panel.
2	Select the IP address record to change and, and click Edit... Result: The Edit IP Address from 'node' screen appears.
	
3	Edit the fields with the changes to make. For more information about the fields on this screen, <i>IP address fields</i> (on page 45).
4	Click Save .

Removing IP addresses

Follow these steps to remove an IP address record from a node.

Step	Action
1	On the Nodes tab, select the node to remove an IP address record from. Result: The IP addresses available to the selected node will appear in the bottom panel.
2	Select the IP address record to remove, and click Remove... Result: The Remove IP address 'ip' prompt appears.
3	Click Remove . Result: The IP address is removed from the database.

Adding nodes

Nodes cannot be added using the configuration screens.

Nodes can only be added at installation time for the SLC being installed, using the host name as the node name. See *Installation Guide*.

Editing nodes

Follow these steps to edit an existing node record.

Step	Action
1	From the table on the Nodes tab, select the node to edit.
2	Click Edit or double-click the record. Result: The Edit Node 'Node_Name' screen appears.

Step

Action

Edit Node 'eng-host06-z1'

Name: eng-host06-z1

Redirection Port: 7377

Concat Group: Dawn

Routing Scheme: DocTest

Interface	IP Address
NIC_A	192.0.2.0
NIC_B	(Unassigned)
	192.0.2.0
	192.168.14.156

Description: Created from Python

Help Cancel Save

3 Edit the fields with the changes to make.

For more information about the fields on this screen, see *Nodes fields* (on page 44).

Notes:

- The **Routing Scheme** list box lists all the schemes which can be assigned to this node.
- The node name cannot be changed once it is installed. The only way to change is to remove the SLC concerned and then re-install using the desired node name.
- You can change the values of the IP Address column by clicking in the cell to change.

4 Click **Save** to save the updated Node record in the configuration database.

Deleting nodes

Nodes cannot be deleted using the configuration screens.

Nodes can only be deleted by the removal of a SLC.

Schemes

Introduction

The **Schemes** tab allows you to manage all the routing definitions for the Messaging Manager configuration.

From this tab you can add or edit schemes, specifying the name and description. You can also edit the scheme configuration by opening the Schemes screen. This is documented in the chapter - *Messaging Manager Schemes* (on page 75).

Note: Schemes are assigned to nodes in the node configuration on the **Nodes** tab.

A scheme is a set of rules for how to treat and route messages.

These rules define, for multiple protocols, what:

- Paths to use
- Connections to use
- Billing domain to use
- Filtering to use
- Actions to take

Note: Only one scheme may be used by each instance of Messaging Manager. However, where several instances of MM are running, each may use a different scheme.

Configuration options

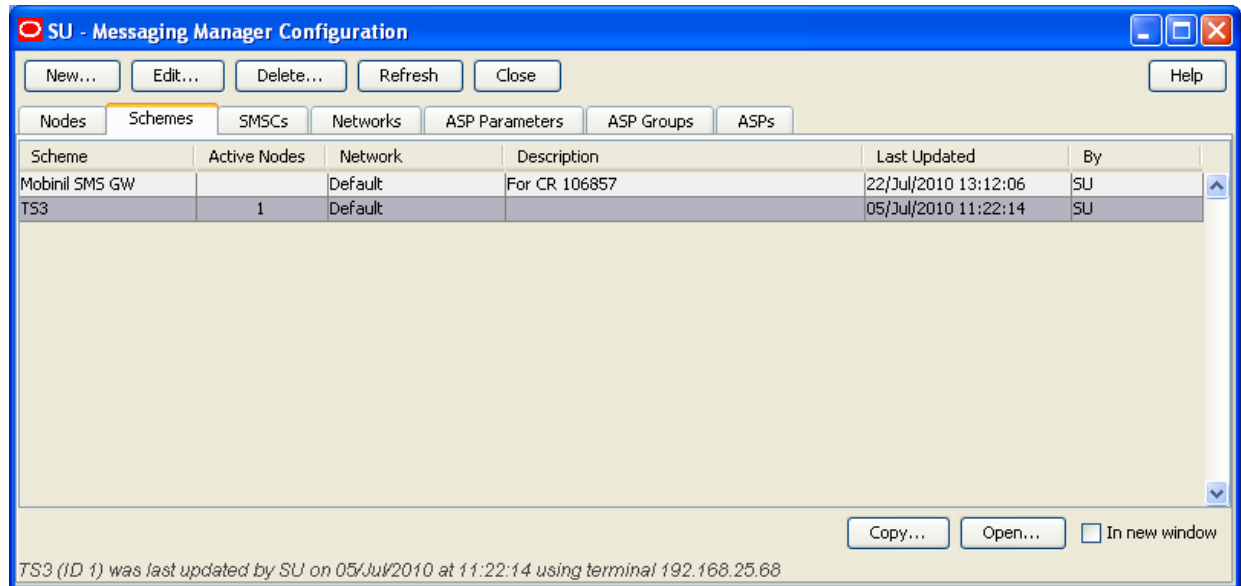
This table shows the functions to be configured for a scheme.

Function	Description	More information
Adapters	Configure protocol adapters.	<i>Adapters</i> (on page 77)
Interfaces	Configure network interfaces.	<i>Interfaces</i> (on page 80)
Paths	Configure the paths associated with adapters.	<i>Paths</i> (on page 82)
Connections	Configure connections used by paths.	<i>Path Connections</i> (on page 88)
Screening rules	Configuring screening and anti-spam rules.	<i>Screening</i> (on page 100)
Addressing rules	Configure address categorization rules.	<i>Addressing</i> (see "Address Domains" on page 29, on page 117)
Throttling rules	Configure throttling rules.	<i>Throttling</i> (on page 122)
Triggering rules	Configure triggering rules.	<i>Triggering</i> (on page 125, on page 31)
Routing rules	Configure outbound routing rules.	<i>Routing</i> (on page 131)

For more information about how these functions are configured together in a scheme (including the order in which rules are applied), see *MM User's Guide, Message Routing and Processing* topic.

Schemes tab

Here is an example of the **Schemes** tab.



Schemes columns

This table describes the content of each column.

Column	Description
Scheme	Name of the routing scheme.
Active Nodes	Number of nodes using this routing scheme.
Network	The network which this scheme will use unless overridden by other configuration. This column is populated by the Default Network field.
Description	Meaningful description of this routing scheme.
Last Updated	Date and time when this routing scheme was last updated.
By	User ID of last update for this routing scheme.

Schemes buttons

This table describes the function of buttons specific to the **Schemes** tab.

Note: Some buttons are only available for some routing schemes.

Button	Description
	Copies the currently selected scheme and all associated data to a new scheme. See <i>Copying schemes</i> (on page 50).
	Displays the selected scheme details for editing. See <i>Opening schemes</i> (on page 49).

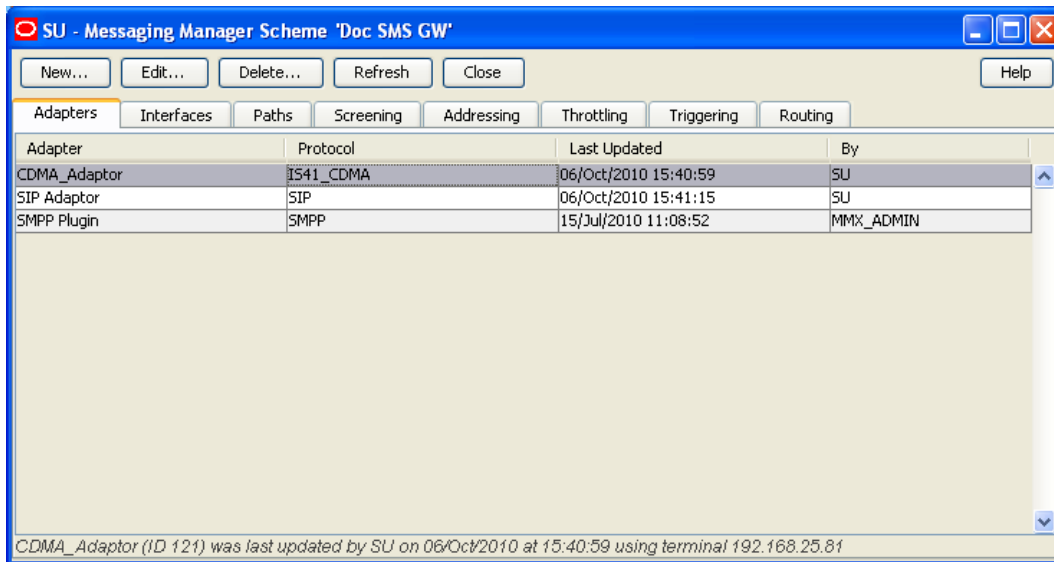
Opening schemes

To view and manage a scheme configuration, it must be opened.

Follow these steps to open a scheme:

Step	Action
1	In the table on the Schemes tab, select the record to open.
2	If one or more schemes are already open, perform one of the following actions: • Select the In New Window check box to open the selected scheme in a new window • Deselect the In New Window check box to open the selected scheme in one of the current scheme windows.
3	Perform one of the following actions: • Double-click the record in the table • Click Edit

Result: The Messaging Manager Scheme '*scheme_name*' screen appears.



For details on using this screen, see *Messaging Manager Schemes* (on page 75).

Copying schemes

A new scheme can be added from scratch or based on an existing scheme.

Follow these steps to create a new scheme from an existing scheme.

Note: All nodes, adapters and scheme details are copied from the existing scheme and attached to the new scheme.

Step	Action
1	In the table on the Schemes tab, select the record to copy.
2	Click Copy .
	Result: The Copy Scheme ' <i>Scheme_Name</i> ' screen appears.

Step	Action
------	--------

3 In the **Save As** field, enter the name of the new scheme.

4 In the **Description** field, enter a description of the new scheme.

Result: The Save button becomes available.

5 Click one of:

- **Save** to save the new scheme record in the configuration database
- **Cancel** to close the panel without copying the scheme

Note: Copying a scheme will copy all the existing configuration elements of the original scheme to the new scheme.

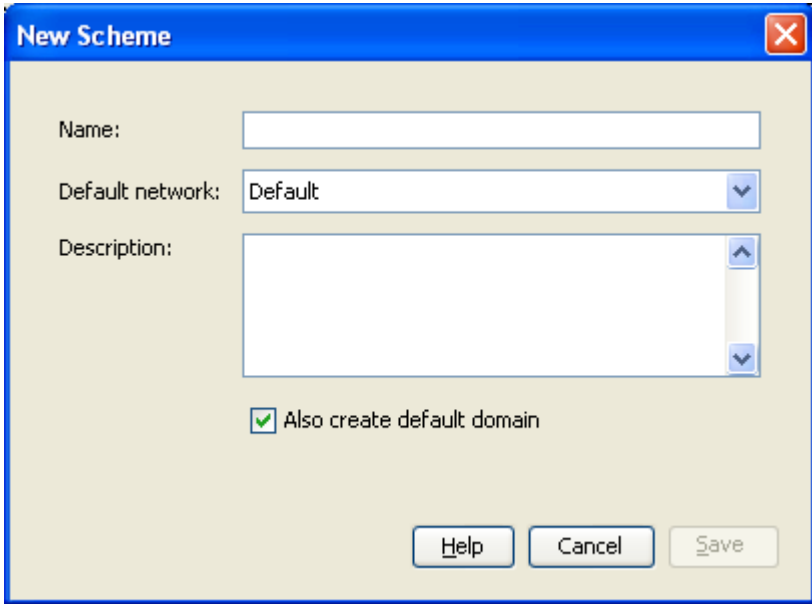
Scheme fields

This table describes the function of each field on the New Scheme and Edit Scheme screen.

Field	Description
Name	The scheme name. Note: This field cannot be changed after it is first saved.
Default Network	The network to use unless overridden by other configuration. The values configured in this field are displayed in the network column.
Description	Free text description for this scheme.
Also create default domain	A check box on the new scheme. Select to auto generate a default domain.

Adding schemes

Follow these steps to add a new scheme to the configuration database.

Step	Action
1	From the Schemes tab screen, click New... Result: The New Scheme screen opens. 
2	In the Name field, enter the name of the new scheme.
3	In the Description field, enter a description of the new scheme.
4	If you wish this scheme to: - Also create a default domain, leave the Also create default domain check box selected. This will create domain named 'Default'. - Otherwise deselect the Also create default domain check box. Result: The Save button becomes available.
5	Click Save to save the new scheme record in the configuration database.

Note: When a scheme is created, a set of default paths will be created that cannot be changed by the user. These paths are created as follows:

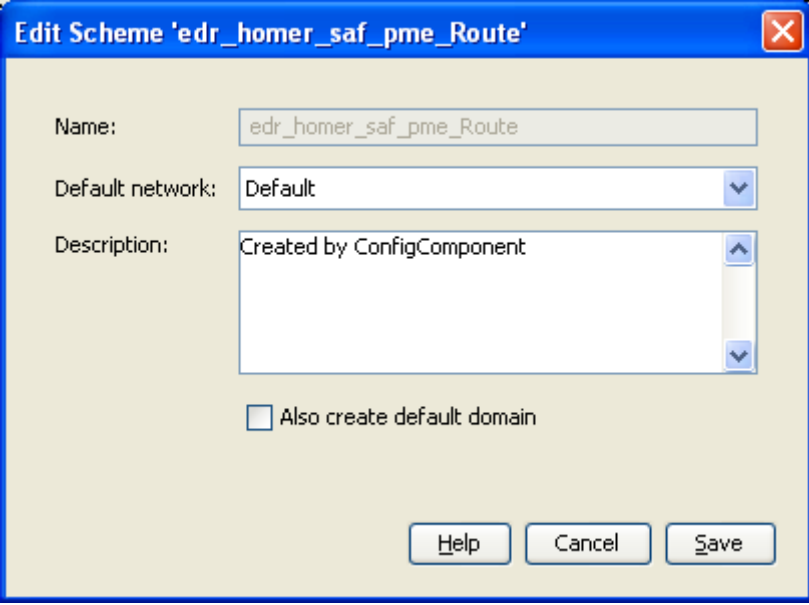
- For each MAP adapter record these predefined paths will be created:
 - MAP_SME_Adapter_Name
 - MAP_MC_Adapter_Name
- For each IS41_CDMA adapter record these predefined paths will be created:
 - IS41_CDMA_SME_Adapter_Name
 - IS41_CDMA_MC_Adapter_Name
- For each IS41_TDMA adapter record this predefined path will be created:
 - IS41_TDMA_SME_Adapter_Name
- For each Internal adapter record this predefined path will be created:
 - INTERNAL_SME_Adapter_Name

Editing schemes

Follow these steps to edit an existing scheme record.

Step	Action
1	In the table on the Schemes tab, select the scheme to edit.
2	Click Edit or double-click the record.

Result: The Edit Scheme '*Scheme_Name*' screen opens.



The screenshot shows a dialog box titled "Edit Scheme 'edr_homer_saf_pme_Route'". It contains the following fields and controls:

- Name:** A text box containing "edr_homer_saf_pme_Route".
- Default network:** A dropdown menu showing "Default".
- Description:** A text area containing "Created by ConfigComponent".
- Also create default domain:** An unchecked checkbox.
- Buttons:** "Help", "Cancel", and "Save" at the bottom right.

- | | |
|---|--|
| 3 | Configure this record by entering data in the fields on this screen.
For more information about the fields on this screen, see <i>Scheme fields</i> (on page 51). |
| 4 | Click Save to save the updated scheme record in the configuration database. |

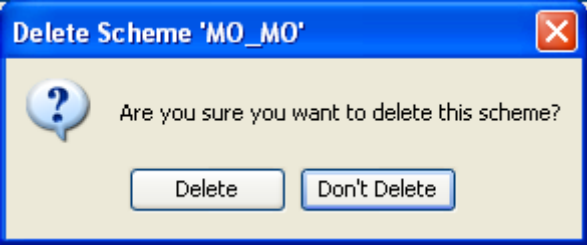
Deleting schemes

Follow these steps to delete an existing Scheme record.

Step	Action
1	In the table on the Schemes tab, select the record to delete.
2	Click Delete .

Result: One of the following dialogs appears:

- The Delete Scheme '*Scheme_Name*' confirmation prompt appears:

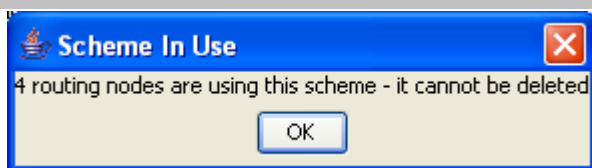


The screenshot shows a confirmation dialog box titled "Delete Scheme 'MO_MO'". It contains the following elements:

- A question mark icon in a speech bubble.
- The text: "Are you sure you want to delete this scheme?"
- Two buttons: "Delete" and "Don't Delete".

- The Scheme In Use prompt appears.

Step	Action
------	--------



- 3 If the scheme can be deleted, click one of the following:
- **Delete** to delete the record from the configuration database
 - **Don't Delete** to cancel the delete.

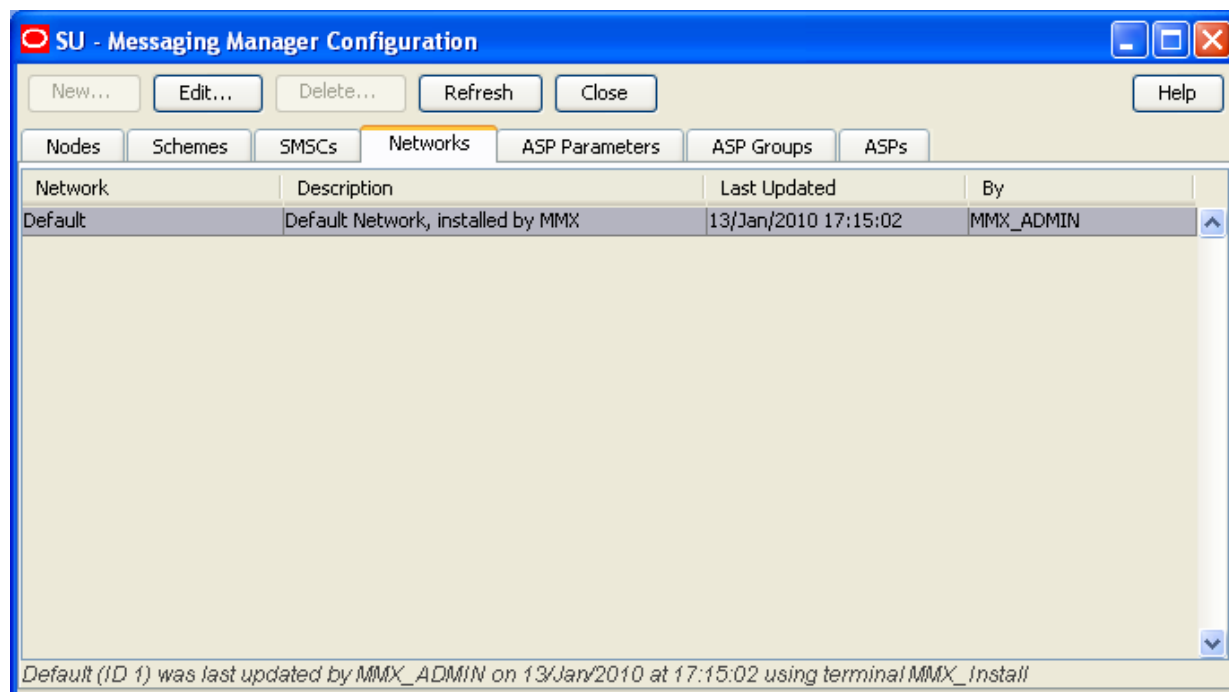
Networks

Introduction

The **Networks** tab allows you to define the global (outside routing schemes) parameters to achieve the desired flexibility of the foreign subscriber gateway.

Networks tab

Here is an example of the **Networks** tab.



Networks columns

This table describes the content of each column.

Column	Description
Network	Name of the network.
Description	Meaningful description of this network.
Last Updated	Date and time when this network was last updated.

Column	Description
By	User ID of last update for this network.

Networks fields

This table describes the function of each field.

Field	Description
IMSI Masking	- Selected - Specifies that MM will replace real MSIDs (IMSI or MINs) with internally generated temporary MSIDs. - Deselected - Default - temporary MSIDs not used, unless Accept trigger rules for a RouteInfo action are encountered.
IMSI MCC	Country code to use when building temporary IMSIs.
IMSI MNC	Network code to use when building temporary IMSIs.
MSIN prefix	Fixed initial digits of the MSIN part of the IMSI when building temporary IMSIs.
MSIN length	<= 15 Number of digits to use for the remaining part of the MSIN when building temporary IMSIs.
MIN prefix	Up to 10 fixed initial digits to use when building a temporary MIN.

Editing networks

Follow these steps to edit an existing network.

Step	Action
1	From the table on the Networks tab, select the network to edit.
2	Perform one of the following actions: - Double-click the record in the table - Click Edit Result: The Edit Network ' <i>Network_Name</i> ' screen appears.

Step	Action
------	--------

Edit Network 'Default'

Name:

IMSI MCC: IMSI MNC:

☒ IMSI masking

MSIN prefix: MSIN length:

MIN prefix:

Description:

- 3 To generate temporary MSIDs (for IMSIs or MINs), select the **IMSI masking** check box.

Note: Leaving the IMSI masking check box deselected makes all but the **Description** field unused for all except RouteInfo actions.

Masking takes place regardless, using the values from this configuration screen when Accept trigger rules for a RouteInfo action are encountered.
- 4 When generating temporary MSIDs for IMSIs, enter the country code to use in the **IMSI MCC** field.
- 5 When generating temporary MSIDs for IMSIs, enter the network code to use in the **IMSI MNC** field.
- 6 When generating temporary MSIDs for IMSIs, enter the fixed initial digits part of the MSIN in the **MSIN prefix** field.
- 7 When generating temporary MSIDs for IMSIs, enter the number of remaining digits to use (up to 15) for the MSIN in the **MSIN length** field.
- 8 When generating temporary MSIDs for MINs, enter the fixed initial digits to use (up to 10) in the **MIN prefix** field.

Note: A MIN is exactly 10 digits in length, hence the number of digits to use for the remaining part of a temporary MIN is determined by the length of the MIN prefix.
- 9 Enter the network description in the **Description** field.
- 10 Click **Save** to save the updated network record in the configuration database.

SMSCs

Introduction

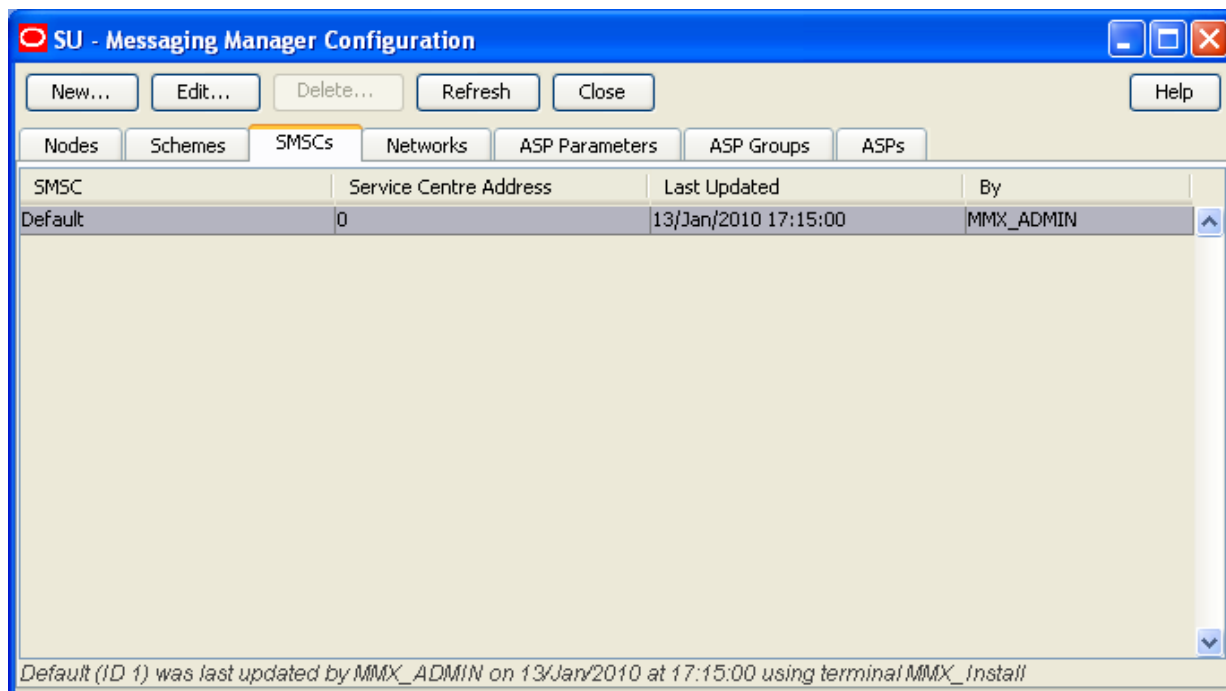
The **SMSCs** tab allows you to map a message center to a Service Center Address (SCA). If required, the SCA may be entered as a Global Title.

You can associate a SMSC with a path if it is used to receive messages from ASPs or handsets, but not if it is used to receive messages from a SMSC.

An SMSC can be associated with a path, meaning that a message received on that path will also be associated with that SMSC. Also, the SMSC assigned to a message plays a part in routing of the message if the message is a 'Submit' type message.

SMSCs tab

Here is an example of the **SMSCs** tab.



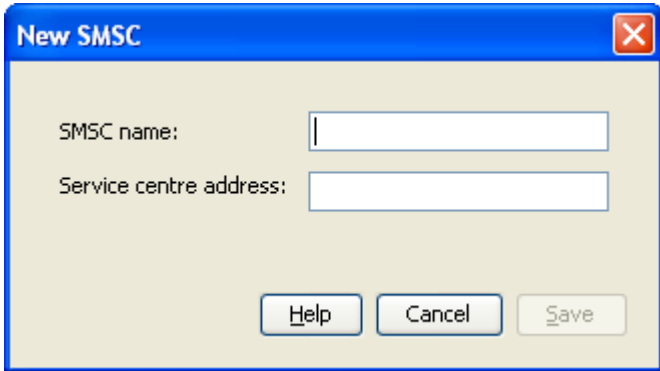
SMSCs fields

This table describes the function of each field.

Field	Description
SMSC name	The name of the SMSC. This field is required.
Service Centre Address	The Service Center Address for the SMSC. This field is required.

Adding SMSCs

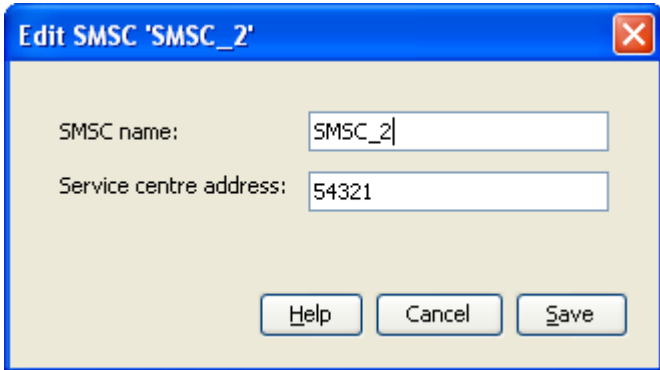
Follow these steps to add an SMSC to the database.

Step	Action
1	From the SMSCs tab screen, click New . Result: The New SMSC screen appears.
	
2	In the SMSC name field, enter name of the new SMSC. For more information about the fields on this screen, see <i>SMSCs fields</i> (on page 57). Result: The Save button becomes available.
3	In the Service centre address field, enter the service center address for the SMSC.
4	Click Save to save the new SMSC in the configuration database.

Note: When MM is installed, a default SMSC is created. The initial SCA value of this default SMSC is set to 0. This should be change to a valid value when the initial configuration of MM is done.

Editing SMSCs

Follow these steps to edit an existing SMSC.

Step	Action
1	From the table on the SMSCs tab, select the record you want to edit.
2	Perform one of the following actions: • Double-click the record • Click Edit Result: The Edit SMSC screen appears.
	
3	You can change the Service centre address for the SMSC, as required.

Step	Action
4	Click Save .

Deleting SMSCs

Follow these steps to delete an existing SMSC record.

Step	Action
1	From the table on the SMSCs tab, select the record to delete. Note: You cannot delete the default SMSC.
2	Click Delete . Result: The Delete SMSC confirmation prompt opens.
3	To delete the SMSC record from the configuration database, click Delete .

ASP Parameters

Introduction

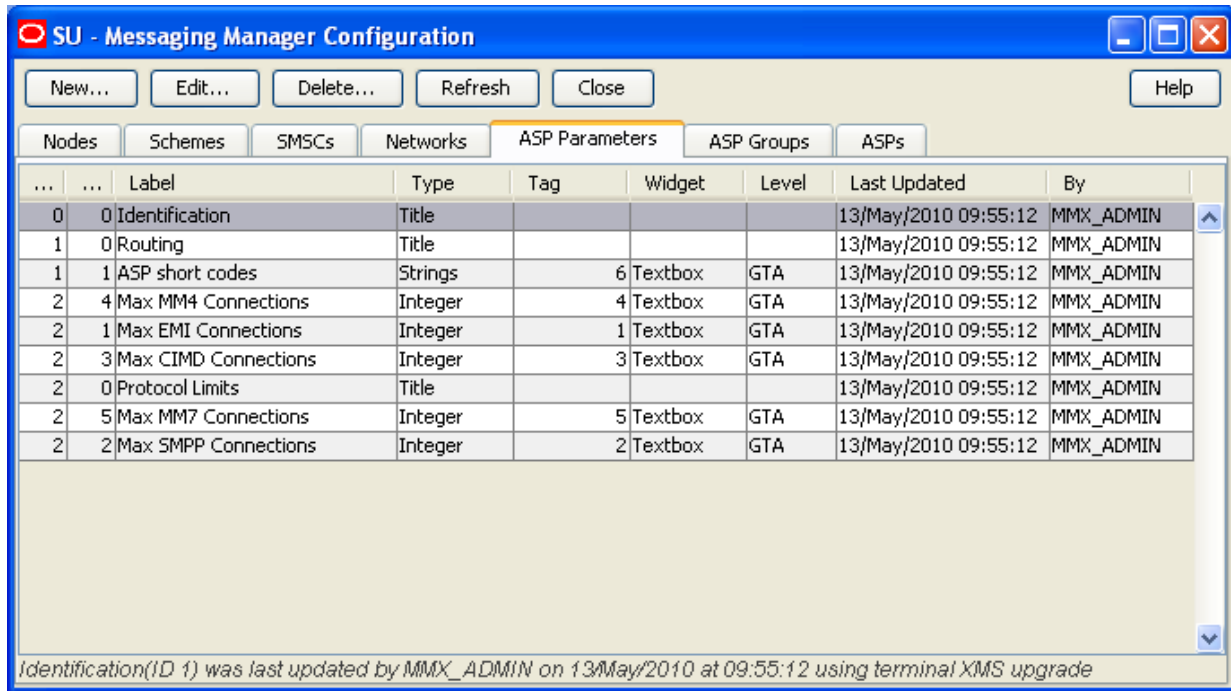
The **ASP Parameters** tab allows you to configure the elements which appear on the ASP screen, which is used by ACS customers to manage their ASP account.

The GUI will refer to the list of constants from this group whenever it needs to present the configurable ASP group, template or account parameters (that is, in the New or Edit dialog box for each type of object).

For more information about ASP accounts and groups, see *ASP Groups and Parameters* (on page 26).

ASP Parameters tab

Here is an example of the **ASP Parameters** tab.



ASP parameters fields

This table describes the function of each field.

Field	Description
Dialog label	Label as presented in the Create and the Edit ASP accounts screens. Required.
Parameter type	Data type (integer, boolean or string) to be used when storing values for this parameter in the ACS Customer profile block. Title defines a page title of the configuration wizard. This enables you to group related parameters. Required.
Page number	The panel on the Create and the Edit ASP account screen that this parameter will appear on. Required.
GUI widget	Presentation widget to use on the Create and the Edit ASP account screens for this ASP parameter. Required (unless Parameter type is set to title).
Row on page	Where on the Create and the Edit ASP account screen this parameter should appear. (The page is set by the Page number field).
Profile tag	The profile field to store the value of this ASP parameter to, if the value is set at the ASP account level (the value is not stored in the profile if it is set by a default, or is a null value). This drop down list is populated by the profile fields associated with the ACS Customer profile block on the ACS Configuration screen. For more information about profiles, see <i>ACS User's Guide</i> .

Field	Description
Special meaning	Whether this ASP parameter is part of a specific set of ASP parameters which have a specific purpose in MM. ASP short code The ASP parameter will store ASP short codes which can be used in IP connections for this ASP account. Short codes are entered as a space or newline separated list. Max <i>protocol</i> connections This ASP parameter will store the maximum number of connections of this protocol allowed for an ASP. Optional.
Maximum length	Max number of characters allowed for the value of this ASP parameter. For both integer and string this will constrain the length of the associated text box (if any). Note: Only applies to parameters where Parameter type is set to integer or string.
Default value	Value the ASP parameter will default to. Optional. Note: A default value may be also set at the ASP Group level.
Editable level	These check boxes define which levels the widget can be edited at: • ASP group • ASP template • ASP account For more information about how these levels work to set defaults, see <i>ASP groups and parameter defaults</i> (on page 27).
A value is mandatory	If this checkbox is ticked, the ASP account will not be saved unless this ASP parameter has one of: • Been given a specific value • Set to the ASP Group default (if one is available)
Allowable values	The values that this ASP parameter can have. Can be expressed as a range, or a list. A variable can be defined with a single allowable value. If this field is empty, then all values for the given data type will be allowed. For strings, you can specify a regex value to be used for validation.

Note: To create a list with a restricted set of options, you must:

- make the widget type = list, and
- code the allowable values as a comma separated list in Allowable values (for example, a list with names would be entered as: 1:One, 2:Two, 3:Three, 4:Four)

Title

Titles are used to provide the labels for the ASP configuration screens (Create and Edit ASP Groups, Create and Edit ASP Template and Create and Edit ASP Accounts).

Notes:

- Only one title can be defined for each page.
- The title will be displayed at the top of the page only, regardless of any value in the Row field.

Adding ASP parameters

Follow these steps to add a new ASP parameter to the configuration database.

Step	Action
1	From the ASP Parameters tab, click New... Result: The New ASP Parameter screen opens. This screen enables you to create new ASP parameters which will then be available for use in the ASP account screens.

- Enter data in the fields to configure this record.

Note: If you do not set a value for maximum length, it will default to 0. This will mean this ASP parameter cannot have a value entered for it in the Create and the Edit ASP account screens.

For more information about:

 - The fields in this screen, see *ASP parameters fields* (on page 60)
 - ASP accounts, see *ASP Groups and Parameters* (on page 26)
- Click **Save** to save the new ASP parameter in the configuration database.

Editing ASP parameters

Follow these steps to edit an existing ASP parameter.

Step	Action
1	In the table on the ASP Parameters tab, select the parameter to edit.
2	Click Edit... Result: The Edit ASP Parameters '<i>asp_Parameter_Name</i>' screen opens.

Step	Action
	This screen enables you to edit existing ASP parameters used in the ASP account screens. For more information about ASP accounts, see <i>ASP Groups and Parameters</i> (on page 26).

The screenshot shows a dialog box titled "Edit ASP Parameter 'MAX SMPP Connections'". It contains the following fields and controls:

- Dialog label:** Text box containing "MAX SMPP Connections".
- Page number:** Text box containing "2".
- Row on page:** Text box containing "5".
- Special meaning:** Dropdown menu showing "Max SMPP Connections".
- Maximum length:** Text box containing "0".
- Editable levels:** Three checked checkboxes: "Group", "Template", and "Account".
- Allowable values:** An empty text area.
- Parameter type:** Dropdown menu showing "Integers".
- GUI widget:** Dropdown menu showing "List".
- Profile tag:** Dropdown menu showing "Divert Address Busy (17)".
- Default value:** An empty text box.
- A value is mandatory:** An unchecked checkbox.

At the bottom right, there are three buttons: "Help", "Cancel", and "Save".

- 3 Edit the fields with the changes to make.

Note: If you do not set a value for maximum length, it will default to 0. This will mean this ASP parameter cannot have a value entered for it in the Create and the Edit ASP account screens.

For more information about the fields in this screen, see *ASP parameters fields* (on page 60).

- 4 Click **Save** to save the updated scheme record in the configuration database.

Deleting ASP Parameters

Follow these steps to delete an existing ASP parameter record.

Warning: If you delete an ASP parameter, it will delete all the values for that parameter in all the ASP accounts and ASP groups.

Step	Action
1	In the table on the ASP Parameters tab, select the record to delete.
2	Click Delete.... Result: The Delete ASP Parameter confirmation prompt appears. This prompt enables you to delete an existing ASP parameter. For more information about ASP parameters, see <i>ASP Groups and Parameters</i> (on page 26).
3	Click one of: • Delete to delete the ASP Parameter from the configuration database

Step	Action
	• Don't Delete to cancel the delete

ASP Groups

Introduction

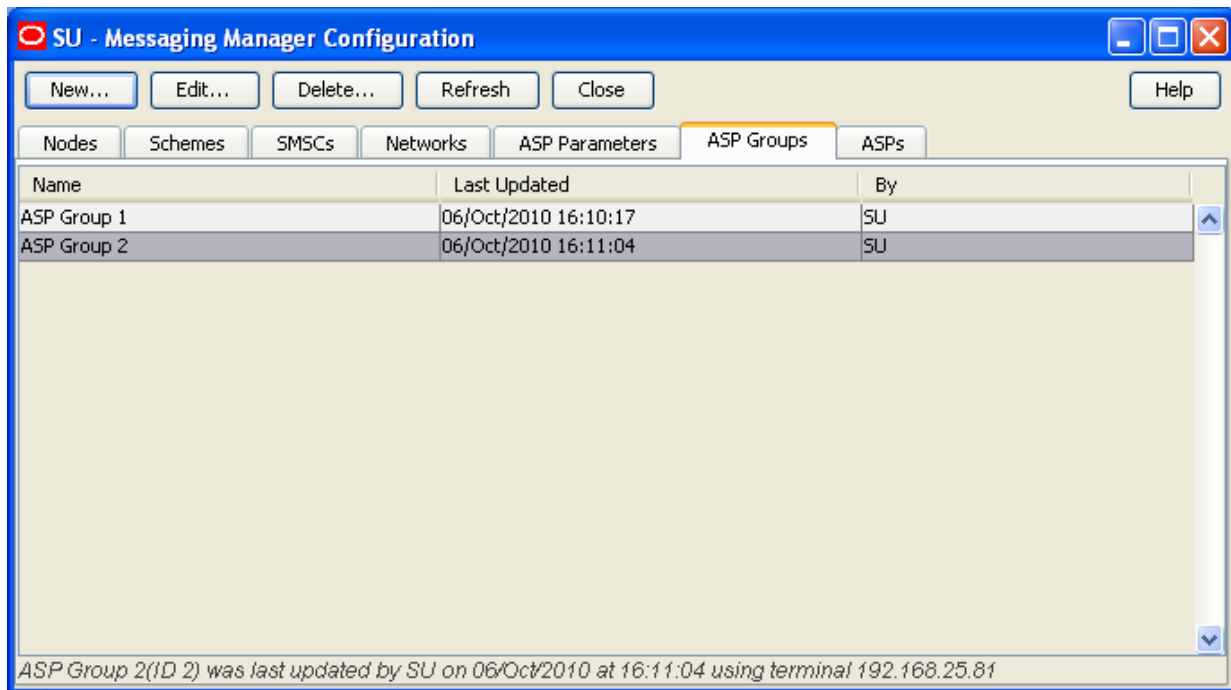
The **ASP Groups** tab allows you to define groups of ASP accounts.

ASP Groups should be configured before ASPs are configured.

For more information about ASP accounts and groups, see *ASP Groups and Parameters* (on page 26).

ASP Groups tab

Here is an example of the **ASP Groups** tab.



ASP groups fields

This table describes the function of each field.

Field	Description
Name	Customer allocated name for customer group.
Other fields	The other fields in this screen are configured in the ASP Parameters tab. The panels in this screen are configured by the Title objects in the ASP Parameters tab. For more information about configuring the fields which appear on this screen, see <i>ASP Parameters</i> (on page 59).

Adding ASP groups

Follow these steps to add a new ASP group.

Step	Action
1	From the ASP Groups tab, click New... Result: The New ASP Group screen opens. This screen enables you to add new ASP groups. For more information about address rules, see <i>ASP Groups and Parameters</i> (on page 26).

- 2 Enter data in the fields to configure this record.

Notes:

- The values in this screen will set the defaults for the ASP accounts which use this ASP group. Where no default should be set in the ASP accounts, do not enter a value here.
- To save an ASP group, you must have a value in the Name field.
- Other than the **Name** field, all the fields in this screen are configured on the ASP Parameters screen. For more information about these fields, refer to your administrator.

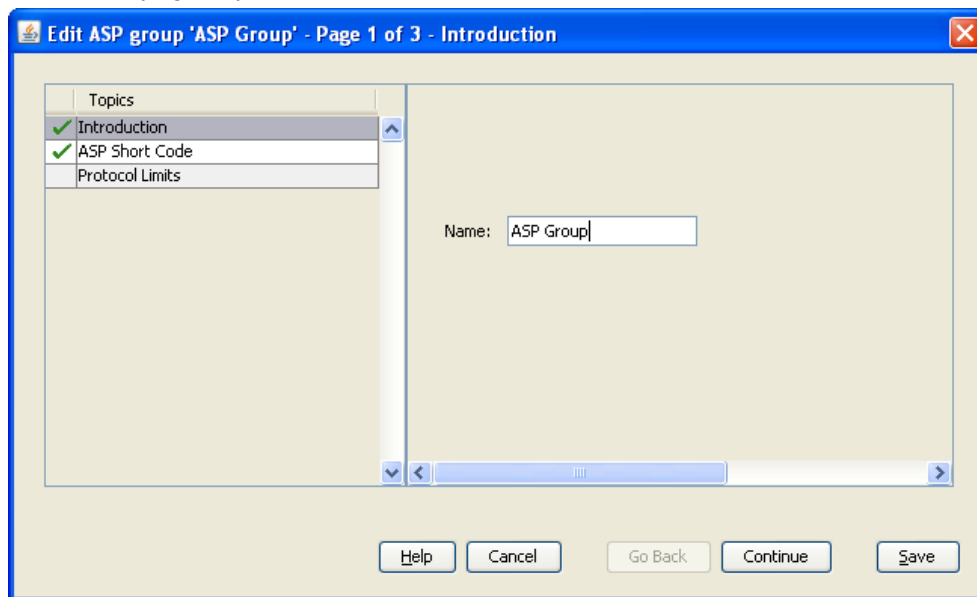
- 3 Click **Save** to save the new ASP group in the configuration database.

Editing ASP groups

Follow these steps to edit an existing ASP group.

Step	Action
1	In the table on the ASP Groups tab, select the group to edit.

Step	Action
2	Click Edit... Result: The Edit ASP Groups 'asp_Parameter_Name' screen opens. This screen enables you to edit existing ASP groups. For more information about ASP groups, see <i>ASP Groups and Parameters</i> (on page 26).



- 3 Edit the fields with the changes to make.

Notes:

- Other than the **Name** field, all the fields in this screen are configured on the ASP Parameters screen. For more information about these fields, refer to your administrator.
- The values in this screen will set the defaults for the ASP accounts which use this ASP group. Where no default should be set in the ASP accounts, do not enter a value here.

- 4 Click **Save** to save the updated Scheme record in the configuration database.

Deleting ASP groups

Follow these steps to delete an existing ASP group record.

Warning: Do not delete an ASP group which is being used by one or more ASP accounts. You will not be able to edit those ASP accounts after the ASP Group has been deleted.

Step	Action
1	In the table on the ASP Groups tab, select the group to delete.
2	Click Delete.... Result: The Delete ASP Group confirmation prompt appears. This prompt enables you to delete an existing ASP group. For more information about ASP groups, see <i>ASP Groups and Parameters</i> (on page 26).
3	Click Delete to delete the ASP group from the configuration database.

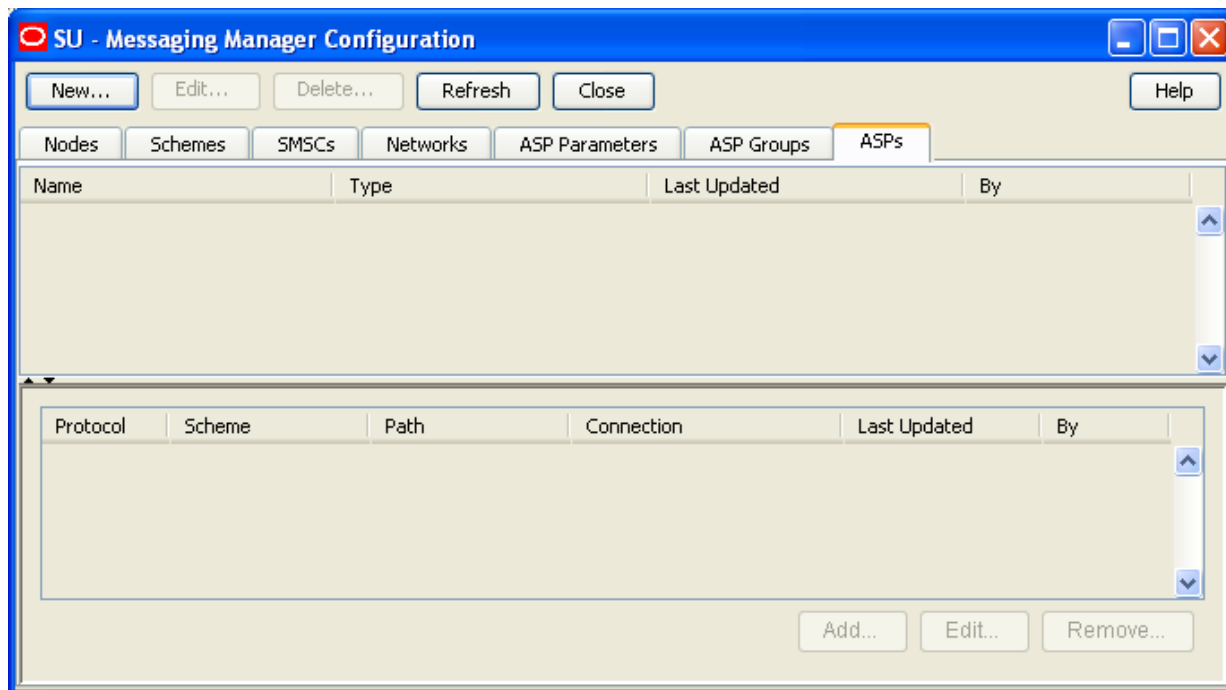
ASPs

Introduction

The **ASPs** tab allows you to define ASP accounts and provides a convenient way to rapidly allocate ASP paths and connections.

ASPs tab

Here is an example of the **ASPs** tab.



ASPs fields

This table describes the function of each field.

Field	Description
Name	The unique name of this ASP account or template.
Type	Defines whether this record is an ASP template or an ASP account.
Based on template	The template to base this ASP account on. Notes: - This field is only available on the New ASP screen. Once an ASP account or template has been created its association with the template is lost. - You can link the ASP account to a group other than the group specified in the template selected in this field.
Allocate to ASP group	The ASP group this ASP account belongs to. This field is populated by the records on the <i>ASP Groups</i> (on page 64) tab. This field is required.

Note: This screen will have other configuration on later panels. This configuration is defined in the *ASP Parameters* (on page 59) tab. The specific configuration which appears here will be the configuration which is defined for the ASP group specified in the **Allocate to ASP group** field.

Adding ASP accounts or templates

Follow these steps to add a new ASP account or ASP account template.

Step	Action
1	From the ASP tab screen, click New... Result: The New ASP screen opens. This screen enables you to add new ASP accounts and account templates. For more information about ASPs, see <i>ASP Groups and Parameters</i> (on page 26).

- 2 Enter data in the fields to configure this record.

Notes:

- ASP account templates provide a set of configuration which can be used to pre-populate configuration in a new ASP account. Once the ASP account is saved, its relationship with the template is lost.
- Other than the Name, Type, Based on template and Allocate to ASP group fields, all the fields in this screen are configured on the ASP Parameters tab.
- Defaults are configured on the ASP Parameters tab, and on the **ASP Groups** tab, in the ASP Group selected in the Allocate to ASP group drop down list. For more information about these fields, refer to your Administrator.
- If a field cannot have data entered in it (even when the default check box is deselected), it may have a maximum field length of 0. Check the ASP Parameters record for this field (for more information about setting the Maximum field length, see *ASP parameters fields* (on page 60)).

- 3 Click **Save** to save the new ASP account or template.

Editing ASP accounts and templates

Follow these steps to edit an existing ASP account or ASP account template.

Step	Action
1	In the table on the ASPs tab, select the record to edit.
2	Click Edit... .
Results:	
- If the record was an ASP account, the Edit ASP account '<i>asp_Account_Name</i>' screen opens. - If the record was an ASP template, the Edit ASP template '<i>asp_Template_Name</i>' screen opens.	

The screenshot shows a window titled "Edit ASP Template 'Alternate Connection Maxes' - Page 1 of 3 - Introduction". On the left, a "Topics" list contains "Introduction" (checked), "ASP Short Code" (checked), and "Protocol Limits". The main area displays the following fields:

- Name:** Alternate Connection Maxes
- Type:** Radio buttons for "Account" and "Template" (selected).
- Allocate to ASP group:** A dropdown menu showing "ASP Group1".

At the bottom, there are five buttons: "Help", "Cancel", "Go Back", "Continue", and "Save".

These screens enable you to edit existing ASP accounts and ASP account templates. For more information about ASP accounts and templates, see *ASP Groups and Parameters* (on page 26).

Step	Action

- 3 Edit the fields with the changes to make.

Notes:

- Editing ASP account templates will not affect the ASP accounts which were based on that template.
- Other than the Name and Allocate to ASP group fields, all the fields in this screen are configured on the **ASP Parameters** tab.
- Defaults are configured on the **ASP Parameters** tab, and on the ASP Groups tab, in the ASP Group selected in the Allocate to ASP group drop down list.
- For more information about these fields, refer to your Administrator.
- If a field cannot have data entered in it (even when the default check box is deselected), it may have a maximum field length of 0. Check the ASP Parameters record for this field (for more information about setting the Maximum field length, see *ASP parameters fields* (on page 60)).

- 4 Click **Save** to save the updated ASP account or template in the configuration database.

Deleting ASP accounts and templates

Follow these steps to delete an existing ASP account or ASP account template.

Note: Deleting ASP account templates will not affect the ASP accounts which were based on that template.

Step	Action
1	In the table on the ASPs tab, select the record to delete.
2	Click Delete....
	Result: The Delete ASP confirmation prompt appears.

Step	Action
	This prompt enables you to delete an existing ASP account or ASP account template. For more information about ASP groups, see <i>ASP Groups and Parameters</i> (on page 26).
3	Click Delete to delete the ASP account or template from the configuration database.

IP connections

The bottom panel on the **ASPs** tab contains a list of IP connections currently associated with the ASP account selected in the top panel. It contains all paths and connections owned by the adapter instances in all routing schemes that have been associated with that ASP account.

Note: This panel is only displayed when an ASP Account is selected in the top panel.

IP connection fields - ASPs tab

This table describes the function of each field.

Field	Description
Protocol	Protocol this IP connection will use. Desired protocol (restricted to this ASP's supported protocols).
Routing scheme	The routing scheme this IP connection will be part of. Note: This field is populated by the <i>Schemes</i> (on page 48) tab, with schemes which can support the protocol selected in the protocol field.
Adapter	The adapter this IP connection should use. Note: This field is populated by the <i>Adapters</i> (on page 77) option in the Schemes detail.
Make new adapter (named)	Create a new adapter with the name entered in this field. Optional. This adapter will be added to the scheme specified in the Routing scheme field.
Path	Paths in the selected scheme supporting that protocol and already associated with the ASP. Alternatively a text box can be completed, to name the new path that should be created to hold the new connection. In this case the validation, and the database updates, are performed in a single unit of work so the dialog will either display an error message objecting to the path or connection fields, or it will create the path and connection together in one transaction. • Login username • Login password • Routing interface to select for local listen • Routing interface to select for local source • Failover check box
Make new path (named)	Create a new path with the name entered in this field. Optional. This path will be added to the scheme specified in the Routing scheme field.
ASP short code	ASP short code for the service which will use this connection. Optional.
Failover check box	If another connection in the path disconnects, then MM will attempt to open paths with this check box selected. Can be toggled on the tab for immediate database update.
Enabled check box	Enable and disable connections as can be done in the Connections list inside a routing scheme.

Field	Description
	Can be toggled on the tab for immediate database update.

Adding IP connections in ASPs

Follow these steps to add a new IP connection to the ASP account selected in the top panel.

Step	Action
1	From the ASPs tab, click Add... Result: The New connection for ASP Account screen opens.

This screen enables you to create and edit connections belonging to an ASP without leaving the **ASPs** tab. For more information about connections, see *Paths and Connections* (on page 17).

- 2 Enter data in the fields to configure this record.
This screen creates a connection in the selected routing scheme, and will create a new path if necessary. The fields in this screen generally must be completed in a top-down order.
For specific information about the details required for this protocol, see *Path Connections* (on page 88).

- 3 Click **Save**.
Result: The details are saved, and the New '*protocol*' connection screen opens.
For more information about filling out this screen, see *Path Connections* (on page 88).

Editing IP connections in ASPs

Follow these steps to edit an existing IP connection from the **ASPs** tab.

Step	Action
1	In the table on the ASPs tab, select the record to edit.

Step	Action
2	Click Edit... The Edit <i>protocol</i> Connection '<i>Connection_Name</i>' dialog for the selected IP connection opens. The edit connection dialog includes all the connection configuration fields relevant to the type of protocol. These fields are not visible when you open the New IP Connection for ASP dialog. Note: You can also edit connections from the Paths tab by selecting and opening the associated scheme on the Schemes tab.
3	Update the fields as required. See: • <i>IP Connections</i> (on page 89) for more information about configuring IP connections and for information about the connection fields for the different connection protocols • <i>Paths and Connections</i> (on page 17) for general information about paths and connections
4	Click Save to save the updated IP connection in the configuration database.

Example Edit SMPP Connection dialog

Here is an example edit connection dialog for the SMPP protocol. In this example, the name of the connection is XMSP12.

The screenshot shows the 'Edit SMPP Connection' dialog box for a connection named 'XMSP12'. The dialog is organized into several sections:

- General Fields:**
 - Name:** XMSP12
 - Weighting:** 10
 - Enabled:** ☒ **Preopen:** ☐ **RX:** ☒ **TX:** ☒ **Shadowed:** ☐
- Local/Remote Configuration:**
 - Local username:** m2
 - Local password:**
 - Remote username:** r2
 - Remote password:**
 - Connections allowed:** 1
- IP Address / Host Name and Port:**
 - Local listen:** (dropdown menu)
 - Local source:** (dropdown menu)
 - Remote listen:** cwm.me.uk
 - Remote source:** (text field)
 - Port:** 4321 (for both local and remote)
- SMPP Options:**
 - SMPP version:** 3.4 (dropdown menu)
 - Max. concurrent transactions:** 1024
 - Outgoing timeout:** 10
 - Idle timeout:** 0
 - Heartbeat interval:** 0
 - System ID:** eSG MMX
 - System type:** MMX
 - Augment IDs:** ☐
 - eSG Extensions:** ☐
- Buttons:** Help, Cancel, Save

Deleting IP connection in ASPs

Follow these steps to delete an existing IP connection from an ASP account.

Step	Action
1	In the table on the ASPs tab, select the record to delete.
2	Click Delete.... Result: The Delete IP connection confirmation prompt appears. This prompt enables you to delete an IP connection associated with the ASP selected in the top panel. For more information about connections, see <i>Paths and Connections</i> (on page 17). Note: This prompt is the same as the delete connection screens which are accessible from the Paths & Connections option in the Schemes tab.
3	Click Delete to delete the IP connection from the configuration database.

Messaging Manager Schemes

Overview

Introduction

This chapter explains the functionality of the Oracle Communications Convergent Charging Controller Messaging Manager Schemes screen. The Schemes screen is accessed through the Messaging Manager Configuration screen and is the main screen for configuring the paths, addressing, screening, triggering, routing and throttling of Messaging Manager schemes.

In this chapter

This chapter contains the following topics.

Messaging Manager Scheme Screen	75
Adapters	77
Interfaces	80
Paths	82
Path Connections	88
IP Connections	89
SS7 Connections.....	98
Screening	100
Global Title Screening Rules.....	107
SCA Consistency Rules	109
Screening Rules	111
RLV Prefix Rules	114
Addressing.....	117
Throttling.....	122
Triggering	125
Routing	131

Messaging Manager Scheme Screen

Accessing the Messaging Manager Scheme screen

You access the Messaging ManagerScheme screen through the **Schemes** tab of the Messaging Manager Configuration screen. For details, see *Opening schemes* (on page 49).

Scheme tabs

The Scheme screen allows you to configure the details of a scheme.

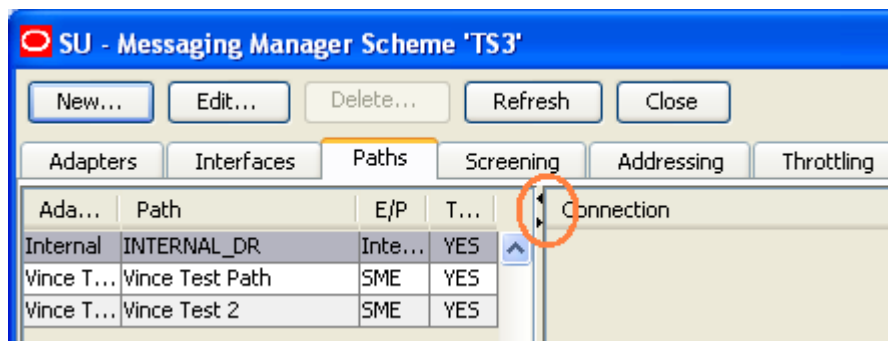
This table describes the tabs on the screen.

Tab	Description	See
Adapters	Defines the adapters which route traffic to and from the scheme.	<i>Adapters</i> (on page 77)

Tab	Description	See
Interfaces	Defines the interfaces which are available to the scheme.	<i>Interfaces</i> (on page 80)
Paths	Defines the paths available to the scheme.	<i>Paths</i> (on page 82)
Screening	Defines the anti-spam rules for the scheme.	<i>Screening</i> (on page 100)
Addressing	Defines the addressing rules for the scheme.	<i>Addressing</i> (see "Address Domains" on page 29, on page 117)
Throttling	Reports summary of all the domain throttling values.	<i>Throttling</i> (on page 122)
Triggering	Defines the triggering rules for the scheme.	<i>Triggering</i> (on page 125)
Routing	Defines the routing rules for the scheme.	<i>Routing</i> (on page 131)

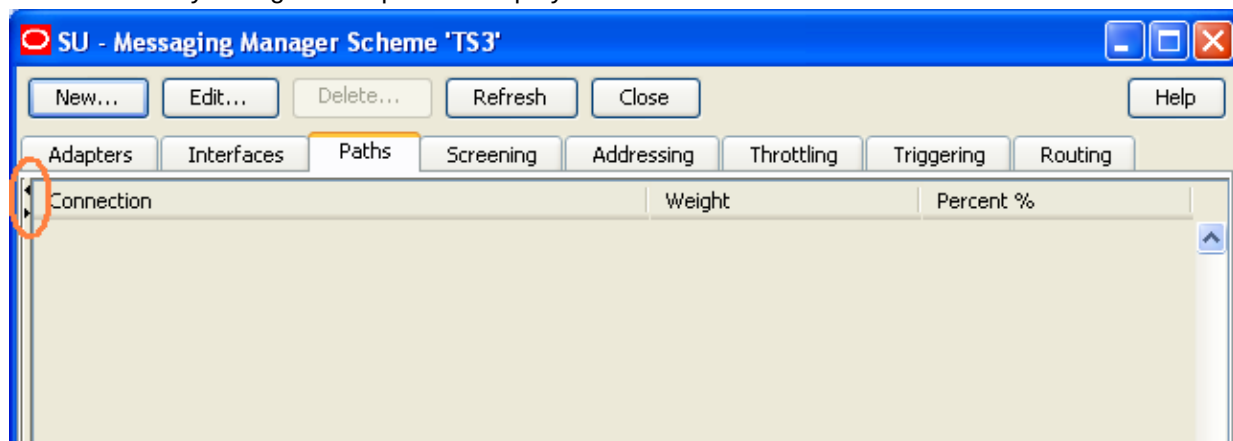
Adjusting panel displays

On the **Screening** and **Paths** tabs you can expand or collapse the panels on the screen using the arrows on the horizontal/ vertical bar between the panels.

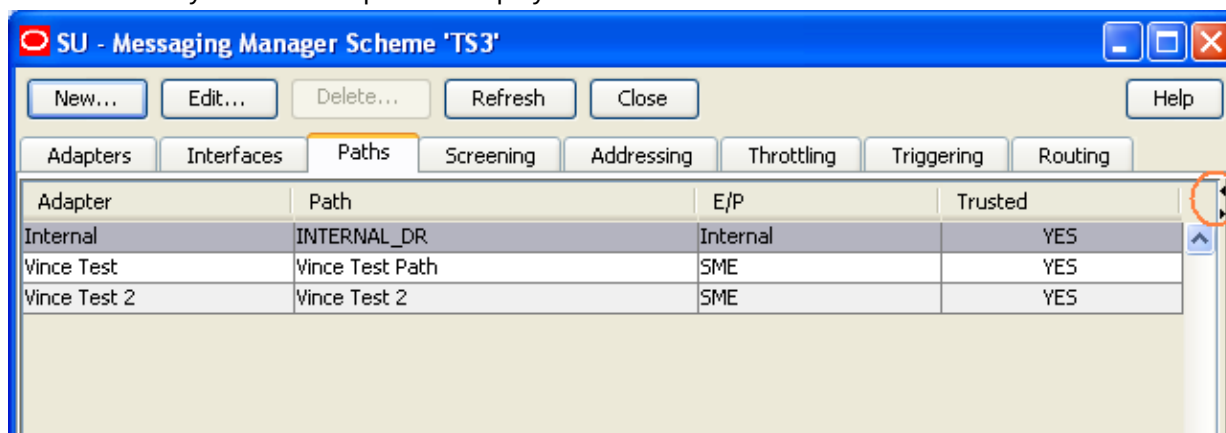


The following describes how to adjust the display:

- **To Display only the right hand panel:**
Click the arrow which points left.
Result: Only the right hand panel is displayed.



- To Display both panels when only the right hand panel is displayed
Click the arrow which points right.
 - To Display only the left hand panel
Click the arrow which points right.
- Result:** Only the left hand panel is displayed.



- To Display both panels when only the right hand panel is displayed
Click the arrow which points left.

Adapters

Introduction

The **Adapters** tab enables you to add, change and delete adapter records. Adapters are used by Messaging Manager to communicate to the network using different protocols.

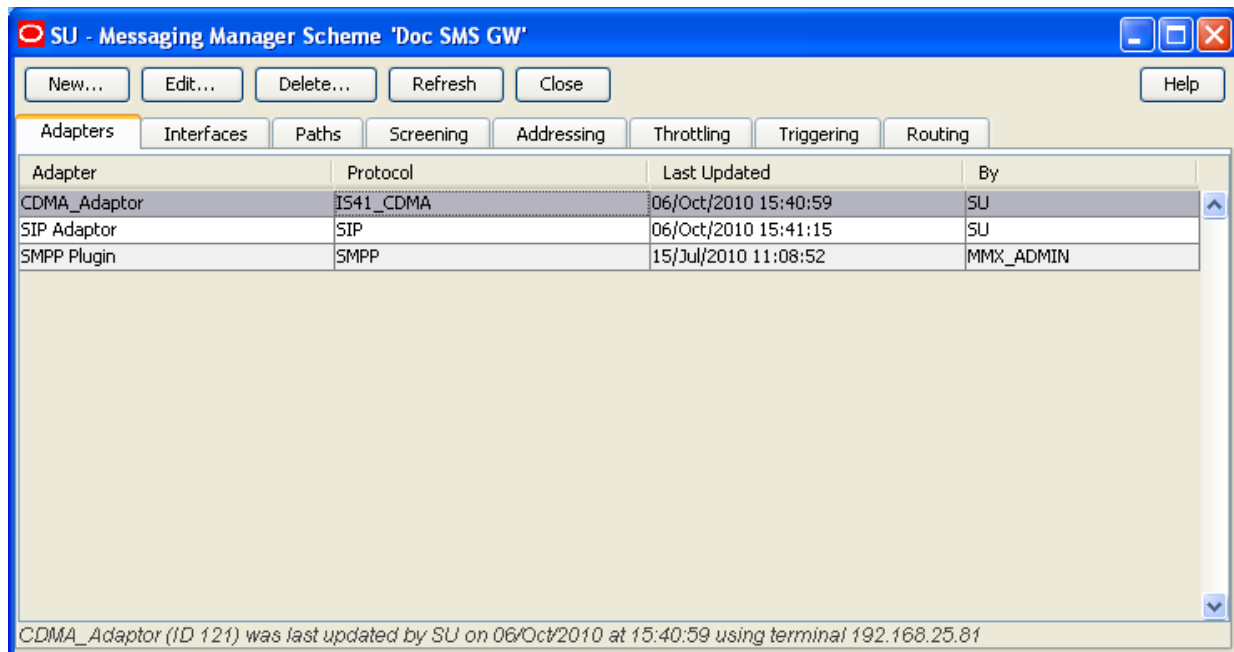
Entries in the **eserv.config** file identify which adapters will be loaded by Messaging Manager at startup. The link between **eserv.config** and the adapter configuration values is made on this tab.

It is important to note that there may be many adapters configured in the system that use the same protocol, but each adapter may only use a single protocol.

Note: Messaging Manager provides a special adapter, which has a protocol of INTERNAL, for communications between the Send Short Message feature node and Messaging Manager. This is the only function of the INTERNAL adapter.

Adapters tab

Here is an example of the **Adapters** tab.



Adapters fields

This table describes the function of each field.

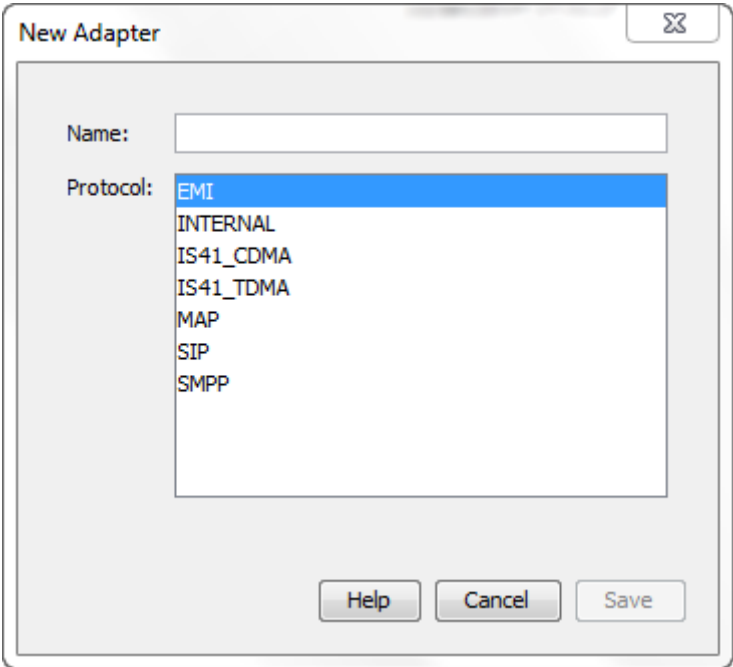
Field	Description
Adapter	The name of the adapter. The name must exactly match the adapter name specified in the <code>adapterName</code> parameter in the eserv.config configuration file. Note: The SLEE will fail to successfully start, or restart, if the adapters you configure in the Messaging Manager UI do not have a corresponding adapter section defined in the eserv.config file. For more information about configuring adapters in eserv.config, see <i>Messaging Manager Technical Guide</i>.
Protocol	List of available protocols that an adapter can use.

Adding adapters

Follow these steps to add a new adapter to the configuration database.

Step	Action
1	From the Adapters tab, click New. The New Adapter dialog displays.

Step	Action
------	--------

A dialog box titled "New Adapter" with a close button in the top right corner. It contains a "Name:" label followed by a text input field. Below that is a "Protocol:" label followed by a list box. The list box contains the following items: EMI (highlighted), INTERNAL, IS41_CDMA, IS41_TDMA, MAP, SIP, and SMPP. At the bottom of the dialog are three buttons: "Help", "Cancel", and "Save".

- 2 Enter the name of this adapter in the **Name** field. The name must exactly match the adapter name specified in the `adapterName` parameter in the `eserv.config` configuration file.
For more information, see *Adapters fields* (on page 78).
- 3 Select the protocol that this adapter will use from the **Protocol** list.
- 4 Click **Save** to save the new adapter record in the configuration database. The name of the new adapter displays in the **Adapter** field on the **Adapter** tab.

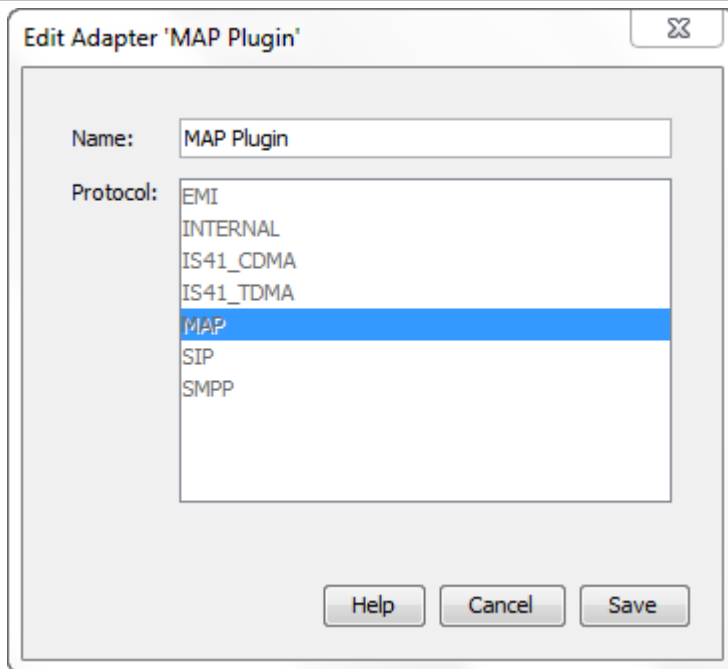
Editing adapters

Follow these steps to edit an existing Adapter record; for example, to update the adapter name to match what is in the `eserv.config` file.

Step	Action
------	--------

- 1 From the table on the **Adapters** tab, select the record to edit. Click **Edit** or double-click the record.
The Edit Adapter '*Adapter_Name*' dialog displays.

Step	Action
------	--------



- 2 Update the name of the adapter in the **Name** field to match the `adapterName` parameter in the `eserv.config` configuration file .
For more information about the fields on this screen, see *Adapters fields* (on page 78).
- 3 Click **Save**.

Deleting adapters

Follow these steps to delete an existing adapter record.

Step	Action
------	--------

- 1 From the **Adapters** tab, click **Delete**.
The Delete Adapter *adapter_name* dialog displays.
- 2 Click **Delete** to delete the record from the configuration database.

Interfaces

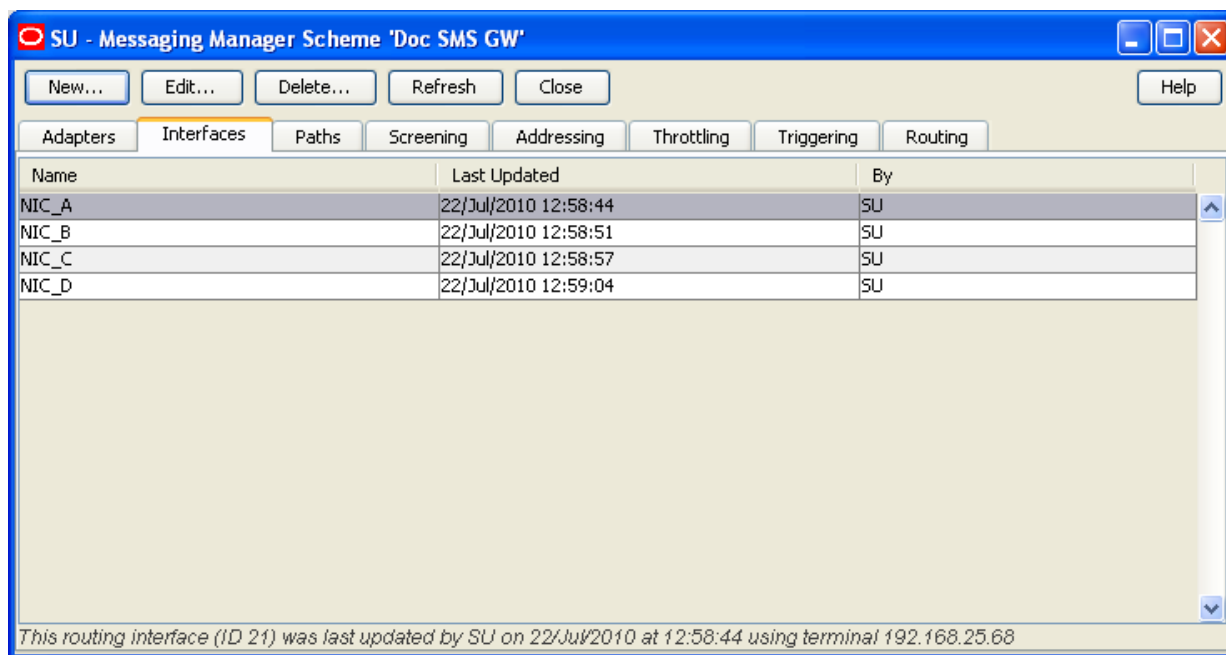
Introduction

The **Interfaces** tab enables you to configure Interface records.

Interfaces are used in IP connections and nodes. The IP addresses associated with interfaces are defined in nodes. An interface record in a scheme can have a different IP address in each node the scheme is assigned to.

Interfaces panel

Here is an example of the **Interfaces** tab.



Interfaces fields

This table describes the function of the field.

Field	Description
Name	The name of this interface.

Adding interfaces

Follow these steps to add a new interface to a routing scheme.

For more information about interfaces, see *Interfaces and nodes* (on page 12).

- | Step | Action |
|------|--|
| 1 | On the Interfaces tab, click New....
Result: The New Routing Interface screen opens. |
-
- 2 In the **Name** field, enter the name of this interface.

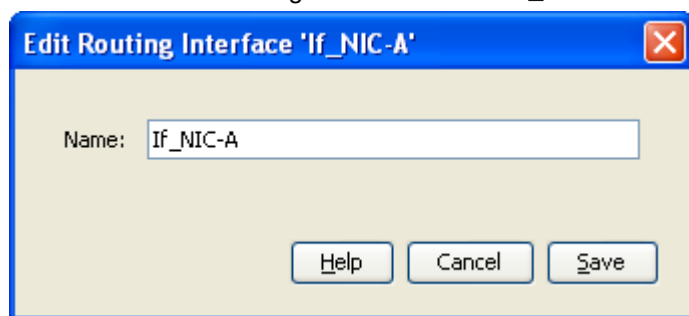
Step	Action
3	Click Save to save the new Interface record in the configuration database.

Editing interfaces

Follow these steps to edit an existing interface name.

For more information about interfaces, see *Interfaces and nodes* (on page 12).

Step	Action
1	On the Interfaces tab, select the record to edit.
2	Click Edit . Result: The Edit Routing Interface ' <i>Interface_Name</i> ' screen opens.



3	In the Name field, update the interface's name.
4	Click Save .

Deleting interfaces

Follow these steps to delete an existing interface record.

Step	Action
1	On the Interfaces tab, select the record to delete.
2	Click Delete.... Result: The Delete Routing Interface confirmation prompt opens.
3	Click Delete to delete the record from the configuration database.

Paths

Introduction

The **Paths** tab enables you to add, update and remove the user-defined paths for this scheme. All paths into and out of Messaging Manager need to be specified in this tab.

A path is a common label applied to a collection of similar connections. Connections are grouped as follows:

- Messages received from connections within the same path will be treated equally. Routing, classification, relay rules, all downstream processing will only examine the path, and will not examine the individual connection details.

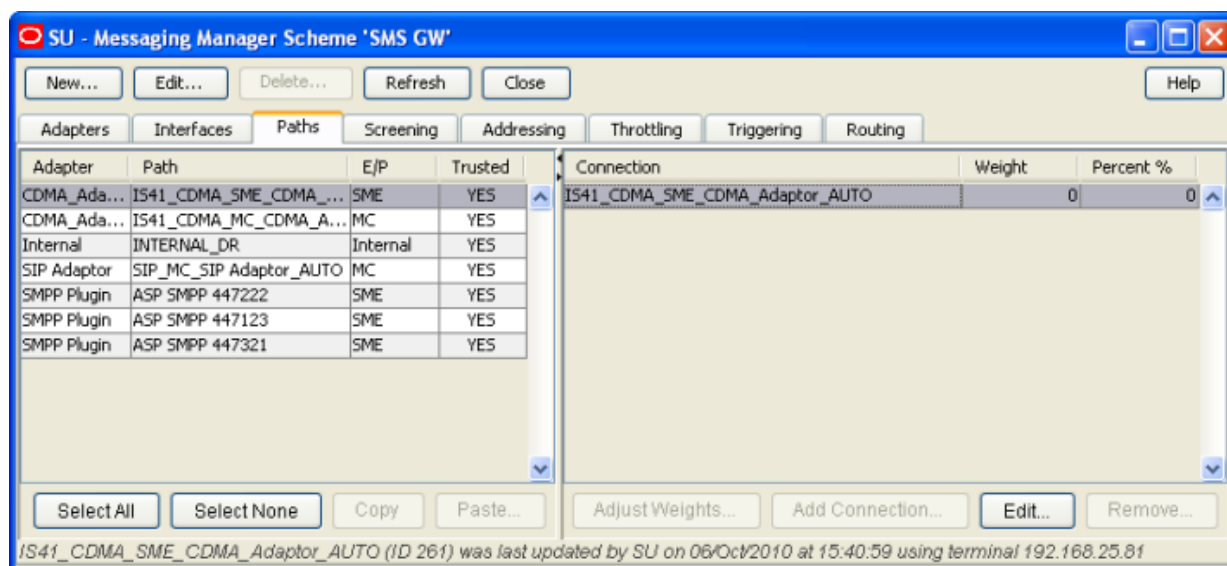
- Outbound delivery will select a path, and it is assumed that all connections within that path are functionally equal. Weighting parameters and outbound connection parameters may determine that one connection is preferred over another, but any single message delivered on that path may select any valid connection at any time.

All connections in a path must:

- Connect to the same endpoint type (SMC or SME)
- Use the same protocol (one of SMPP, EMI, MAP, IS41_CDMA, or IS41_TDMA) through the same adapter

Paths tab

Here is an example of the **Paths** tab.



Note: The columns on this screen can be expanded or collapsed in the same way as for the **Screening** tab. For more information about how to use this functionality, see *Adjusting panel displays* (on page 76).

Paths tab columns

These tables describe the content of each column. The information is sorted by adapter and then path.

Column	Description
Adapter	The adapter this path is using.
Path	The path name. Note: This name must be able to be matched at least once against the entries in the path prefix list.
E/P	Displays the endpoint type of each path.
Trusted	Indicator of path spam trustworthiness.

These column contents are for the selected adapter and path combination.

Column	Description
Connection	Lists all the connections for the selected path.
Weight	Lists all the weightings for the selected path.

Column	Description
Percent %	Lists all the calculated weighting percentages for the selected path.

Paths tab buttons

This table describes the function of each button, specific to the **Paths** tab, at the bottom of the tab.

Note: Buttons are active depending on the selection context.

Button	Description
Select <u>A</u> ll	Selects all the paths for this scheme.
Select <u>N</u> one	De-selects any selected paths for this scheme. This button is available whenever a path is selected.
<u>C</u> opy	Copies the data from the currently selected record ready for pasting into another record.
Paste...	This pastes a previously copied set of data into the current record.
Adjust <u>W</u> eights...	Opens the Adjust Connection Weights on Path <i>Path_Name</i> screen.
Add Connection...	Opens a new screen with blank connection record fields.
<u>E</u> dit...	Opens the Edit Connection screen for the selected connection.
<u>R</u> emove...	Deletes the selected connection record. This button is available on selecting a rule.

Other path buttons

This table describes the function of other buttons found on **Paths** tab sub panels.

Note: Buttons are active depending on the selection context.

Button	Description
<u>R</u> emove...	After selecting a path connection and clicking Remove... , if you are sure you want to delete the selected record, click Remove to proceed. If you do not want to delete the record, click Don't Remove .
Don't Remove	
Equalise <u>W</u> eights	Used to adjust the weighting of all connections for the selected path to be equal.

Path screen fields

This table describes the function of each field in the New Path and Edit Path screens.

Field	Description
Name	Name for this path. This field is required.
Adapter	The adapter this path will use. The field is required.
Endpoint type	The destination type. There are two options: - MC (Message Centre - SMSC) - SME (Short Message Entity - ASP or MSC). This field is required.

Field	Description
ASP account	The ASP account that is associated with this path. This list is populated by the <i>ASPs</i> (on page 67) tab. Optional. This field is not available on paths that use an SS7 or internal adapter.
ASP short code	If you select a short code, MM will set up a deliver routing rule to this path, where short code is the destination address of the rule. The available short codes are the short codes configured for the ASP account selected in the ASP account field. This field is not available on paths that use an SS7 or internal adapter. Optional.
Default routing path	The path to use when no matching routing rule can be found when using the route action. This field is optional. Warning: If this path is needed and has not been provided here, the message is dropped.
Message centre	SMSC associated with this path. See <i>SMSCs</i> (on page 57) for an explanation of the association. Notes: • This field is disabled (grayed out) if you select <i>MC</i> for the endpoint type. • If you have selected <i>SME</i> for the endpoint type, this field is required.
Statistics category	The text entered in this field will be added to the <i>DETAIL</i> column of the <i>SMF_STATISTICS</i> database table. This field is optional. For more information, see <i>MM Technical Guide</i>. Note: For delivery reports this value will automatically be <i>INTERNAL_DR</i>.
Max messages/sec	Sets the maximum number of messages per second allowed through the path for EMI and SMPP protocols. This field is optional.
This is a trusted path	Whether or not messages received on this path will go through the screening rules. Trusted paths do not have screening applied to them.
Enabled	This path is available for traffic. For incoming paths, a disabled path will not be available to be assigned to messages. For outbound paths, a disabled path will not be used to carry traffic. Notes:

Field	Description
	- If you disable all the paths for a routing rule, the routing rule will stop delivering traffic. - Changing the enabled status of a path does not change the enabled status of the path's connections.

Adding paths

Follow these steps to add a new path to an adapter.

Step	Action
1	From the Paths tab, click New. Result: The New Path screen appears.

- Fill in the **Name**, **Adapter** and **Endpoint type** fields.
For more information about the fields in this screen, see *Path screen fields* (on page 84).
- If you have selected for the endpoint type:
 - MC, select a value from the default routing path field if a default routing path is needed for this path
 - SME, select a value from the **SMSC**: drop down list
- Configure any remaining fields to complete the path.
- Click **Save** to save the new path record in the configuration database.

Editing paths

Follow these steps to edit an existing path:

Step	Action
1	In the table on the Paths tab, select the record to edit.
2	Click Edit at the top of the tab or double-click the record.

Result: The Edit Path 'Path_Name' screen opens.

- | | |
|---|---|
| 3 | Edit the fields to reflect the changes you need to make.
For more information about the fields in this screen, see <i>Path screen fields</i> (on page 84). |
| 4 | Click Save to save the path record in the configuration database. |

Deleting paths

Follow these steps to delete an existing path.

Step	Action
1	From the table on the Paths tab, select the record to delete.
2	Click Delete .
	Result: The Delete Path 'Path_Name' confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

Path Connections

Introduction

When adding a connection to a path, the input screen shown will depend on the protocol type used by the adapter.

For IP connections (EMI, SMPP, SIP), see *IP Connections* (on page 89).

For all other protocols, predefined paths and their SS7 connections are automatically added when the adapter is created. These predefined connections cannot be edited or deleted. However, more paths and connections may be added. For details, see *SS7 Connections* (on page 98).

Multiple connections can be configured for each path. These are used by Messaging Manager for receiving and delivering messages.

About user authorization for local and remote connections

Convergent Charging Controller provides a secure credential vault for storing the user names and passwords and for authorizing users. Messaging Manager stores the user names and passwords for local and remote connections to the secure credential vault and retrieves them when it needs to authorize a connection.

When you add an EMI or SMPP connection, you specify the local user name and password for connections into Messaging Manager and the remote user name and password for connections from Messaging Manager to a remote system. You can edit the connection to change the local or remote user password if required. See *Changing connection passwords* (on page 97) for more information.

Adjust connection weightings

Follow these steps to adjust the weighting that are given to each connection in a path.

Note: The weightings of connections can only be adjusted for user defined connections.

Step	Action
1	From the Paths tab, click Adjust Weights... Result: The Adjust Connection Weights on Path '<i>Path_Name</i>' screen appears.
2	Adjust the ratio of the weighting for each connection as required. Weightings may be adjusted either by moving the slider using the mouse, or by entering a weighting ratio into the field to the right of the slider.

Step	Action
3	Select the Failover check box for any connections to be used in the case that all other connections fail. Note: This check box is meaningless for SS7 connections.
4	To set the weighting of all connections to be equal, click Equalise Weights .
5	Click Save to save the new connection weights.

Deleting connections

Follow these steps to delete an existing connection.

Step	Action
1	From the table in the right-hand panel on the Paths tab, select the connection to delete.
2	Click Remove.... Result: The Remove Connection ' <i>Connection_Name</i> ' confirmation prompt will appear.
3	If the connection can be deleted, click Delete to delete the record from the configuration database.

IP Connections

Common connection fields

This table describes the function of each field in the top part of both the EMI and SMPP connection screens.

Field	Description
Name	The name of the connection.
Weighting	The weighting to apply to this connection when determining which connection to use. This value is converted to a percentage of the weightings for all the connections on this path, which in turn is used as the loading factor for the connection. Allowed values: 0 (zero) to 100, where 0 is the failover connection weighting. The connection with zero weighting will be used when all other connections cannot be used.
Enabled	Selected Allow Messaging Manager to use this connection for traffic Deselected Do not allow Messaging Manager to use this connection for traffic
Preopen	Selected Messaging Manager opens this connection on startup. Deselected Messaging Manager waits for a message to open the connection

Field	Description
RX	Selected The remote endpoint receives messages from Messaging Manager Deselected The remote endpoint does not receive messages from Messaging Manager
TX	Selected Allow this connection to transmit messages (remote point of view) Deselected Do not allow this connection to transmit messages
Shadowed	Available only for SMPP connections where the SMPP path endpoint is SME.(Short Message Entity). Selected Messaging Manager reports successful login to the ASP only after Messaging Manager logs in to the default routing path as defined in the SME path Deselected Messaging Manager reports successful log in to the ASP immediately
Local username	Authorized user name for Messaging Manager access from ASP.
Local password	Required password for the user name specified in the Local username field. When you edit a connection, a check box is displayed to the left of Local password . To change the local password, select the check box and enter a new password. To specify no password, leave the password field empty.
Remote username	Authorized user name for Messaging Manager to access SMSC.
Remote password	Required password for the user name specified in the Remote username field. When you edit a connection, a check box is displayed to the left of Remote password . To change the remote password, select the check box and enter a new password. To specify no password, leave the password field empty.
Connections allowed	Allow the same ASP to connect this number of times on the same port using the same login.
Local listen	IP address or host name of the local listener defined in eserv.config .
Port	Port number of the local listener.
Local source	The Messaging Manager local source to use for connections to a remote listener.
Port	Port number of the local source.
Remote listen	IP address or host name of the remote listener for connections from Messaging Manager.
Port	Port number of the remote listener.
Remote source	The remote source for connections to Messaging Manager.

Adding EMI connections

Follow these steps to add a new EMI type connection to the selected path.

Step	Action
1	From the Paths tab, click Add Connection .

Step**Action**

Result: The New EMI Connection screen appears.

New EMI Connection

Name:

Weighting:

☒ Enabled ☐ Preopen ☐ RX ☐ TX

Local username: Local listen:

Local password: Local source:

Remote username: Remote listen:

Remote password: Remote source:

Connections allowed:

EMI Options

Window size: Alert poll time:

Max window queue length: Alert address:

Login orig. type of number: Alert protocol ID:

Login orig. number plan ID: Session timeout:

Default source address: Response timeout:

Allow alt. source address: ☒ Response poll time:

Provide VMSC in HPLMN: ☐ Default protocol ID:

Allow user time zones: ☐

CDR information:

- 2 Complete the fields as required in the top part of the screen. See *Common connection fields* (on page 89).

Note: When adding a new connection the **Save** button becomes available when you have entered content and the **Name** field.

- 3 Complete the **EMI Options** fields as required. See *EMI connection fields* (on page 92).
- 4 Click **Save** to save the new Connection record in the configuration database.

Note: The system determines which type of connection is required by the looking at the protocol that is used by the adapter selected when creating the path. This protocol is used to open the correct type of New Connection screen.

EMI connection fields

This table describes the function of each field in the **EMI Options** area of the EMI Connection screen.

Field	Description
Window size	Determines the number of messages that Messaging Manager can receive from the ASP before waiting for a response. Allowed values: 0-100 Default: 100
Max window queue length	When the Window size is exceeded, the messages are queued up, this parameter determines the length of the queue. Messaging Manager can queue outgoing messages to cope with temporary peaks in outgoing load that result in the window filling up. Default: 1024
Login orig. type of number	Originator Type Of Number. Allowed values: -1 none (default) 1 international number (starts with country code) 2 national number 6 Abbreviated number (short number alias)
Login orig. number plan ID	Originator Numbering Plan ID. Allowed values: -1 none (default) 1 E.164 address 3 X121 address 5 Private (TCP/IP address/ abbreviated number if omitted)
Default source address	Where there is no source address supplied Messaging Manager will generally use the Login username if supplied. This option allows a specific source address to be used instead. This field is optional.
Allow alt. source address	If set to true, will allow Messaging Manager to accept Alternate Source Addresses. Default: Selected (true)
Provide VMSC in HPLMN	If true Messaging Manager will populate the VMSC address in the HPLMN field if available. Default: Not selected (false)
Allow user time zones	If set to true, the EMI adapter converts timezones of all outgoing times using the user timezone from a genericSM. If set to false the adapter does not perform any timezone conversion. Default: Not selected (false)
CDR information	Used to allow connection based static information to be added to the CDRs. The exact information entered into this field will be entered into the CDR. It is recommended that any information entered into this field uses standard CDR format. For more information about CDR format, see <i>EDR Reference Guide</i> .
Alert poll time	How long, in seconds, to wait before polling for alerts. Default: -1

Field	Description
Alert address	The address of Messaging Manager that is sent to the message centre in MT alert messages. Default: 0
Alert protocol ID	Alert Protocol Identifier. Default: 639
Session timeout	Timeout (in seconds) for the EMI connection to the ASP. Default: -1 (that is, it never times out)
Response timeout	Determines the time in seconds that the IP adapter listener will wait for a response from the ASP to any EMI message it sends. However, a distinction is made between messages queued for transmission because the connection is down and those which have been sent. MM does not timeout responses for sent messages. Therefore the backup route will not be tried unless a negative response is received or if the connection is already down. Default: 4
Response poll time	The length of time (in seconds) between polls. Default: 2
Default protocol ID	Default Protocol Identifier. Default: 64

Editing EMI connections

Follow these steps to edit an existing EMI type connection.

Step	Action
1	From the table on the right-hand panel of the Paths tab, select the record to edit.
2	Click Edit at the bottom of the screen or double-click the record. Result: The Edit EMI Connection ' <i>Connection_Name</i> ' screen opens, where <i>Connection_Name</i> is the name of the selected connection.
3	Update the fields as required. See <i>Common connection fields</i> (on page 89) and <i>EMI connection fields</i> (on page 92) for information about the available connection fields.
4	Click Save to save the connection record in the configuration database.

Example Edit EMI Connection dialog

Here is an example edit connection dialog for the EMI protocol. In this example, the name of the connection is XMSPI1.

The screenshot shows the 'Edit EMI Connection' dialog box for a connection named 'XMSPI1'. The dialog has a title bar with a close button (X). The main area contains several fields and checkboxes for configuring the connection.

Fields and Checkboxes:

- Name:** XMSPI1
- Weighting:** 10
- Enabled:** ☒ **Preopen:** ☐ **RX:** ☒ **TX:** ☒
- Local username:** m1
- Local password:** ☐
- Remote username:** r1
- Remote password:** ☐
- Connections allowed:** 1
- Local listen:** (dropdown menu)
- Local source:** (dropdown menu)
- Remote listen:** cwm.me.uk
- Remote source:**
- IP address / host name:** (label above Remote listen)
- Port:** 1234

EMI Options:

- Window size:** 100
- Max window queue length:** 1024
- Login orig. type of number:** International number
- Login orig. number plan ID:** E.164 address
- Default source address:**
- Allow alt. source address:** ☒
- Provide VMSC in HPLMN:** ☐
- Allow user time zones:** ☐
- CDR information:**
- Alert poll time:** -1
- Alert address:** 0
- Alert protocol ID:** PC appl via abbrev. no.
- Session timeout:** -1
- Response timeout:** 4
- Response poll time:** 2
- Default protocol ID:** 65

Buttons: Help, Cancel, Save

Adding SMPP connections

Follow these steps to add a new SMPP connection to the selected path:

Step	Action
1	From the Paths tab, click Add Connection.... Result: The New SMPP Connection screen appears.

Step	Action
	New SMPP Connection Name: Weighting: 1 ☒ Enabled ☐ Preopen ☐ RX ☐ TX ☐ Shadowed Local username: Local password: Remote username: Remote password: Connections allowed: 1 IP address / host name Port Local listen: Local source: Remote listen: Remote source: SMPP Options SMPP version: 3.4 Max. concurrent transactions: 1024 System ID: MMX System type: MMX Outgoing timeout: 10 Idle timeout: 0 Heartbeat interval: 0 ☒ Augment IDs ☐ eSG Extensions Help Cancel Save

- 2 Complete the fields as required in the top part of the screen. See *Common connection fields* (on page 89).

Note: When adding a new connection the **Save** button becomes available on entering the **Name** field.

- 3 Complete the **SMPP Options** fields as required. See *SMPP connection fields* (on page 95).

- 4 Click **Save** to save the new connection record in the configuration database.

Note: The system determines which type of connection is required by the looking at the protocol that is used by the adapter selected when creating the path. This protocol is used to open the correct type of New Connection screen.

SMPP connection fields

This table describes the function of each field in the **SMPP Options** area of the SMPP Connection screen.

Field	Description
Version	The version of SMPP that will be used by default. Default: 0x34 (version 3.4)
System ID	ID of Messaging Manager application. Used on SMPP messages. Default: Oracle MMX
System type	System type on SMPP messages.

Field	Description
	Default: MMX
Max. concurrent transactions	Number of concurrent transactions allowed per second. Default: 1024
Outgoing timeout	Timeout, in seconds, on outgoing side. Default: 10
Idle timeout	How long a connection may be idle for. Default: 0
Heartbeat interval	Specifies the length of time to wait after receiving a message from the peer until an <code>enquire_link</code> message is sent. The connection will be closed if an <code>enquire_link_resp</code> (or any other kind of message) within the time specified by <code>outgoingTimeout</code> is not received. Default: 0 (that is, no heartbeats sent)
Augment IDs	If selected, the message ID sent back to the ASP by MM will be prefixed with the correlation ID from the outgoing SMSC connection. Note: This field is only available for SMPP connections in an ASP path.
Correlation ID	The correlation ID of the SMPP SMSC connection. Notes: - This field is only available for SMPP connections in an SMSC path. - The Correlation ID allows two connections to be related, by placing the same <code>smscCorrelationId</code> setting for both connections. It is used where there are different connections used for rx and tx to the SMSC and they need to be related, for example, so they can use the same name in persistent store keys. For more information, see <i>MM Technical Guide</i>.
eSG Extensions	Whether to transmit non-standard data on this connection. That is, is the path used to communicate with SEI instead of an SMPP ASP.

Editing SMPP connections

Follow these steps to edit an existing SMPP type connection.

Step	Action
1	From the table on the right-hand panel of the Paths tab, select the record to edit.
2	Click Edit at the bottom of the screen or double-click the record. Result: The Edit SMPP Connection ' <i>Connection_Name</i> ' screen opens, where <i>Connection_Name</i> is the name of the selected connection.
3	Update the fields as required. See <i>Common connection fields</i> (on page 89) and <i>SMPP connection fields</i> (on page 95) for more information about the available fields.
4	Click Save to save the connection record in the configuration database.

Example Edit SMPP Connection dialog

Here is an example edit connection dialog for the SMPP protocol. In this example, the name of the connection is XMSP12.

The screenshot shows the 'Edit SMPP Connection' dialog box for a connection named 'XMSP12'. The dialog is organized into several sections:

- General Fields:**
 - Name: XMSP12
 - Weighting: 10
 - Enabled: ☒ Preopen: ☐ RX: ☒ TX: ☒ Shadowed: ☐
- Local and Remote Settings:**
 - Local username: m2
 - Local password: ☐ (disabled)
 - Remote username: r2
 - Remote password: ☐ (disabled)
 - Connections allowed: 1
 - Local listen: (dropdown)
 - Local source: (dropdown)
 - Remote listen: cwm.me.uk
 - Remote source: (empty field)
- IP address / host name and Port:**
 - Local listen: (dropdown) Port: 4321
 - Local source: (dropdown) Port: 0
 - Remote listen: cwm.me.uk Port: 4321
 - Remote source: (empty field)
- SMPP Options:**
 - SMPP version: 3.4
 - Max. concurrent transactions: 1024
 - System ID: eSG MMX
 - System type: MMX
 - Outgoing timeout: 10
 - Idle timeout: 0
 - Heartbeat interval: 0
 - Augment IDs: ☐ eSG Extensions: ☐
- Buttons:** Help, Cancel, Save

Changing connection passwords

Follow these steps to change the password of the local or remote user for an EMI or SMPP connection.

Step	Action
1	From the table on the right-hand panel of the Paths tab, select the record to edit.
2	Click Edit at the bottom of the screen or double-click the record. Result: The Edit <i>protocol</i> Connection ' <i>Connection_Name</i> ' screen opens. Note: You can also edit a connection record from the Asps tab.
3	Select the check box to the left of the password field you want to change. Result: The password field is enabled.
4	Enter a new password in the password field. To specify no password, leave the password field empty.
5	Click Save . The new password is saved in the credentials vault.

SS7 Connections

Adding SS7 connections

Follow these steps to add a new SS7 type connection to the selected path.

Step	Action
1	From the Paths tab, click Add Connection.... Result: The New SS7 Connection screen appears.

New SS7 Connection

This routing scheme is currently deployed on 1 SCP

Name: ☒ Enabled

☐ Inbound ☐ Outbound

Remote PC: ☒ Match any PC PC: 0
SCCP Calling Party point code (exact match) *SCCP Called Party point code. At least one of GT and PC is required.*

Remote SSN: ☒ Match any SSN SSN: 8
SCCP Calling Party subsystem number (exact match) *SCCP Called Party subsystem number (required)*

Remote GT: ☒ Match any GT GT: 0
SCCP Calling Party global title (prefix match) *SCCP Called Party global title Digits*

TT: 0
SCCP Called Party global title Translation Type

Weight: 0 % ☒ Failover

- Enter a name for the connection.
- The inbound connection is used for matching the inbound path. The outbound connection sets the connection for outbound messages. Both are allowed.
If required, select one or both check boxes.
Result: The fields below each check box will become active.

Note: The **Save** button becomes available if you select the **Inbound** check box.

- Complete the fields as required See *SS7 connection fields* (on page 99) below.

Note: If you select only the **Outbound** check box the **Save** button becomes available after you have entered a PC and an SSN in the fields.

- Click **Save** to save the new connection record in the configuration database.

Note: The system determines which type of connection is required, by the looking at the protocol that is used by the adapter selected when creating the path. This protocol is used to open the correct type of New Connection screen.

Virtual SMSCs

You can create virtual SMSCs in order to provide different services to different groups of end users. The users are provided with the Service Centre Address (SCA) of the virtual SMSC instead of the "real" SMSC's SCA. This allows Messaging Manager to route based on the SCA to which the message is addressed and provide different services based on the SCA.

Messaging Manager allows the inbound path assigned to a message to be based on the SMSC SCA:

- To which the message is addressed, in the case of mobile originated messages
- Received from, in the case of mobile terminated messages

SS7 connection fields

These tables describes the function of each field.

In and Outbound

Here are the fields available for both inbound and outbound paths.

Field	Description
Name	The name of the connection.
Enabled	Is this connection available for traffic?

Inbound

Here are the fields available for inbound path.

Field	Description
Remote PC	The SCCP calling party point code This parameter takes priority over SSN match.
Remote SSN	The SCCP calling party subsystem number.
Remote GT	The SCCP calling party global title (prefix match).

Note: Each of these fields is active only if the **Match any** check box beside it is not selected.

Outbound

Here are the fields available for outbound path.

Field	Description
PC	The SCCP called party point code This parameter takes priority over SSN match.
SSN	The SCCP called party subsystem number.
GT	The SCCP called party global title (prefix match).
TT	The translation type of the SCCP called party GT.
Weight	The relative load for this connection on the path. This value is converted to a percentage of all the connection weights on this path which in turn is used as the loading factor for the connection. Allowed values: 0 to 100.
Failover	There is no concept of failover for SS7 connections, so this field is ignored.
Congestion threshold	Whenever this number of consecutive congestion responses is received, the SMSC will not be used until the back-off period expires.

Field	Description
	Note: This field is only available if the destination point is an SMSC (that is, endpoint type is MC).
Congestion backoff	If congested, the number of seconds to wait before retrying the SMSC. Note: This field is only available if the destination point is an SMSC (that is, endpoint type is MC).

Editing SS7 connections

Follow these steps to edit an existing SS7 connection:

Step	Action
1	From the table on the right hand panel on the Paths tab, select the record to edit.
2	Click Edit at the bottom of the screen or double-click the record. Result: The Edit SS7 Connection ' <i>Connection_Name</i> ' screen appears.

The screenshot shows the 'Edit SS7 Connection' dialog box for the connection named 'MAP_MC_2MAP_AUTO'. The dialog is titled 'Edit SS7 Connection 'MAP_MC_2MAP_AUTO'' and has a close button in the top right corner. It contains several fields and checkboxes for configuring the SS7 connection.

Name: MAP_MC_2MAP_AUTO ☒ Enabled

☒ Inbound ☐ Outbound

Remote PC: (Any) ☒ Match any PC PC: 0
SCCP Calling Party point code (exact match) SCCP Called Party point code. At least one of GT and PC is required.

Remote SSN: (Any) ☒ Match any SSN SSN: 8
SCCP Calling Party subsystem number (exact match) SCCP Called Party subsystem number (required)

Remote GT: (Any) ☒ Match any GT GT: 0
SCCP Calling Party global title (prefix match) SCCP Called Party global title Digits

SCA/SMSC: (Any) ☒ Match any SMSC TT: 0
Service centre address (exact match) SCCP Called Party global title Translation Type

Weight: 0 % ☐ Failover

Congestion threshold: messages

Congestion backoff: seconds

Buttons: Help Cancel Save

- 3 Change the fields as required. See *SS7 connection fields* (on page 99).
- 4 Click **Save** to save the new connection record in the configuration database.

Screening

Introduction

The **Screening** tab controls the screening-out of undesired messages, by allowing the creation of rules that check various message parameters such as originating and destination addresses.

The top part of the tab contains the current list of rules for the selected transaction type.

The bottom part of the tab shows any extra details available for the currently selected rule.

Monitoring screening rules

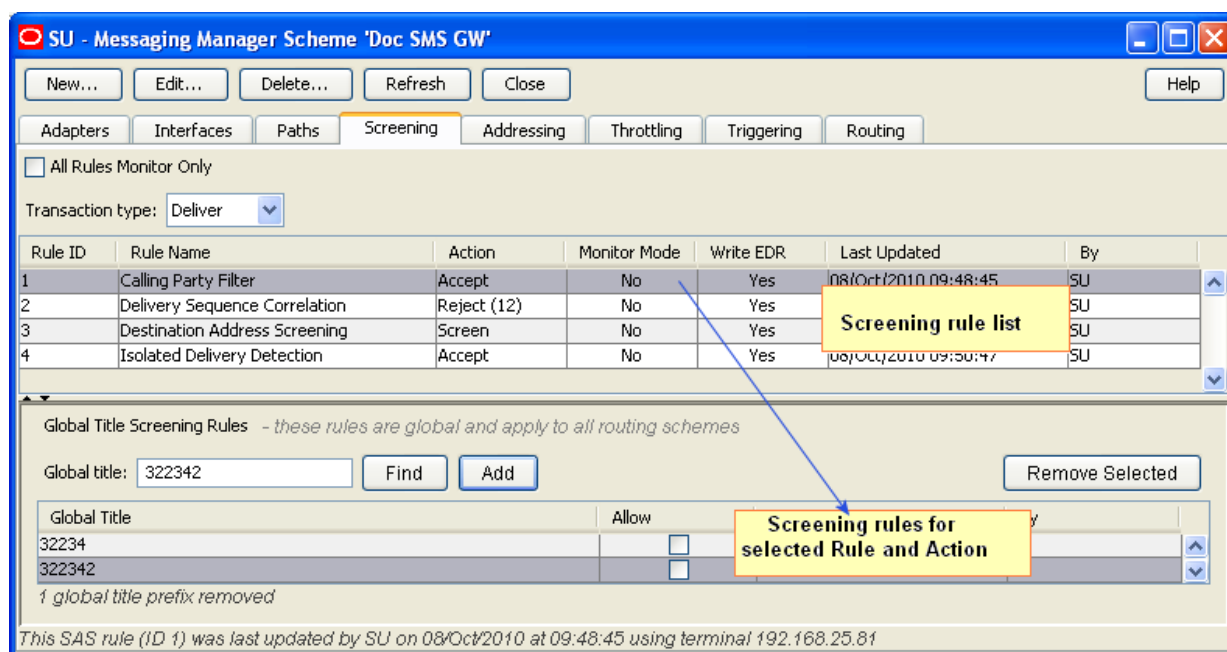
If a screening rule is in monitoring state, the rule is not applied. Instead an EDR is written recording the SMS/call details, and the screening rule ID for the rule which would have blocked the SMS/call.

Note: If a rule is in monitoring state, an EDR will be written regardless of whether the **Write EDR** check box is selected for that rule.

For more information about EDR post-processing, see *EDR Reference Guide*.

Screening tab

Here is an example of a **Screening** tab.



Note: The columns on this screen can be expanded or collapsed in the same way as for the **Paths** tab. For more information about how to use this functionality, see *Adjusting panel displays* (on page 76).

Screening tab columns

This table describes the content of each column. This table is sorted by rule name.

Column	Description
Rule ID	The numeric ID for the rule. This is auto-generated on creation of the rule. Note: This field cannot be changed after it is first saved.
Rule Name	One of the rule types in screening rule list. Note: This field cannot be changed after it is first saved.
Action	The action that will be taken if this rule causes the message to fail screening. Notes:

Column	Description
	- This does not apply to the originating and the destination address screening rules, as these will specify an action for each configured prefix. - This field cannot be changed after it is first saved.
Monitor Mode	Whether or not this rule is in monitor state. YES or * means the rule is in monitor state. For more information about monitoring, see <i>Monitoring screening rules</i> (on page 27).
Write EDR	Indicator for EDR production when the rule is invoked. If the rule is in monitor state, and the rule has been set to not write EDRs, this column will show * and EDRs will be written until the rule is moved from monitoring to applying.

Screening rule fields

This table describes the function of each field.

Field	Description						
Transaction type	The type of message being handled by Messaging Manager, selected from a configured list. Allowed values: - Deliver - Notify - Route Info - Submit						
Rule type	The name given to the rule, selected from a built-in list, as described in <i>Screening rule list</i> (on page 27).						
Action	The action the rule will perform when invoked, selected from a configured list. Allowed values: <table> <tr> <td>Accept</td><td>Do not do anything with the message, but return an ACK to the originator.</td></tr> <tr> <td>Discard</td><td>Drop the message without sending any response to the originator.</td></tr> <tr> <td>Reject</td><td>Do not do anything with the message, and send an error back to the originator.</td></tr> </table>	Accept	Do not do anything with the message, but return an ACK to the originator.	Discard	Drop the message without sending any response to the originator.	Reject	Do not do anything with the message, and send an error back to the originator.
Accept	Do not do anything with the message, but return an ACK to the originator.						
Discard	Drop the message without sending any response to the originator.						
Reject	Do not do anything with the message, and send an error back to the originator.						
Release cause	The error code to use that explains the reject reason. See <i>Action and Error Codes</i> (on page 141).						
Monitor mode	Do not apply this rule. Instead monitor the effect this rule would have if it was applied. For more information about monitoring, see <i>Monitoring screening rules</i> (on page 27).						
Write EDR	Causes an EDR to be written when the rule is invoked. Note: This value is ignored if the rule is in monitoring state. A rule is being monitored if its Monitor this rule check box is selected, or the Monitor check box on the Screening option is selected.						

Screening rule list

The set of screening rules available is different for each transaction type as shown in the following table.

Rule Type	Submit	Deliver	Notify	RouteInfo
<i>Calling Party Filter</i> (on page 27)	Y	Y	Y	Y
<i>Delivery Sequence Correlation</i> (on page 28)		Y	Y	
<i>Destination Address Screening</i> (on page 28)	Y	Y	Y	Y
<i>Isolated Delivery</i> (on page 28)		Y	Y	
<i>Layer Address Correlation</i> (on page 28) (GSM only)	Y	Y	Y	Y
<i>Originating Address Screening</i> (on page 29)	Y	Y	Y	
<i>Roaming Location Validation</i> (on page 29)	Y			

Notes:

- Screening rules are not applied to traffic from any path which has the **This is a trusted path** check box selected. For more information about this check box, see *Path screen fields* (on page 84).
- To use the full screening capabilities, a valid screening license must be purchased. Unlicensed users will only have access to the originating address screening and destination address screening rules.

Calling Party Filter

This check is used to:

- Screen out (blacklist) known rogue entities on the network (pirates)
- Allow (white list) known safe entities

A message will be screened if all of the following apply:

- It is received on a path that does not have the **This is a trusted path** check box selected
- The “Calling Party Filter” rule is configured for the message’s transaction type
- The message’s SCCP calling party global title is matched by the screened global title list

When this rule is selected the *Global Title Screening Rules* (on page 107) panel is displayed on the screen.

Delivery Sequence Correlation

If an inbound deliver or notify message is received on a path that is not flagged as trusted and the “Delivery Sequence Correlation” rule is specified, Messaging Manager will compare the message parameters with the corresponding RouteInfo that was previously received. Message parameters are matched as follows, and the message is screened out if any of the comparisons fail:

MT SMS Field	Expected Value
SCCP Calling Party	SCCP calling party of the RouteInfo
SCCP Called Party	GT returned by Messaging Manager in response to the RouteInfo
SCA	SCCP calling party of the RouteInfo

Destination Address Screening

Destination address screening rules check the digits of the destination address against a configured list of prefixes. For each address prefix, an address rule will specify that the message has either passed or failed screening.

If the address rule is a:

- 'pass' rule, it will assign a destination domain for subsequent processing.
- 'fail' rule, it will specify the action to take.

When this rule is selected the *Destination Screening Rules* (on page 111) panel is displayed in the bottom part of the screen.

Isolated Delivery

When a mobile-terminated SMS (MAP MT-ForwardSM and IS41 SMDPP) is received, the isolated delivery rule checks that a RouteInfo message (HLR lookup) was received before the SMS. If a delivery sequence correlation rule (described above) is also used, Messaging Manager will check that the details in the two requests match up.

If MSID masking is on, or an Accept action is used, MM responds to incoming RouteInfo messages with a temporary IMSI (or MIN). This means that when a subsequent deliver or notify message is received, it will use the MM-generated IMSI, so can be linked with the previous RouteInfo.

If an inbound deliver or notify message is received on a path that is not flagged as trusted, the "Isolated Delivery" rule will check that the IMSI corresponds to one that was previously generated in response to a RouteInfo. The message will be screened out if this is not the case.

Layer Address Correlation

When a message is received, MM can do a basic check to ensure that the parameters provided in the SCCP layer and MAP layer are consistent.

If this rule is used and a MAP message is received on a path that is not flagged as trusted, MM will verify that the prefixes of the following MAP and SCCP address match:

Message Type	SCCP Field	MAP Field
RouteInfo	CallingParty	Service Centre Address
Deliver / Notify	CallingParty	SM-RP-OA
Submit	CalledParty	SM-RP-DA

The number of digits to compare for the SCA Consistency check is determined by finding the longest country prefix matching the address, in the *SCA Consistency Rules* (on page 109) panel displayed in the bottom part of the screen.

Originating Address Screening

This rule checks the digits of the originating address against a configured list of prefixes. For each address prefix, an address rule will specify that the message has either passed or failed screening.

If the address rule is a:

- 'Pass' rule, it will assign an originating domain for subsequent processing
- 'Fail' rule, it will specify the action to take

When this rule is selected the *Originating Screening Rules* (on page 111) panel is displayed in the bottom part of the screen.

Roaming Location Validation

An additional correlation check can be applied to mobile-originated SMSs (MAP MO-ForwardSM and IS41 SMDPP) to validate that when a message comes from a local subscriber via a foreign network, that subscriber is actually known to be roaming.

If a mobile-originated SMS is received on a path that is not flagged as trusted, this rule will force Navigator to query the HLR to determine the MSC serving the originating subscriber. A message will pass if the Calling Party SCCP Address and MSC address from the HLR match, to the determined number of digits.

When this rule is selected the *RLV Prefix Rules* (on page 114) panel is displayed in the bottom part of the screen.

Adding Screening rules

Follow these steps to add a screening rule.

- | Step | Action |
|------|--|
| 1 | <p>From the Screening tab, select the transaction type for the required rule from the Transaction Type drop down list.</p> <p>Note: The New button is unavailable when all allowable rules have been added for the transaction type. No more rules can be added.</p> |
| 2 | <p>From the Screening tab, click New.</p> <p>Result: The New SAS Rule screen appears with the selected transaction type pre-populated.</p> |

New SAS Rule

Rule Identification

Transaction type: Deliver

Rule type: Calling Party Filter

Rule Processing

Action:

Release cause:

☐ Monitor Mode

☒ Write EDR

Help Cancel Save

- 3 Select the new rule from the **Rule type** drop down list.
- Note:** This list shows what rules can still be added to the selected transaction type.

Step	Action
4	Select the action this rule will perform from the Action drop down list. Note: This list shows all the allowed actions for the rule type.
5	If the reject action was selected, select the ACS release cause number form the Release cause drop down list. Note: This list shows all the allowed ACS release cause numbers that have been configured. See <i>Action and Error Codes</i> (on page 141).
6	Complete the rest of the fields on the screen. For more information about the rest of the fields on this screen, see <i>Screening rule fields</i> (on page 102).
7	Click Save to save the new rule record in the configuration database.

Editing Screening rules

Follow these steps to edit a screening rule.

Step	Action
1	From the Screening tab, select the transaction type for the required rule from the Transaction Type drop down list. Result: A list of rules for the transaction type are shown.
2	From the Screening tab, click Edit . Result: The Edit SAS Filter Rule 'Rule_Id' screen appears.

- | | |
|---|---|
| 3 | To cause an EDR to be generated when this rule is invoked, select the Write EDR check box. |
| 4 | Click Save to save the new rule record in the configuration database. |

Delete Screening rules

Follow these steps to delete a screening rule.

Step	Action
1	From the Screening tab, select the transaction type for the required rule from the Transaction Type drop down list. Result: A list of rules for the transaction type are shown.
2	From the table on the Screening tab, select the record to delete. Note: The default originating or destination address rules cannot be deleted.
3	Click Delete . Result: The Delete SAS Rule 'Rule_Name' confirmation prompt appears.
4	Click Delete to delete the record from the configuration database.

Global Title Screening Rules

Introduction

Global title screening defines originating global title (GT) prefixes that are one of the following short messages when calling party filter is active for the transaction type:

- Barred from sending
- Allowed to send

Note: The screening is global, that is, the list applies to all routing schemes.

When applying a rule, the system goes through the list and applies the longest, starting with the same digits, prefix rule. For example, 44 will be applied over 4, 4 over a blank prefix.

Global Title Screening Rules panel

Here is an example Global Title Screening Rules panel of the **Screening** tab.

This panel is visible when you select the *Calling Party Filter* (on page 27) rule type.

Global Title Screening Rules - these rules are global and apply to all routing schemes

Global title:

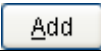
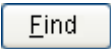
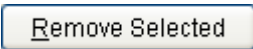
Global Title	Allow	Last Updated	By
	☐	Thu Nov 15 02:49:23 GM...	SU
32234	☐	Tue Nov 13 22:20:14 GM...	MMX_ADMIN
322343	☒	Tue Nov 13 22:20:14 GM...	MMX_ADMIN

This SAS rule (ID 29) was last updated by SU on 14/Nov/2007 at 01:23:45 using terminal 127000001001

Rules buttons

This table describes the function of each button, specific to the panel, at the bottom of the tab.

Note: Buttons are active depending on the selection context.

Button	Description
	Add a new rule.
	Locates a rule containing the entered digits.
	Deletes the selected rule.

Finding a rule

Follow these steps to find a rule.

Step	Action
1	Enter the number string to find in the Global title field. Result: The Find button becomes available.
2	Click Find . Result: The first rule containing the entered string is highlighted.
3	Click Find repeatedly to cycle through the rules containing the entered string.

Adding a rule

Follow these steps to add a rule.

Step	Action
1	Type the prefix number string to add as a new rule in the Global title field and click Add . Result: The typed number is added to the list. Note: You can add a blank prefix. In this case, if there are no other prefixes that override the rule, then the rule will apply to all prefixes.
2	In the Allow check box, to: - Blacklist this prefix, deselect the box - Allow the prefix, select the box.

Removing a rule

Follow these steps to remove a screening rule.

Step	Action
1	Locate and select the rule to delete. Either use the scroll bar or the Finding a rule procedure.
2	Click Remove Selected . Result: The Remove Global Title Prefix ' <i>Global_Title</i> ' confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

SCA Consistency Rules

Introduction

The SCA consistency rules are available when *Layer Address Correlation* (on page 28) is selected as the rule type.

This check is for MAP messages only and confirms that the MAP layer and SCCP layer are consistent with their calling and called party addresses. The SCA consistency rules match the SCCP address against the country prefix and then compare the MAP and SCCP addresses based on the match length digits value.

Note: The SCA consistency rules are global and apply to all routing schemes.

SCA Consistency Rules panel

Here is an example SCA Consistency Rules panel of the **Screening** tab.

This panel is visible when you select the *Layer Address Correlation* (on page 28) rule type.

Rules buttons

This table describes the function of each button, specific to the panel, at the bottom of the tab.

Note: Buttons are active depending on the selection context.

Button	Description
	Add a new rule.
	Edit an existing rule.
	Locates a rule containing the entered digits.
	Deletes the selected rule.

Finding SCA Consistency Rules

Follow these steps to find SCA consistency rules.

Step	Action
1	Type the prefix number string to find in the Country prefix field. Result: The Find button becomes available.

Step	Action
2	Click Find . Result: The first rule containing the entered string is highlighted.
3	Click Find repeatedly to cycle through the rules containing the entered string.

Adding SCA Consistency Rules

Follow these steps to add new SCA consistency rules.

Step	Action
1	Click Add.... Result: The New SCA Consistency Rule screen appears.

- 2 Enter the prefix digits to compare in the **Country Prefix** field.
- 3 The number of digits to compare is automatically calculated, but this can be overridden if required by selecting from the **Digits to Match** drop down list.
- 4 Click **Save** to save the new SCA consistency rule record in the configuration database.

Editing SCA Consistency Rules

Follow these steps to edit SCA consistency rules.

Step	Action
1	Locate and select the SCA consistency rule to edit. Use either the scroll bar or the <i>Finding SCA Consistency Rules</i> (on page 109) procedure.
2	Click Edit.... Result: The Edit SCA Consistency Rule 'Country_Prefix' screen appears.

Step	Action
3	Override the number of digits to compare by selecting from the Digits to Match drop down list.
4	Click Save to save the SCA consistency rule record in the database.

Deleting SCA Consistency Rules

Follow these steps to delete a SCA consistency rule.

Step	Action
1	Locate and select the SCA consistency rule to delete. Use either the scroll bar or the <i>Finding SCA Consistency Rules</i> (on page 109) procedure.
2	Click Remove Selected . Result: The Remove SCA Consistency Rule ' <i>country prefix</i> ' confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

Screening Rules

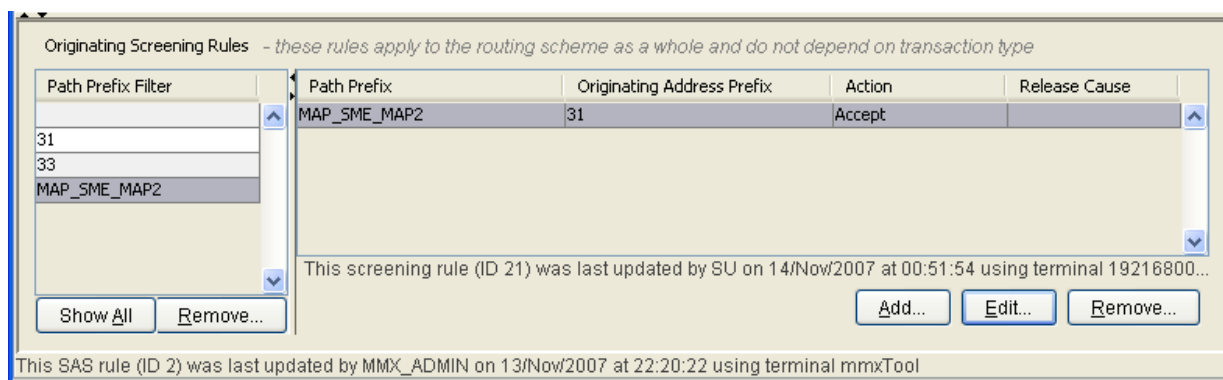
Introduction

Screening rules apply to both destination and originating addresses. This topic illustrates how to configure originating address rules. There is no procedural difference between the destination and originating address types.

Screening Rules panel

Here is an example Screening Rules panel of the **Screening** tab.

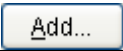
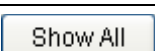
This panel is visible when you select the *Destination Address Screening* (on page 28), or *Originating Address Screening* (on page 29) the rule type.



Screening rule panel buttons

This table describes the function of each button, specific to the **Screening Rules** panel, at the bottom of the tab.

Note: Buttons are active depending on the selection context.

Button	Description
	Add a new screening rule.
	Edit an existing screening rule.
	Deletes the selected path prefix filter (and all rules that use the filter), or deletes the selected path prefix screening rule.
	Shows all the screening path prefix rules.

Screening Rules fields

This table describes the function of each field.

Field	Description
<i>Path_Direction</i> path name prefix	The path prefix filter.
<i>Path_Direction</i> address prefix	The address prefix.
Perform action	The drop down list is the action which will be attached to the screening rule. You can select from: • Allow • Accept (this drops the call) • Reject • Discard
Release cause	If the perform action drop down list has the reject action selected, this field is the error code which will be returned with the reject message. Note: These are defined on the Global tab (on page 143) of the Action and Error Codes screen.

Adding Screening rules

Follow these steps to add new destination or originating address screening rules.

Step	Action
1	Select the Path Prefix Filter to add the rule to. Note: If this is a rule for a new filter, this step can be ignored and the filter is added as part of adding the rule.
2	Click Add . Result: The Add <i>Address_Type</i> Screening Rule screen appears.

Step	Action
------	--------

Add Originating Screening Rule

This routing scheme is currently deployed on 1 SCP

Screening selection criteria

Incoming path name prefix: MAP_SME_MAP2

Originating address prefix:

Screening response

Perform action: Allow

Release cause:

Help

Cancel

Save

- 3 If missing, type the path prefix filter in the *Path_Direction* path name prefix field.
- 4 Continue to configure this record by entering data in the fields in the middle of this screen. For more information about the fields on this screen, see *Screening Rules fields* (on page 112).
- 5 If the **Reject** action selected, select the error code from the **Release cause** drop down list.
- 6 Click **Save** to save the new screening rule record in the configuration database.

Editing screening rules

Follow these steps to edit destination or originating address screening rules.

Step	Action
------	--------

- 1 From the **Screening** tab, select the **Path Prefix** to edit from the Screening Rules panel table.
- 2 Click **Edit...**
Result: The *Edit Address_Type* Screening Rule screen appears.

Step	Action
------	--------

- 3 Edit the fields to reflect the changes you need to make.
For more information about the fields in this screen, see *Screening Rules fields* (on page 112).
- 4 Click **Save** to save the screening rule record in the configuration database.

Deleting screening rules

Follow these steps to delete Destination or Originating Address Screening Rules.

Step	Action
------	--------

- 1 From the **Screening** tab, select the **Path Prefix** to delete from the Screening Rules panel table.
- 2 Click **Delete**.
Result: The Remove Screening Rule screen appears.
- 3 Click **Delete** to delete the record from the configuration database.

RLV Prefix Rules

Introduction

The RLV prefix rule allows you to configure how many digits must match for the roaming location validation check.

The number of digits to match can be configured based on the address prefix.

When doing the roaming location validation check, MM will compare the MSC address from the HLR against the configured prefixes to determine how many digits to match.

A message will pass the roaming location validation check if the calling party SCCP address and MSC address from the HLR match, to the determined number of digits.

RLV Prefix Rules panel

Here is an example RLV Prefix Rules panel of the **Screening** tab.

Note: This panel is visible when you select the *Roaming Location Validation* (on page 29) rule type. Roaming location validation rule types are only available for submit rules.

Prefix	Match Length	Last Updated	By
21	2	08/Jul/2008 04:11:28	
5555	4	08/Jul/2008 03:09:45	

This SAS rule (ID 6612) was last updated by MMX_ADMIN on 19/Jun/2008 at 00:46:13 using terminal mmxTool

Rules buttons

This table describes the function of each button, specific to the panel, at the bottom of the tab.

Note: Buttons are active depending on the selection context.

Button	Description
Add...	Add a new rule.
Edit...	Edit an existing rule.
Find	Locates a rule containing the entered digits.
Remove Selected	Deletes the selected rule.

Finding RLV Prefix Rules

Follow these steps to find RLV prefix rules.

Step	Action
1	Enter the prefix number string to find in the Prefix field. Result: The Find button becomes available.
2	Click Find . Result: The first rule containing the entered string is highlighted.
3	Click Find repeatedly to cycle through the rules containing the entered string.

Adding RLV Prefix Rules

Follow these steps to add new RLV prefix rules.

Step	Action
1	Click Add... . Result: The New RLV Prefix Rule screen appears.

Step	Action
------	--------

- 2 Enter the prefix digits to compare in the **Prefix** field.

Note: You can add a blank prefix. In this case, if there are no other prefixes that override the rule, then the rule will apply to all prefixes.

- 3 The number of digits to compare is automatically calculated, but this can be overridden if required by selecting from the **Digits to Match** drop down list.
- 4 Click **Save** to save the record in the database.

Editing RLV Prefix Rules

Follow these steps to edit RLV prefix rules.

Step	Action
------	--------

- 1 Locate and select the RLV prefix rule to edit. Use either the scroll bar or the *Finding RLV Prefix Rules* (on page 115) procedure.
- 2 Click **Edit....**

Result: The Edit RLV Prefix Rule 'Prefix' screen appears.

- 3 Override the number of digits to compare by selecting from the **Digits to Match** drop down list.
- 4 Click **Save** to save the record in the database.

Deleting RLV Prefix Rules

Follow these steps to delete an RLV prefix rule.

Step	Action
1	Locate and select the RLV prefix rule to delete. Use either the scroll bar or the <i>Finding RLV Prefix Rules</i> (on page 115) procedure.
2	Click Remove Selected . Result: The Remove RLV Prefix Rule ' <i>Prefix</i> ' confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

Addressing

Introduction

The **Addressing** tab enables you to:

- Add, update and remove address rules for originating and destination prefixes for each path prefix
- Add, update and remove domains
- Select a domain to map each rule against

Each message that enters the system is assigned to a domain for each of its originating and destination addresses. Domains are configured as a group, so all routing and triggering changes are applied to the entire domain. A domain allows specification of throttling levels. Additionally, it plays a role in determining control plan selection and routing selection.

Any given routing scheme defines a single set of domains which are used to classify both originating and destination addresses. The originating and destination domains are used to determine the outbound route. Each domain may contain as many address rules as required.

A domain is defined by the set of domain address rules which reference it. A domain is associated with a single scheme, and a domain address rule belongs to a single domain in that scheme.

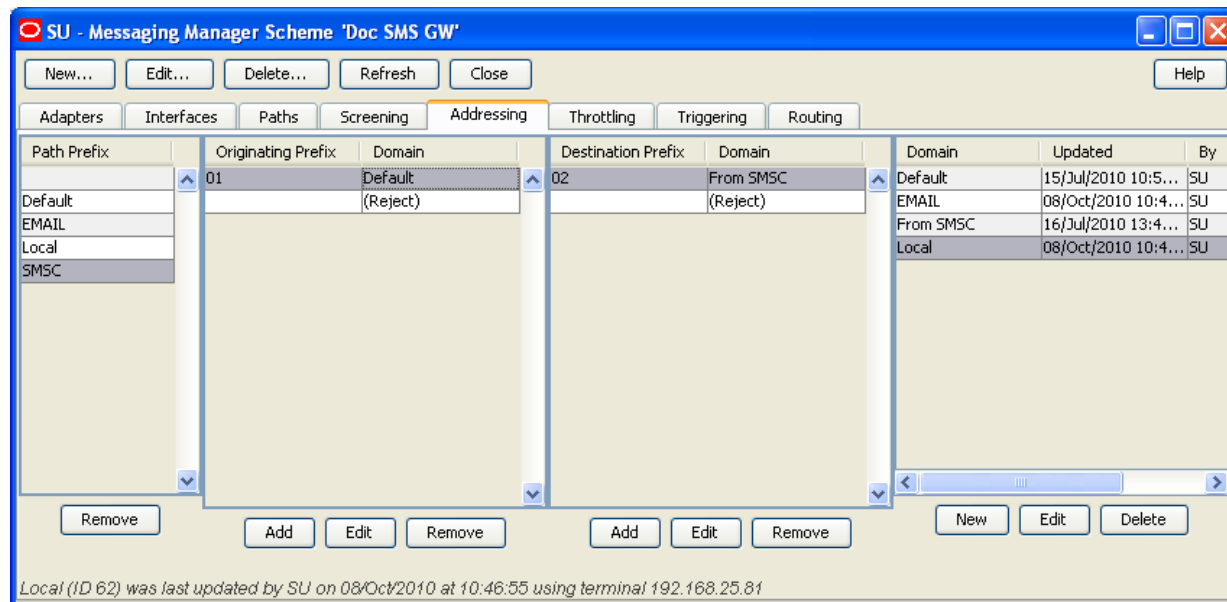
A domain address rule identifies a set of addresses and associates that set with a set of paths. The address set is specified by an address prefix (for example, 00644) and a message type, (for example, Normal, delivery receipt, non-delivery receipt).

An address is considered to be a member of the set defined by the rule if the leading characters of the address match the address prefix and the message type matches the specified type.

The set of paths is identified by a path prefix which works in the same fashion as the address prefix, so a path is considered to be a member of the paths set defined by the rule if the leading characters of the path's name match the path prefix specified in the rule.

Addressing tab

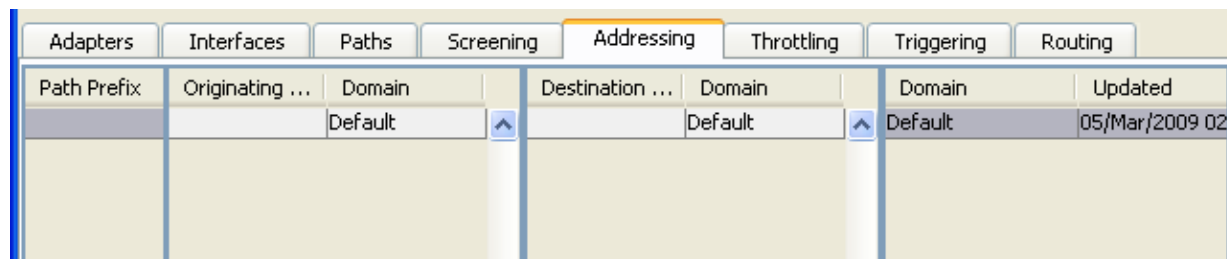
Here is an example **Addressing** tab.



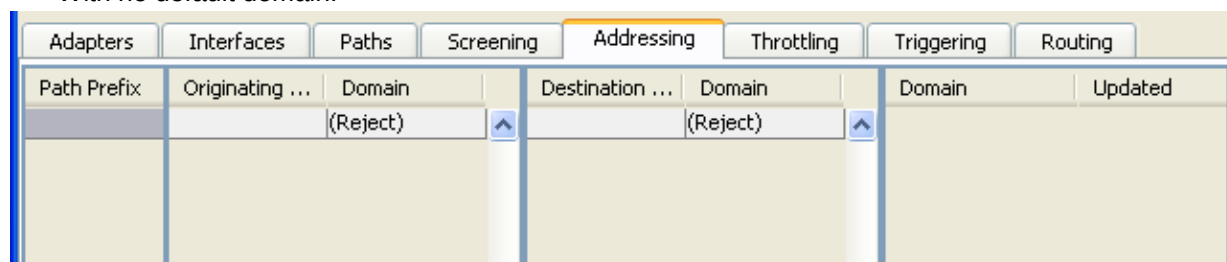
Pre-populated screen areas

The following areas of the **Addressing** tab will be pre-populated, if you have created a new scheme:

- With a default domain:



- With no default domain:



The default path prefix is blank, therefore the default address rules will apply to any prefix.

A default rule with a (Reject) domain is created when there is no domain applied.

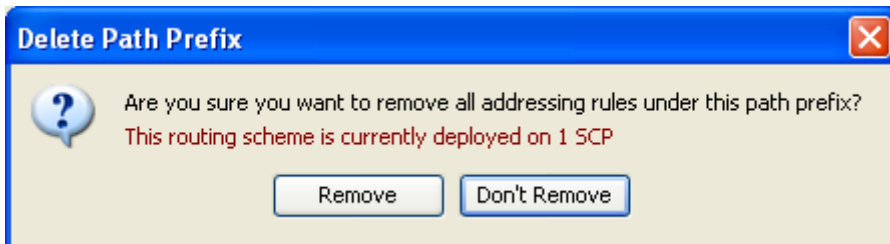
Adding a Path Prefix

The **Path Prefix** area lists the path prefixes that have address rules defined.

A new path prefix is added when you create an address rule that is not attached to any path prefix. See *Adding Address rules* (on page 119) for details.

Removing a Path Prefix

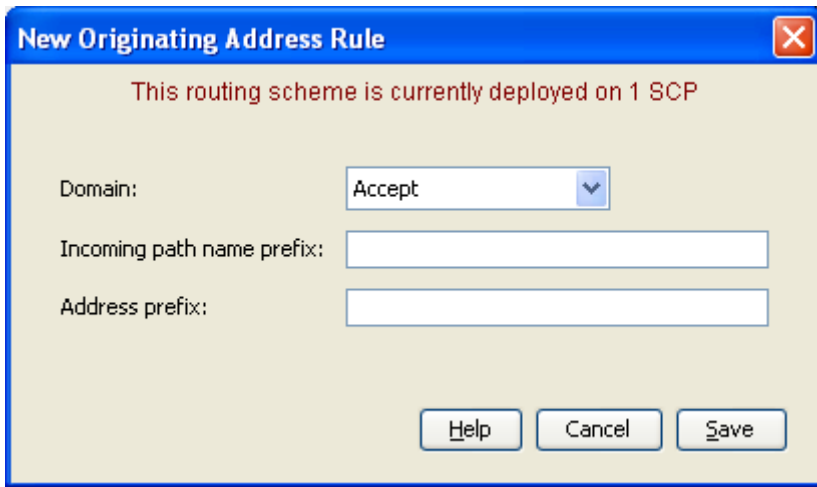
Follow these steps to remove a path prefix.

Step	Action
1	In the table in the Path Prefix area, select the prefix to remove.
2	Click Remove . Result: The Delete Path Prefix confirmation dialog is displayed.
	 The dialog box titled "Delete Path Prefix" contains a question mark icon and the text: "Are you sure you want to remove all addressing rules under this path prefix? This routing scheme is currently deployed on 1 SCP". At the bottom are two buttons: "Remove" and "Don't Remove".
3	Click Remove to delete the path prefix and all its addressing rules or Don't Remove to cancel the delete.

Adding Address rules

Follow these steps to add new destination or originating address rules.

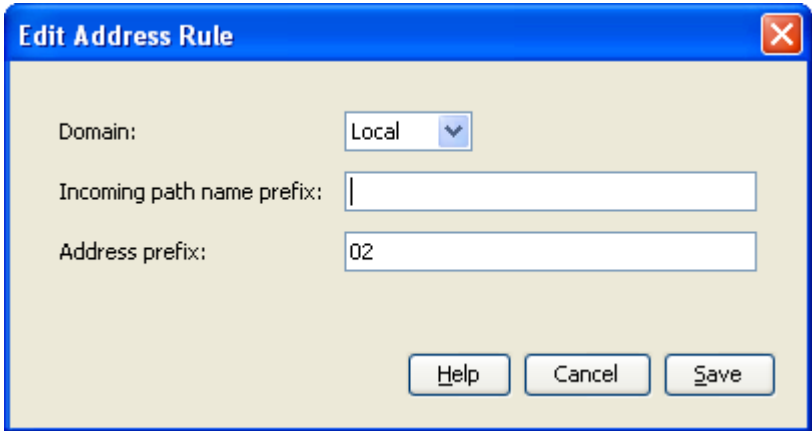
Note: Address rules must be allocated to a domain. If there are no domains in the list, you need to *Adding domains* (on page 121) before you add a rule.

Step	Action
1	Select the Path Prefix to add the rule to. Result: The originating and destination prefixes for the selected path prefix are displayed in the tables to the right. Note: If this is a rule for a new filter, this step can be ignored and the filter is added as part of adding the rule.
2	In the table for the required address type, click Add . Result: The New Address_Type Address Rule screen opens.
	 The dialog box titled "New Originating Address Rule" contains a red warning message: "This routing scheme is currently deployed on 1 SCP". Below this, there are three input fields: "Domain:" with a dropdown menu showing "Accept", "Incoming path name prefix:", and "Address prefix:". At the bottom are three buttons: "Help", "Cancel", and "Save".
3	In the Domain field, select the domain to map the rule against.

Step	Action
	Note: If the domain is not in the list, you need to click Cancel and <i>Adding domains</i> (on page 121) before you add a rule.
4	In the Incoming path name prefix field, enter the prefix. Note: This field is pre-populated with the path prefix selected in Step 1.
5	In the Address prefix field, enter the prefix.
6	Click Save to save the new rule record in the configuration database. Result: Rules are created in pairs. For example, if you create an originating address rule, a destination address rule for the path prefix will be created with a default domain of (Reject).

Editing address rules

Follow these steps to edit a destination or originating address rule.

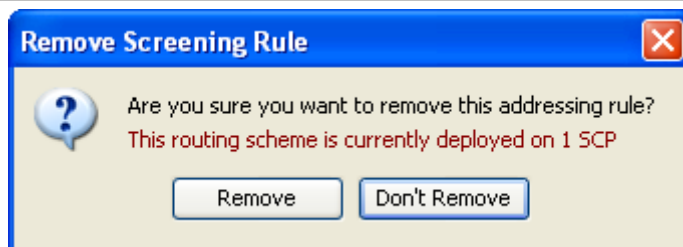
Step	Action
1	Select the Path Prefix of the rule to edit. Result: The originating and destination prefixes for the selected path prefix are displayed in the tables to the right.
2	In the table for the required address type, click Edit . Result: The Edit Address Rule screen appears.
	
3	If required, modify the fields, as described in <i>Adding Address rules</i> (on page 119). Note: If this is a default rule, the '(Reject)' domain is included in the list, otherwise, only the defined domains appear in the list.
4	Click Save to save the rule record in the configuration database.

Removing Address rules

Follow these steps to remove an address rule from either an originating or destination prefix.

Step	Action
1	In the table in a Prefix Area of the Addressing tab, select the record to remove.
2	Click Remove . Result: The Remove Screening Rule confirmation prompt appears.

Step	Action
------	--------



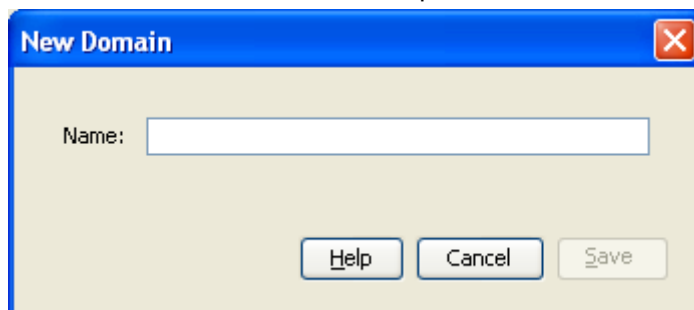
- 3 Click **Remove** to delete the rule or **Don't Remove** to cancel the delete.

Adding domains

Follow these steps to add a new domain to the scheme.

Step	Action
------	--------

- 1 From the **Domain** area of **Addressing** tab, click **New**.
Result: The New Domain screen opens.



- 2 In the **Name** field, enter the name of the new domain.

Note: Domain is defined within the context of a single routing scheme, and must have a unique name within that scheme.

- 3 Click **Save** to save the new domain record in the configuration database.

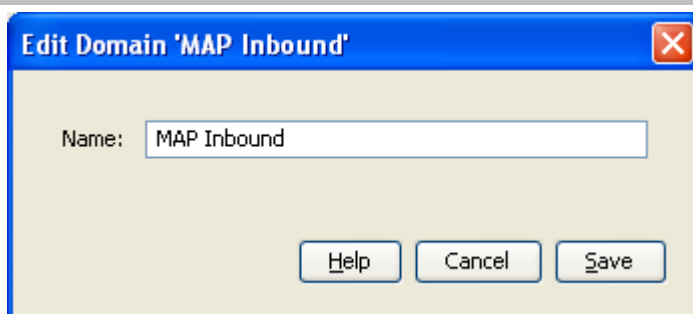
Editing domains

Follow these steps to edit an existing domain.

Step	Action
------	--------

- 1 In the table in the **Domain** area of **Addressing** tab, select the domain record to edit.
 2 Click **Edit**.
Result: The Edit Domain '*Domain_Name*' screen opens.

Step	Action
------	--------



- 3 Change the field value as required.

Note: Changing the name will be reflected everywhere this domain is used within the scheme.

- 4 Click **Save** to save the changed domain record in the configuration database.

Deleting domains

Follow these steps to delete an existing domain:

Step	Action
------	--------

- 1 In the table in the **Domain** area of **Addressing** tab, select the record to delete.
- 2 Click **Delete**.
Result: The Delete Domain '*Domain_Name*' confirmation prompt appears.
- 3 Click **Delete** to delete the record from the configuration database.

Throttling

Introduction

The **Throttling** tab provides a summary report of the throttling values for the selected scheme. This tab allows you to define throttling rules in terms of Originating Domain, Destination Domain, and Message Type (Detection Point).

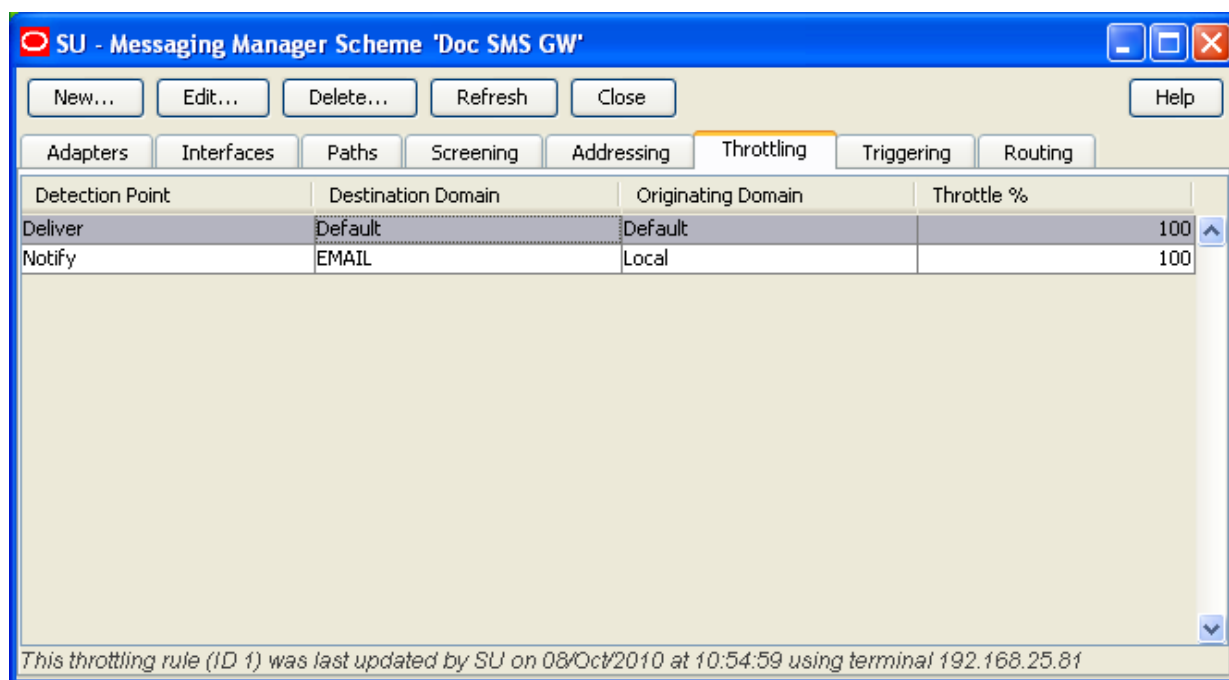
A throttling rule defines the conditions that must be met to throttle a message at a particular limit, specifically in terms of the message's originating & destination Domains and message type. For each message received or generated internally, MM evaluates the message against the throttling rules table to determine if the message is to be throttled.

This provides the ability to implement throttling rules for scenarios such as preferring subscriber-subscriber messages to tele-voting messages, or putting a system-wide throttle on ASP outbound traffic.

For example, tele-voting may be recognized by the destination prefix address of "778". The system may be configured so that tele-voting messages will be throttled when the message rate reaches 80% of the maximum system throughput. The remaining 20% is always available for non tele-voting destinations.

Throttling tab

Here is an example of the **Throttling** tab.



Throttling rules fields

This table describes the content of each field.

Column/Field	Description
Detection Point	The transaction type the throttling rule applies to. Possible values are: • Deliver • Notify • Route Info • Submit For more information about transaction types, see <i>Transaction Types</i> (on page 20). Required.
Destination Domain	The Domain to which the message's destination number belongs. Required.
Originating Domain	The Domain to which the message's originating number belongs. Required.
Throttle at	The level at which throttling is to be applied to messages of this type when overload conditions apply. Required. A percentage of the system maximum concurrent transactions, from 0 to 100 Inclusive. 0 = Throttle (reject) all messages of this type. 100 = No Throttling, allow all messages of this type.

For more information about Domains, see *Address Domains* (on page 29).

Adding Throttling rules

Follow these steps to add throttling rules.

Step	Action
1	From the Throttling tab, click New . Result: The New Throttling Rule screen appears.

- | | |
|---|--|
| 2 | Select values required in each field as described in <i>Throttling rules fields</i> (on page 123). |
| 3 | Click Save to save the record in the configuration database. |

Editing Throttling Rules

Follow these steps to edit an existing Throttling Rule

Step	Action
1	From the table on the Throttling tab, select the record to edit.
2	Click Edit . Result: The Edit Throttling Rule screen appears with the data for the rule selected populated.

Step	Action

- 3 Change the fields, as described in *Throttling rules fields* (on page 123), as required.
- 4 Click **Save** to save the Throttling rule in the configuration database.

Deleting Throttling Rules

Follow these steps to delete a throttling record from the database.

Step	Action
1	From the table on the Throttling tab, select the record to delete.
2	Click Delete .
	Result: The Delete Throttling Rule confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

Triggering

Introduction

The **Triggering** tab enables you to add and maintain Trigger rules. Triggering rules enable MM to decide whether to trigger the message to an ACS control plan for processing, or directly apply an action.

There are four sets of trigger rules:

- 1 Submit
- 2 Deliver
- 3 Notify
- 4 Route Info

The **Detection point** field indicates the set to which the rule belongs.

A trigger rule can optionally specify a routing class. If present, this will be assigned to the message, replacing the existing class when the rule is matched to the message.

A trigger rule either specifies an action to perform, or details of a control plan to invoke. If a control plan is used, the result that it returns to Messaging Manager will determine the action.

Trigger control

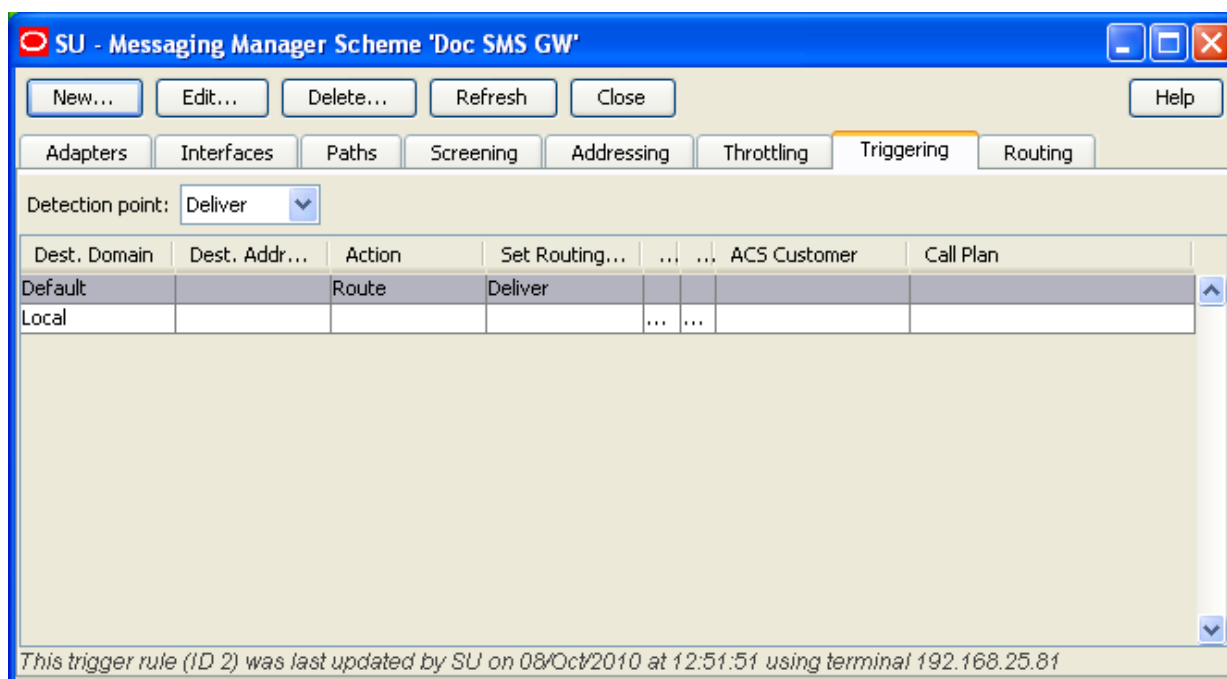
Each Message Type (Submit, Deliver, Notify and Route Info) has its own trigger rules. The transaction is matched against the appropriate rule set to determine the trigger action.

The selected rule may specify a change to the routing class. For example, with a Submit transaction, it is useful to set the trigger routing class to “FDA” so that a First Delivery Attempt becomes the default routing action. This alleviates the need to always set the value to “FDA” in the SMS Service Plan (if it is triggered).

Any change to the routing class occurs regardless of whether the trigger fires or not. If the trigger rule has an SMS Control Plan defined, and the trigger is active, then service control triggering occurs and the SMS Control Plan is invoked to monitor and control the message delivery.

Triggering tab

Here is an example of the **Triggering** tab.



Triggering fields

This table describes the fields that form part of the selection criteria when deciding which (if any) trigger rule to use.

Field	Description
Detection point	The transaction type of the message. Allowed values: • Deliver • Submit • Notify • Route Info See <i>Transaction Types</i> (on page 20) for details.
Originating Domain	Trigger rule applies to messages which have this originating domain. For more information, see <i>Screening Rules</i> (on page 111).

Field	Description
	Notes: - Either Originating Domain or Originating Address prefix must be defined, but not both. - This field is only available when a <code>Submit</code> detection point is selected.
Originating Address prefix	Trigger rule applies to messages which use this originating address (prefix). Notes: - Either Originating Domain or Originating Address prefix must be defined, but not both. - This field is only available when a Submit Detection Point is selected.
Destination Domain	Trigger rule applies to messages which have this destination domain. See <i>Screening Rules</i> (on page 111). Notes: - Either Originating Domain or Originating Address prefix must be defined, but not both. - This field is only available when a Deliver, Notify or Route Info detection point is selected.
Destination Address prefix	Trigger rule applies to messages which use this destination address (prefix). Notes: - Either Originating Domain or Originating Address prefix must be defined, but not both. - This field is only available when a Deliver, Notify or Route Info detection point is selected.

Note: The originating and destination address can be any operator specific number used by an ASP; for example 2222. Telephone numbers cannot be used.

This table describes the rest of the trigger rule fields.

Field	Description
Perform action	What action the trigger is to perform if NOT triggering a control plan. Allowed Values: - Accept - Discard - Reject - Relay (Route Info detection point only) - Route - Route Unchanged (Route Info detection point only) For more information about triggering to control plans, see <i>Triggering</i> (on page 125, on page 31).
Release cause	If you set Perform action to <code>Reject</code> , then select the release cause to send back to the switch from the Release cause list.

Field	Description
	Note: You configure the release causes listed in this field on the Global tab (on page 143) of the Action and Error Codes screen.
Set routing class	Select Set routing class when you want to override the default routing class for SMS messages. You select the routing class override from the predefined list of routing classes. Note: Available for relay or route actions only. The list of supported routing classes depends on which detection point you select. The <i>Deliver</i>, <i>Notification</i> and <i>Submit</i> detection points support these routing classes: • Deliver • FDA • Submit The default <i>Routing Info</i> detection point supports only the <i>Locate</i> routing class. For more information about routing classes, see <i>Routing Class</i> (on page 22).
Trigger a call plan in ACS	Select this check box if you want messages to trigger an ACS control plan.
Use scheduled call plan if present	Select this check box if you want the control plan that is scheduled for the ACS customer to be used.
Use this named call plan	Select this check box if you want to specify the control plan to use. You specify the customer who owns the control plan in the ACS customer field, and the name of the control plan in the Call plan field.
ACS customer	Enter the ACS customer who owns the named control plan. Note: This field is a searchable combo field. For more information about how combo boxes can be used, see <i>Combo boxes</i>.
Call plan	Enter the name of the control plan that this rule uses. Note: This field is a searchable combo field. For more information about how combo boxes can be used, see <i>Combo boxes</i>.

Adding Triggering rules

Follow these steps to add a new Triggering Rule to the selected Scheme.

Step	Action
1	On the Triggering tab, select the Detection Point that the trigger rule is to apply to and click New. Result: - For a 'Deliver', 'Notify' or 'Route Info' Detection Point the following New Trigger Rule screen appears, or - For a 'Submit' Detection Point the New Trigger Rule screen appears with Originating Domain and Originating Address prefix instead of Destination Domain and Destination Address prefix.

Step	Action
------	--------

New Trigger Rule

This routing scheme is currently deployed on 2 SCPs

Trigger Selection Criteria

Detection point: Deliver

Destination Domain:

Destination Address prefix:

Trigger Processing

Perform action: Route

Release cause:

Set routing class: Deliver

Trigger a call plan in ACS

Use scheduled call plan if present

Use this named call plan

ACS customer:

Call plan:

Please press ENTER after keying customer or call plan names.
This will cause the value entered to be retrieved and validated.
You can search in either field by entering partial names.

Note that a limit of 100 rows is returned in each list. If you cannot find the item you're looking for, please narrow your search criteria.

Help

Cancel

Save

2

Select or enter the fields, as described in *Triggering fields* (on page 126), as required.

3

Click **Save** to save the new Triggering rule in the configuration database.

Editing Triggering rules

Follow these steps to update an existing Triggering rule.

Step	Action
1	From the table on the Triggering tab, select the record to edit.
2	Click Edit .

Chapter 5, Messaging Manager Schemes 129

Step	Action
------	--------

Result: The Edit Trigger Rule screen appears.

Edit Trigger Rule

This routing scheme is currently deployed on 1 SCP

Trigger Selection Criteria

Detection point:

Destination Domain:

Destination Address prefix:

Trigger Processing

☐ Perform action:

☐ Release cause:

☐ Set routing class:

☒ Trigger a call plan in ACS

☐ Use scheduled call plan if present

☒ Use this named call plan

ACS customer:

Call plan:

Please press ENTER after keying customer or call plan names.
This will cause the value entered to be retrieved and validated.
You can search in either field by entering partial names.

Note that a limit of 100 rows is returned in each list. If you cannot find the item you're looking for, please narrow your search criteria.

3 Select or complete the fields, as described in *Triggering fields* (on page 126), as required.

4 Click **Save** to save the Triggering rule in the configuration database.

Deleting Triggering rules

Follow these steps to delete an existing Triggering rule.

Step	Action
------	--------

1 From the table on the **Triggering** tab, select the record to delete.

2 Click **Delete**.

Step	Action
	Result: The Delete Trigger Rule ' <i>Rule_Name</i> ' confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

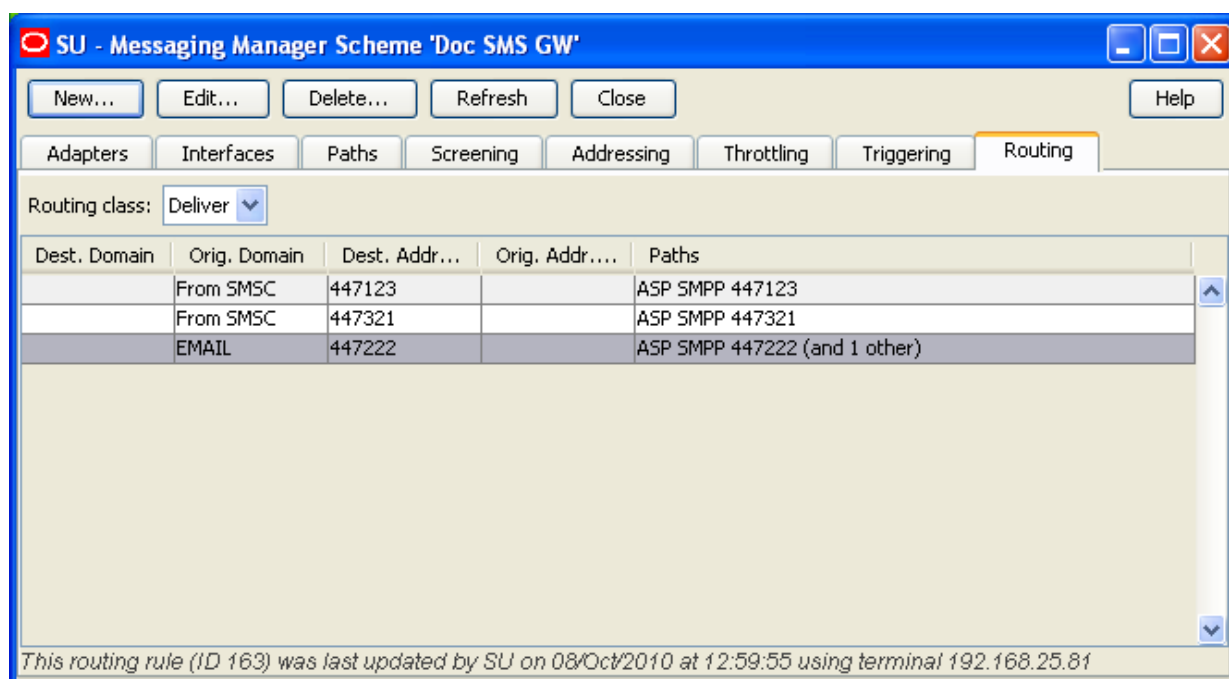
Routing

Introduction

The **Routing** tab enables you to enter and maintain rules that define what paths are used and the sequence they are used in.

Routing tab

Here is an example of the **Routing** tab.



Routing fields

This table describes the function of each field.

Field	Description
Routing class	The routing class type for this outbound route. Allowed values: • Deliver • Submit • Locate
SMSC	The SMSC to use for this outbound route. Note: This field is only available when a Submit Routing class is selected.

Field	Description
Destination domain	SMSs with this destination domain will use this outbound route if no better match is configured. This field is populated by the Domains panel for this routing scheme. Notes: • Either Destination domain or Destination address prefix must be defined, but not both. • This field is only available when a Deliver or Locate Routing class is selected.
Destination address prefix	SMSs with this destination address prefix will use this outbound route if no better match is configured. The destination address prefix to use for this outbound route. Notes: • Either Destination domain or Destination address prefix must be defined, but not both. • This field is only available when a Deliver or Locate Routing class is selected.
Originating domain	SMSs with this originating domain will use this outbound route if no better match is configured. This field is populated by the Domains panel for this routing scheme. Note: Either Originating domain or Originating address prefix must be defined, but not both.
Originating address prefix	SMSs with this originating address prefix will use this outbound route if no better match is configured. Note: Either Originating domain or Originating address prefix must be defined, but not both.
Paths sequencing	List of paths available to this outbound route. Can be selected and manipulated into any desired preferential sequence. Note: Disabled paths will not appear in this drop down list.
Retries	The number of times to retry the path before proceeding to try the next path in the list. Note: These fields are available for MAP and IS-41 protocols only, for EMI and SMPP protocols the entry fields are disabled (as shown for the Deliver and Submit screen examples above).
Interval	The duration in seconds between retrying a path.

Adding Routing rules

Follow these steps to add a new routing rule:

Step	Action
1	On the Routing tab, select the Routing class that the routing rule is to apply to and click New. Result: One of the following screens appear depending on the <i>Routing class</i>:

Step	Action
------	--------

a 'Deliver' Routing class:

New Routing Rule

This routing scheme is currently deployed on 1 SCP

Routing class:

Submit

SMSC:

Default

Originating domain:

Originating address prefix:

Paths sequencing

CDMA1_SMSC

Retries: 0

Interval: 0

Add

Path	Retries	Interval
------	---------	----------

Move Up

Move Down

Remove

Help

Cancel

Save

b 'Submit' Routing class:

Step	Action
------	--------

New Routing Rule ✕

This routing scheme is currently deployed on 1 SCP

Routing class:

Destination domain:

Destination address prefix:

Originating domain:

Originating address prefix:

Paths sequencing

Retries: Interval:

Path	Retries	Inte...

c 'Locate' Routing class:

Step

Action

This routing scheme is currently deployed on 1 SCP

Routing class: Locate

Destination domain:

Destination address prefix:

Paths sequencing

IS41_CDMA_SME_CDMA1

Retries: 0 Interval: 0 Add

Path	Retries	Inte...
------	---------	---------

Move Up Move Down Remove

Help Cancel Save

- 2 Select or enter the fields, as described in *Routing fields* (on page 131), as required.
 - 3 Select a path to use for this Route from the **Paths sequencing** drop down list.
 - 4 Click **Add** to add the selected path to the list of paths to use.
 - 5 Repeat steps 3 and 4 until all required paths are listed.
 - 6 Select each path in turn and enter their number of retries and duration (seconds) between retries in the **Retries** and **Interval** fields.
Click **Update** to save the values.
- Note:** These fields are available for MAP and IS-41 protocols only, for EMI and SMPP protocols the entry fields are disabled (as shown for the Deliver and Submit screen examples above).
- 7 Sort the path list into the desired sequence by selecting the path and then clicking **Move Up** or **Move Down**.
 - 8 Click **Save** to save the new routing rule in the configuration database.

Editing Routing rules

Follow these steps to edit an existing routing rule:

Step	Action
1	On the Routing tab, select the Routing Class for the routing rule to update. Result: All rules for the selected routing class are displayed in the table.
2	From the table in the Routing tab, select the record to edit.
3	Click Edit . Result: The Edit Routing Rule screen applicable to the Routing class for the selected record appears.
4	Select, enter or sort the fields, as described in <i>Routing fields</i> (on page 131), as required.
5	Click Save to save the routing rule to the configuration database.

Deleting Routing rules

Follow these steps to delete an existing routing rule:

Step	Action
1	In the table in the Routing tab, select the record to delete.
2	Click Delete . Result: The Delete Routing Rule ' <i>Route_Name</i> ' confirmation prompt appears.
3	Click Delete to delete the record from the configuration database.

Messaging Manager Replication Screen

Overview

Introduction

Replication is the process used to ensure several instances of databases are kept synchronized. This chapter explains the Messaging Manager replication process.

In this chapter

This chapter contains the following topics.

Messaging Manager Replication	137
Messaging Manager Replication Screen	138
Replication	139

Messaging Manager Replication

Introduction

Configuring Messaging Manager replication enables you to replicate MM data only to nodes which are running MM. Setting up replication has three parts:

- 1 Configuring Messaging Manager replication
- 2 SMF database synchronization across the platform
- 3 Messaging Manager run time synchronization.

For more information about replication, see *SMS User's Guide*.

Configuring MM replication

The **Replication** tab on the Messaging Manager Replication screen enables you to specify which nodes receive Messaging Manager data through replication.

SMF database synchronisation

The replication process copies all the updates to the SCP database on each SLC, as defined by SMS Node Management, **Table Replication** tab.

Replication configuration is set up by clicking the **Create Config File** button in SMS replication screen. For more information about the SMS replication process, see *SMS User's Guide*.

MM run time synchronization

On a regular basis MM Multigate checks MM database tables for any changes made. When found, the differences are extracted and copied to the run time Messaging Manager configuration. This technique allows for Messaging Manager configuration to continuously be updated without the need to stop and restart.

For more information about how to configure the configuration checking period, see `loadIntervalSeconds` parameter in *MM Technical Guide*.

Messaging Manager Replication Screen

Introduction

The Messaging Manager Replication screen enables you to configure which nodes receive MM data. It has only one tab, the **Replication** tab.

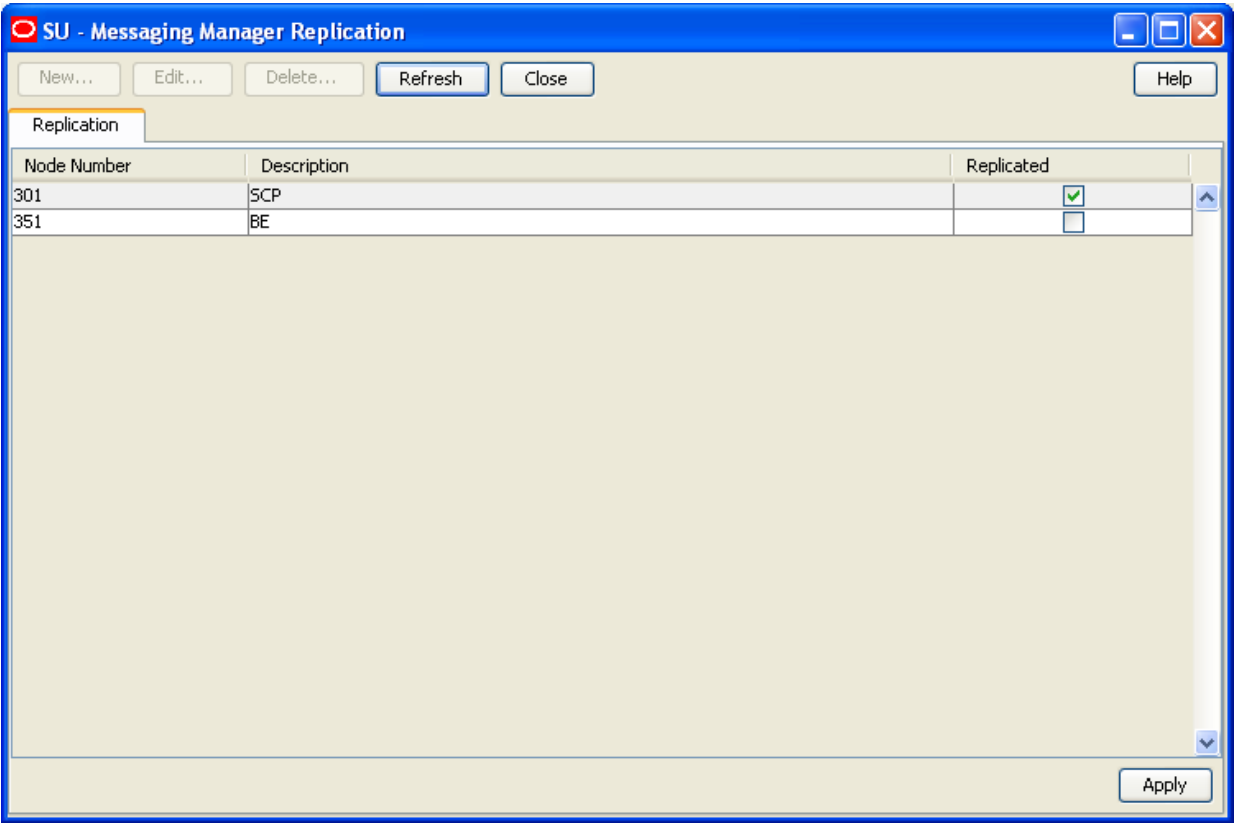
Accessing the Messaging Manager Replication screen

Follow these steps to open the Messaging Manager Replication screen.

Step	Action
1	Select the Services menu from the SMS main screen. 
2	Select Messaging Manager .
3	Select Replication . Result: The Messaging Manager Replication screen displays.

Messaging Manager Replication screen

Here is an example of the Messaging Manager Replication screen.



Replication

Introduction

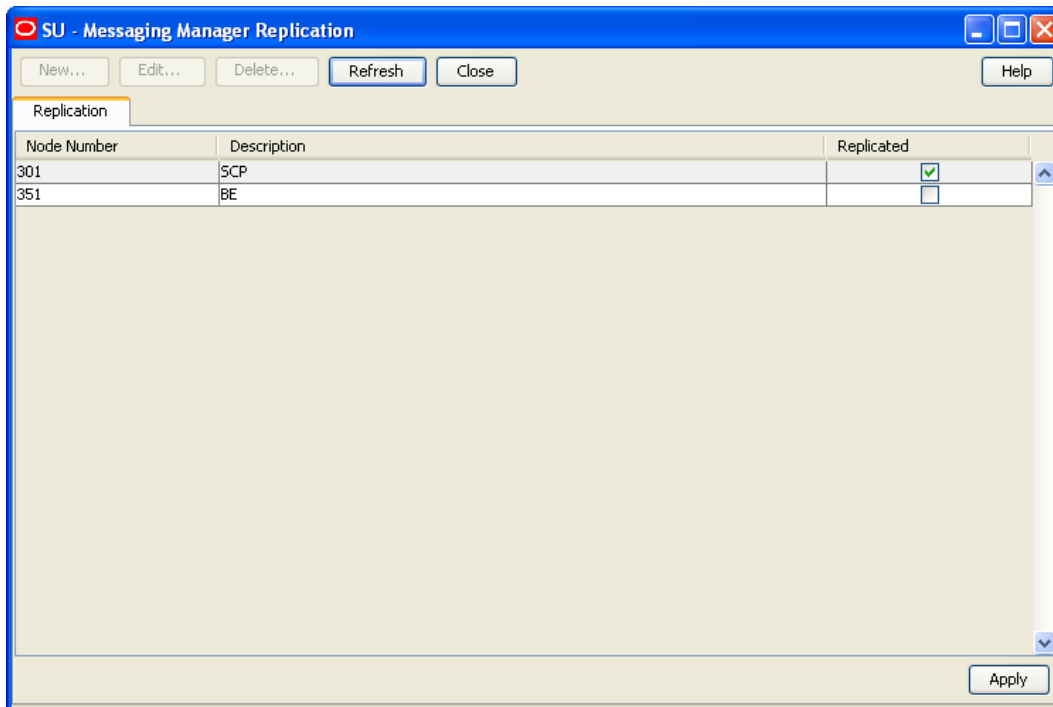
The **Replication** tab enables you to specify which nodes (SLCs) should have Messaging Manager data replicated to them.

Configuring Messaging Manager replication

Follow these steps to flag the Messaging Manager nodes to be included in replication.

Step	Action
1	Open the Messaging Manager Replication screen.

Step	Action
------	--------



- 2 Review the listed Messaging Manager nodes. In each **Replicated** check box, perform one of the following actions:
 - Select, to have the node replicated
 - Deselect, to stop the node from being replicated
- 3 Click **Apply** to save to the database.

Result: SMS will update the "Allocated Replication Groups" in "Table Replication" for all selected nodes.

Messaging Manager Action and Error Codes

Overview

Introduction

This chapter explains how to configure the reject action error codes.

In this chapter

This chapter contains the following topics.

Action and Error Codes	141
Global Action and Error Codes.....	142
SMPP	145
EMI147	
MAP	148
IS-41	150
SIP 152	
Release Cause Mapping	154
Error Mapping	159

Action and Error Codes

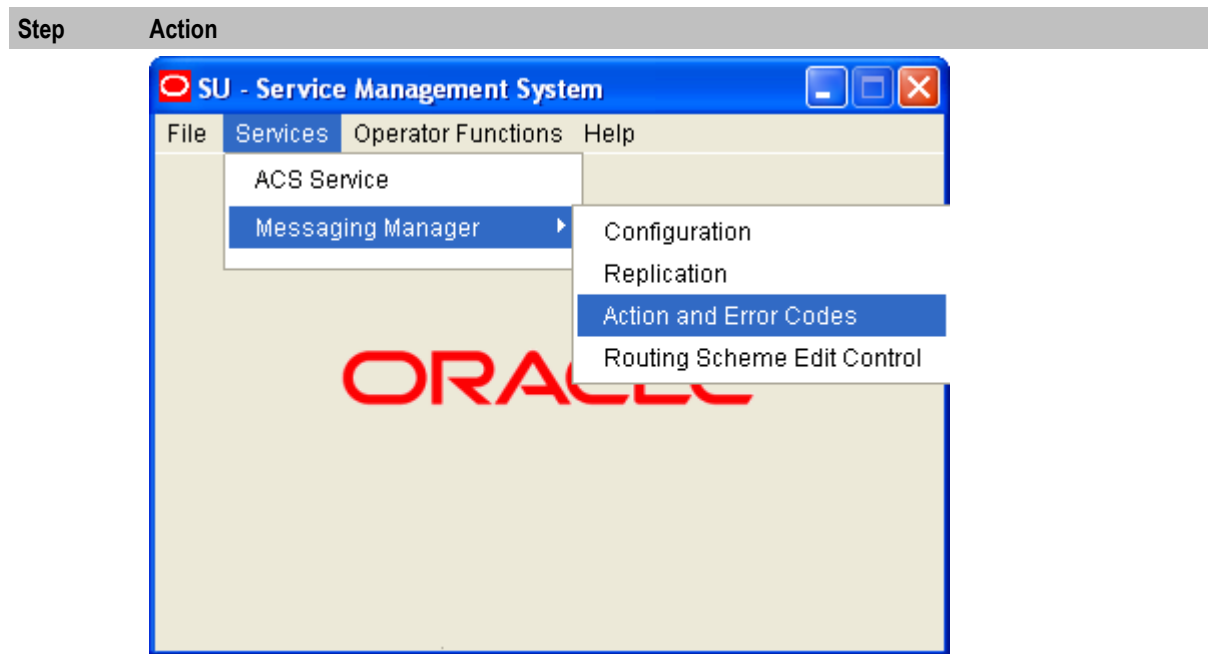
Introduction

The Action and Error Codes configuration allows error codes to be mapped to release causes, and vice versa, and to identify the default release cause for the Reject action (the Discard and Accept actions have permanent, fixed cause values).

Accessing Messaging Manager Action and Error Codes

Follow these steps to open the Messaging Manager Action and Error Codes screen.

Step	Action
1	Select the Services menu from the SMS main screen.



2 Select **Messaging Manager**.

3 Select **Action and Error Codes**.

Result: You see the Messaging Manager Action and Error Codes screen.

For more information about:

- The screen's content and how to enter configuration information, see the other topics in this chapter.
- How all the information works together to create the Messaging Manager configuration, see *Configuration Scenarios* (on page 169).
- Logging into the Service Management System screen, see *SMS User's Guide*.

Release Cause and Error Mappings panels

Each protocol-specific tab (that is, all the tabs except for the Global tab) have two panels:

- 1 Release Cause Mappings panel at the top
- 2 Error Mappings panel at the bottom

Each panel has its own set of New, Edit and Delete buttons in the top right of the panel. These buttons enable you to work with the records in the corresponding panel.

Global Action and Error Codes

Introduction

The **Global** tab displays the global list of action and error codes which define ACS Release Cause values and corresponding error types which may be mapped to protocol-specific error codes.

Global tab

Here is an example **Global** tab.

ACS Release Cause	Error Type	Description	Is Default	Path Fail	Last Updated	By
1	Transient	Network resource shortage		No	27/Oct/2010 22:59:45	MMX_ADMIN
2	Transient	Network Failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
3	Transient	Invalid Teleservice ID		No	27/Oct/2010 22:59:45	MMX_ADMIN
4	Transient	Other network problem		No	27/Oct/2010 22:59:45	MMX_ADMIN
5	Transient	Service centre congestion		No	27/Oct/2010 22:59:45	MMX_ADMIN
6	Transient	PLMN system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
7	Transient	HLR system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
8	Transient	VLR system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
9	Transient	Previous VLR system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
10	Transient	Controlling MSC system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
11	Transient	VMSC system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
12	Transient	EIR system failure		No	27/Oct/2010 22:59:45	MMX_ADMIN
13	Transient	Bad gateway		No	27/Oct/2010 22:59:45	MMX_ADMIN
21	Permanent	Encoding problem		Yes	27/Oct/2010 22:59:44	MMX_ADMIN
22	Permanent	Missing expected parameter		Yes	27/Oct/2010 22:59:44	MMX_ADMIN
23	Permanent	Missing mandatory parameter		Yes	27/Oct/2010 22:59:44	MMX_ADMIN
24	Permanent	Unrecognized parameter value		Yes	27/Oct/2010 22:59:44	MMX_ADMIN
25	Permanent	Unexpected parameter value		Yes	27/Oct/2010 22:59:43	MMX_ADMIN
26	Permanent	User Data size error		Yes	27/Oct/2010 22:59:43	MMX_ADMIN
27	Permanent	Invalid parameter		Yes	27/Oct/2010 22:59:43	MMX_ADMIN
28	Permanent	Error in address service centre		Yes	27/Oct/2010 22:59:43	MMX_ADMIN
29	Permanent	Invalid absolute Validity Period		Yes	27/Oct/2010 22:59:43	MMX_ADMIN
30	Permanent	Short message exceeds maximum		Yes	27/Oct/2010 22:59:43	MMX_ADMIN
31	Permanent	Unable to Unpack GSM message		Yes	27/Oct/2010 22:59:44	MMX_ADMIN

ACS release cause 1 (ID 4) was last updated by MMX_ADMIN on 27/Oct/2010 at 22:59:45 using terminal P110511SMS

Global fields

This table describes the content of each editable column.

Field	Description
ACS Release Cause	The release cause value posted to Messaging Manager by ACS. Note: The maximum allowed value is 118. Higher values are internal system defaults that cannot be changed.
Error Type	The type of error this cause number represents. Values are Permanent, Transient, Abort.
Description	What the error cause number represents.
Is Default	Indicates if the cause is the default for the Reject, Discard, or Accept actions. Note: You are able to modify only the default Reject action. The other actions are predefined.
Path Fail	Whether or not the error code causes a bypass of retries on the current path. The default for: - Transient failures is "No" (clear box). You can change this to "Yes" if required. - Permanent and Abort failures is "Yes" (ticked box). These errors will always cause a path failure. The check box will be ticked and disabled.

Adding Global Release Cause

Follow these steps to add a Global Release Cause.

Step	Action
1	From the Global tab screen, click New . Result: The New Release Cause screen opens.

See *Global fields* (on page 143) for a description of each field.

- In the **ACS Release Cause** field, enter the release cause number.

Note: Must be a unique number, less than 118.

- Enter the description for the release cause in the **Description** field.
- Select the type of error for this release cause from the **Error Type** drop down list.
- Select the **Path Failure** check box if you wish this release cause to be a path failure.
- Select the default action for this release cause from the **This is the default action for** drop down list.

Note: Select the Reject option if this release cause is to be used as the new global reject action cause. For everything else, select null option.

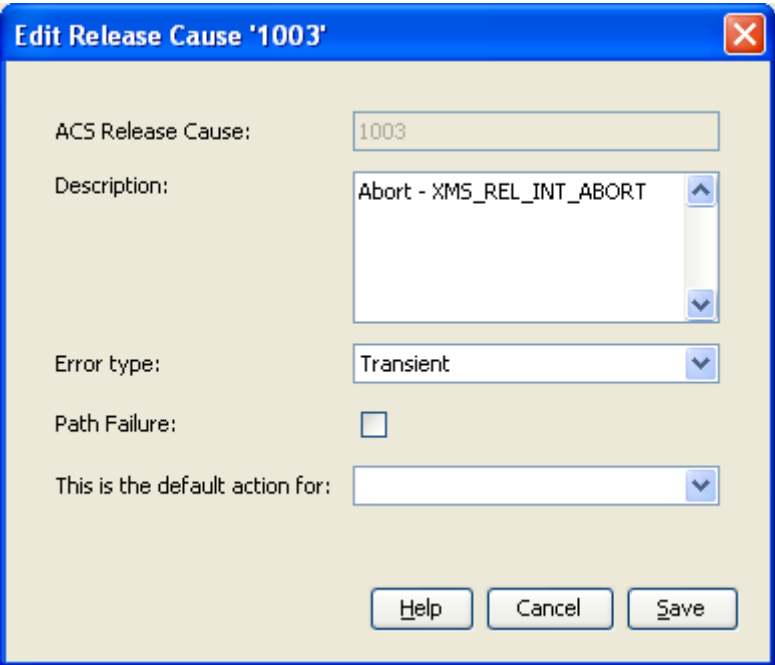
- Click **Save** to save the new release cause record in the configuration database.

Editing Global Release Cause

Follow these steps to edit a global error code.

Step	Action
1	In the table on the Global tab, select the ACS release cause to edit.
2	From the Global tab screen, click Edit . Result: The Edit Release Cause 'Code_Number' screen opens.

Step	Action
------	--------



- 3
- Change the fields as required. See *Global fields* (on page 143) for a description of each field.
- 4
- Click **Save** to save the release cause record in the configuration database.

Deleting Global Release Cause

Follow these steps to delete a Global Release Cause.

Step	Action
1	In the table on the Global tab, select the ACS release cause to delete.
2	Click Delete . Result: The Delete Release Cause 'Cause_Number' screen opens.
3	Click Delete to delete the record from the configuration database. Note: To delete this code, it must have already been removed from the protocols.

SMPP

Introduction

The **SMPP** tab defines, for this protocol, the:

- Error codes returned to the caller for each ACS release cause
- ACS release cause for each error code

SMPP tab

Here is an example SMPP tab.

SU - Action and Error Codes

Buttons: New..., Edit..., Delete..., Refresh, Close, Help

SMPP

If it cannot be determined by the rules below, SMPP Command Status is derived from the type of error in

Transient failure: ESME_RX_T_APPN (0x64)

Permanent failure: ESME_RX_P_APPN (0x65)

Abort: ESME_RSYSERR (0x0C)

Release Cause Mappings: New..., Edit..., Delete...

ACS Release Cause	Error Type	SMPP Command S...	Last Updated	By
11	Permanent	11	11/Mar/2009 00:45...	MMX_ADMIN
12	Transient	69	11/Mar/2009 00:45...	MMX_ADMIN
51	Permanent	51	11/Mar/2009 00:45...	MMX_ADMIN
52	Abort	52	11/Mar/2009 00:45...	MMX_ADMIN
53	Transient	53	11/Mar/2009 00:45...	MMY_ADMIN

Error Mappings: New..., Edit..., Delete...

SMPP Command S...	ACS Release Cause	Error Type	Last Updated	By
11	11	Permanent	11/Mar/2009 00:45...	MMX_ADMIN
45	12	Transient	11/Mar/2009 00:45...	MMX_ADMIN
51	51	Permanent	11/Mar/2009 00:45...	MMX_ADMIN
52	52	Abort	11/Mar/2009 00:45...	MMX_ADMIN
53	53	Transient	11/Mar/2009 00:45...	MMY_ADMIN

Release Cause Mapping for 11 (ID 585) was last updated by MMX_ADMIN on 11/Mar/2009 at 00:45:39 usi...

SMPP fields

This table describes the content of each column.

Field	Description
SMPP Command Status	The status code to map against the ACS release cause. Note: Must be a unique release code for this protocol.
ACS Release Cause	The release cause number used by Messaging Manager to pass back to ACS. Note: This is defined on the Global tab (on page 143).
Error Type	The type of error the ACS release cause number represents. Note: This is defined on the Global tab (on page 143).

EMI

Introduction

The **EMI** tab defines, for this protocol, the:

- Error codes returned to the caller for each ACS release cause
- ACS release cause for each error code

EMI tab

Here is an example **EMI** tab.

SU - Action and Error Codes

New... Edit... Delete... Refresh Close Help

EMI

If it cannot be determined by the rules below, EMI Error Code is set to 4.

Release Cause Mappings New... Edit... Delete...

Context	ACS Release ...	Error Type	EMI Error Code	Last Updated	By
General	22	Permanent	2	11/Mar/2009 00...	MMX_ADMIN
General	24	Transient	4	11/Mar/2009 00...	MMX_ADMIN
General	21	Transient	1	11/Mar/2009 00...	MMX_ADMIN

Error Mappings New... Edit... Delete...

Context	EMI Error Code	ACS Release ...	Error Type	Last Updated	By
General	4	24	Transient	11/Mar/2009 00...	MMX_ADMIN
General	1	21	Transient	11/Mar/2009 00...	MMX_ADMIN
General	2	22	Permanent	11/Mar/2009 00...	MMX_ADMIN

Release Cause Mapping for 2 (ID 588) was last updated by MMX_ADMIN on 11/Mar/2009 at 00:45:39 usin...

EMI fields

This table describes the content of each column.

Field	Description
Context	The circumstances in which this mapping will be applied.

Field	Description
EMI Error Code	The error code to map against the ACS release cause. Note: Must be a unique release code for this protocol.
ACS Release Cause	The release cause number used by Messaging Manager to pass back to ACS. Note: This is defined on the Global tab (on page 143).
Error Type	The type of error the ACS release cause number represents. Note: This is defined on the Global tab (on page 143).

MAP

Introduction

The **MAP** tab defines, for this protocol, the:

- Error codes returned to the caller for each ACS release cause
- ACS release cause for each error code

MAP tab

Here is an example **MAP** tab.

SU - Action and Error Codes

New... Edit... Delete... Refresh Close Help

MAP

If it cannot be determined by the rules below, GSM Error Code is derived from the type of error indicated

Transient failure: defaultTransientFailureErrorCode

Anything else: defaultPermanentFailureErrorCode

Release Cause Mappings New... Edit... Delete...

ACS Release ...	Error Type	GSM Error Code	CauseCode/A...	Last Updated	By
31	Transient	31		11/Mar/2009 00...	MMX_ADMIN
34	Transient	32	4	11/Mar/2009 00...	MMX_ADMIN
36	Permanent	32	6	11/Mar/2009 00...	MMX_ADMIN
39	Transient	34		11/Mar/2009 00...	MMX_ADMIN
51	Permanent	51		11/Mar/2009 00...	MMX_ADMIN

Error Mappings New... Edit... Delete...

GSM Error Code	CauseCode/A...	ACS Release ...	Error Type	Last Updated	By
6		93	Transient	11/Mar/2009 00...	MMX_ADMIN
31		31	Transient	11/Mar/2009 00...	MMX_ADMIN
32	4	34	Transient	11/Mar/2009 00...	MMX_ADMIN
32	6	36	Permanent	11/Mar/2009 00...	MMX_ADMIN
34		39	Transient	11/Mar/2009 00...	MMX_ADMIN

Release Cause Mapping for 31 (ID 590) was last updated by MMX_ADMIN on 11/Mar/2009 at 00:45:39 usi...

MAP fields

This table describes the content of each column.

Field	Description
GSM Error Code	The GSM MAP error code to map against the ACS release cause. Note: Must be a unique release code for this protocol.
CauseCode/Accept Denied Reason	The cause value for an SM Delivery Failure.
ACS Release Cause	The release cause number used by Messaging Manager to pass back to ACS. Note: This is defined on the Global tab (on page 143).
Error Type	The type of error the ACS release cause number represents.

Field	Description
	Note: This is defined on the Global tab (on page 143).

Actions available

From this tab, for a release cause mapping you can:

- *Adding release cause mapping - MAP, IS-41* (on page 155)
- *Editing release cause mapping - MAP, IS-41* (on page 157)
- *Deleting release cause mapping* (on page 158)

For an error mapping you can:

- *Adding error mapping - MAP, IS-41* (on page 160)
- *Editing error mapping - MAP, IS-41* (on page 162)
- *Deleting error mapping* (on page 163)

IS-41

Introduction

The **IS-41** tab defines, for this protocol, the:

- Error codes returned to the caller for each ACS release cause
- ACS release cause for each error code

IS-41 tab

Here is an example **IS-41** tab.

SU - Action and Error Codes

Buttons: New..., Edit..., Delete..., Refresh, Close, Help

IS-41

If it cannot be determined by the rules below, IS-41 SMS Cause Code is derived from the type of error in

Permanent failure: defaultPermanentFailureCauseCode

Anything else: defaultTransientFailureCauseCode

Release Cause Mappings

Context	ACS Release Cause	Error Type	IS-41 SMS Cause Code	Cause Value	Last Updated	By
SMS	31	Transient	33		11/Mar/2009 ...	MMX_ADMIN
SMS	41	Permanent	1		11/Mar/2009 ...	MMX_ADMIN
SMS	43	Transient	3		11/Mar/2009 ...	MMX_ADMIN
SMS	42	Abort	2		11/Mar/2009 ...	MMX_ADMIN
SMS	93	Transient	38		11/Mar/2009 ...	MMX_ADMIN

Error Mappings

Context	IS-41 SMS Cause Code	Cause Value	ACS Release Cause	Error Type	Last Updated	By
SMS	1		41	Permanent	11/Mar/2009 ...	MMX_ADMIN
SMS	3		43	Transient	11/Mar/2009 ...	MMX_ADMIN
SMS	2		42	Abort	11/Mar/2009 ...	MMX_ADMIN
SMS	38		93	Transient	11/Mar/2009 ...	MMX_ADMIN
SMS	33		31	Transient	11/Mar/2009 ...	MMX_ADMIN

Release Cause Mapping for 33 (ID 591) was last updated by MMX_ADMIN on 11/Mar/2009 at 00:45:39 usi...

IS-41 fields

This table describes the content of each editable column.

Field	Description
Context	The circumstances in which this mapping will be applied.
IS-41 SMS Cause Code	The cause code for an IS-41 error (SMDPP, or SMS Request) to map against the ACS Release Cause. Note: Must be a unique release code for this protocol.
Cause Value	<i>Not used for IS-41</i>
ACS Release Cause	The release cause number used by MM to pass back to ACS.
Error Type	The type of error this Release Cause number represents.

Actions available

From this tab, for a release cause mapping you can:

- *Adding release cause mapping - MAP, IS-41* (on page 155)
- *Editing release cause mapping - MAP, IS-41* (on page 157)
- *Deleting release cause mapping* (on page 158)

For an error mapping you can:

- *Adding error mapping - MAP, IS-41* (on page 160)
- *Editing error mapping - MAP, IS-41* (on page 162)
- *Deleting error mapping* (on page 163)

SIP

Introduction

The **SIP** tab defines, for this protocol, the:

- Error codes returned to the caller for each ACS release cause
- ACS release cause for each error code

SIP tab

Here is an example **SIP** tab.

SU - Action and Error Codes

New... Edit... Delete... Refresh Close Help

SIP

If it cannot be determined by the rules below, SIP Status is derived from the type of error indicated by the

Transient failure: Status 500

Permanent failure: Status 600

Release Cause Mappings New... Edit... Delete...

ACS Release Cause	Error Type	SIP Status	Last Updated	By
51	Permanent	404	11/Mar/2009 00:45...	MMX_ADMIN
52	Abort	603	11/Mar/2009 00:45...	MMX_ADMIN
53	Transient	503	11/Mar/2009 00:45...	MMX_ADMIN

Error Mappings New... Edit... Delete...

SIP Command Sta...	ACS Release Cause	Error Type	Last Updated	By
404	51	Permanent	11/Mar/2009 00:45...	MMX_ADMIN
503	53	Transient	11/Mar/2009 00:45...	MMX_ADMIN
603	52	Abort	11/Mar/2009 00:45...	MMX_ADMIN

Release Cause Mapping for 404 (ID 598) was last updated by MMX_ADMIN on 11/Mar/2009 at 00:45:39 u...

SIP fields

This table describes the content of each column.

Field	Description
SIP Status	The status code to map against the ACS release cause. Note: Must be a unique release code for this protocol.
SIP Command Status	The status code to map against the ACS release cause.
ACS Release Cause	The release cause number used by Messaging Manager to pass back to ACS. Note: This is defined on the Global tab (on page 143).
Error Type	The type of error the ACS release cause number represents.

Field	Description
	Note: This is defined on the Global tab (on page 143).

Release Cause Mapping

Introduction

The names of the fields, except the release cause field, on the following screens, are different, depending on the protocol selected.

Adding release cause mapping - IP

In this example the SMPP protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

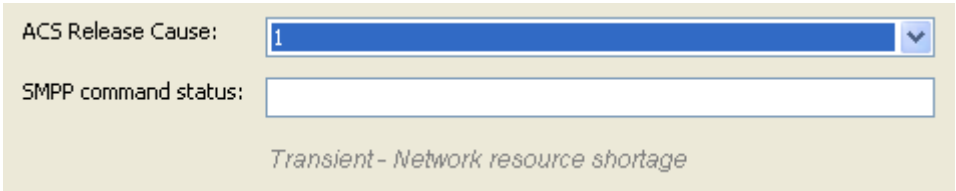
- SMPP
- EMI
- SIP

Follow these steps to add a release mapping to a protocol.

Step	Action
1	From the Action and Error Codes screen, click the required protocol tab to add the release mapping to. Result: The <i>Protocol</i> tab shows all the release cause and error mappings currently defined for the protocol. The top table on the tab displays the release cause mappings.
2	To the right of Release Cause Mappings label at the top of the release cause mappings panel, click New.... Result: The New Release Cause Mapping screen opens.

Note: The New Release Cause Mapping screen for the EMI protocol also has a Context field not shown in this screen shot. For more information, see *EMI fields* (on page 147).

- 3 If you are creating an EMI release cause mapping, enter a context into the **Context** field.
- 4 From the ACS Release Cause drop down list, select the global release cause number to map with.

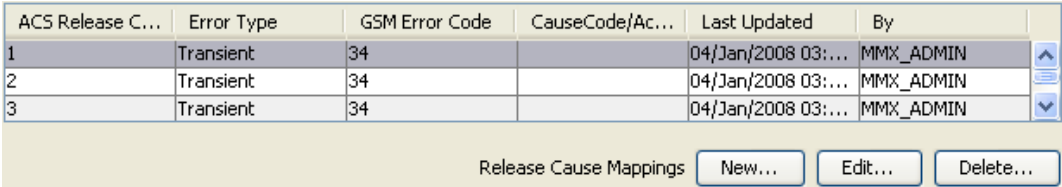
- | Step | Action | | | | | | | | | | | | |
|----------|--|---------------------------------------|------------|------------------|------|---------------------|---------------------------------------|-----|----------------|--------------------------------------|-----|------------|--------------------------------------|
| | <p>Result: The error type and description of the release cause are displayed below the fields. For more information about how to configure what text displays here, see <i>Global fields</i> (on page 143).</p>  | | | | | | | | | | | | |
| 5 | <p>Enter the protocol error code to map to in the bottom field. The name of the field varies according to the protocol:</p> <table border="1"> <thead> <tr> <th>Protocol</th> <th>Field name</th> <th>More information</th> </tr> </thead> <tbody> <tr> <td>SMPP</td> <td>SMPP command status</td> <td>See <i>SMPP fields</i> (on page 146).</td> </tr> <tr> <td>EMI</td> <td>EMI error code</td> <td>See <i>EMI fields</i> (on page 147).</td> </tr> <tr> <td>SIP</td> <td>SIP Status</td> <td>See <i>SIP fields</i> (on page 153).</td> </tr> </tbody> </table> <p>Note: Must be a unique release code for this protocol.</p> | Protocol | Field name | More information | SMPP | SMPP command status | See <i>SMPP fields</i> (on page 146). | EMI | EMI error code | See <i>EMI fields</i> (on page 147). | SIP | SIP Status | See <i>SIP fields</i> (on page 153). |
| Protocol | Field name | More information | | | | | | | | | | | |
| SMPP | SMPP command status | See <i>SMPP fields</i> (on page 146). | | | | | | | | | | | |
| EMI | EMI error code | See <i>EMI fields</i> (on page 147). | | | | | | | | | | | |
| SIP | SIP Status | See <i>SIP fields</i> (on page 153). | | | | | | | | | | | |
| 6 | Click Save to save the new release cause mapping record in the configuration database. | | | | | | | | | | | | |

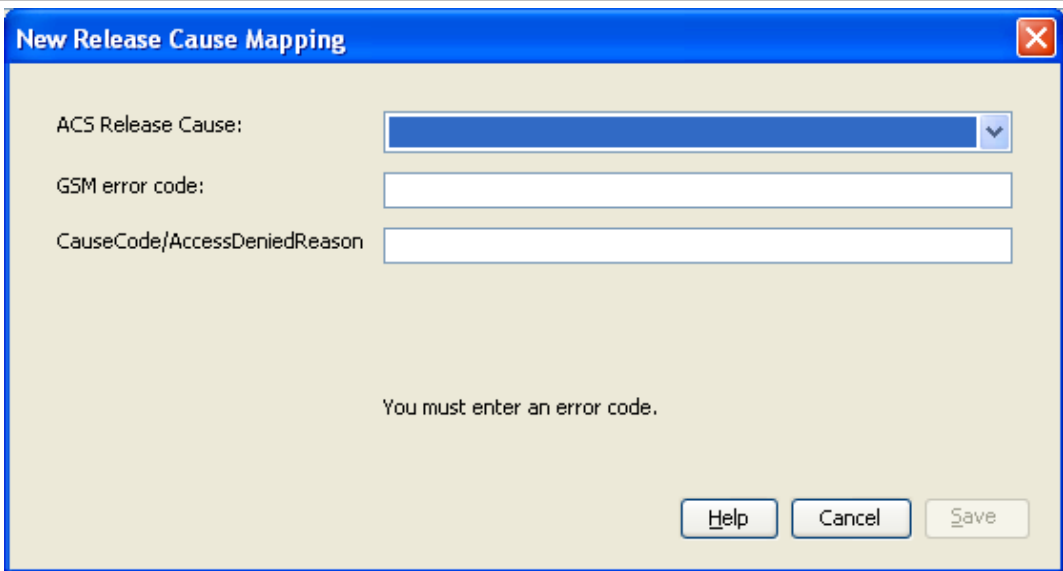
Adding release cause mapping - MAP, IS-41

In this example the MAP protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

- MAP
- IS-41

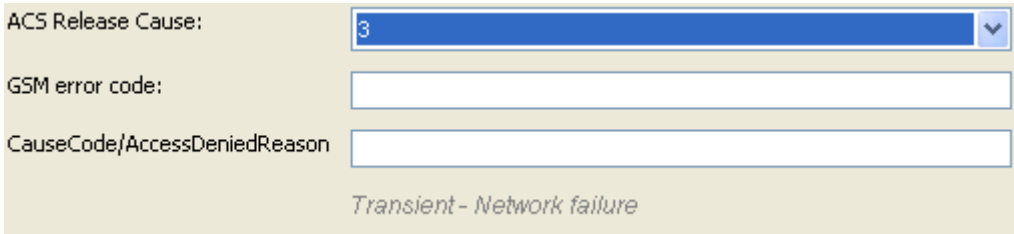
Follow these steps to add a release mapping to a protocol.

- | Step | Action |
|------|---|
| 1 | <p>From the Action and Error Codes screen, click the required protocol tab to add the release mapping to.</p> <p>Result: The <i>Protocol</i> tab shows all the release cause and error mappings currently defined for the protocol. The top table on the tab displays the release cause mappings.</p>  |
| 2 | <p>To the right of Release Cause Mappings, click New.</p> <p>Result: The New Release Cause Mapping screen opens.</p> |

Step	Action
	 The dialog box titled "New Release Cause Mapping" contains three input fields: "ACS Release Cause:" (a dropdown menu), "GSM error code:" (a text box), and "CauseCode/AccessDeniedReason" (a text box). Below the fields is a message: "You must enter an error code." At the bottom right are buttons for "Help", "Cancel", and "Save".

- 3 Select the global release cause number to map with from the **ACS Release Cause** drop down list.

Result: The error type and description of the release cause are displayed below the fields. Refer to *Global fields* (on page 143).



The dialog box now shows the "ACS Release Cause:" dropdown menu with the value "3" selected. Below the fields, the text "Transient - Network failure" is displayed.

- 4 Enter the protocol error codes to map to in the bottom fields. The names of the fields vary according to the protocol:
- MAP - see *MAP fields* (on page 149).
 - IS-41 - see *IS-41 fields* (on page 151).
- Note:** Must be a unique release code for this protocol.
- 5 Click **Save** to save the cause mapping record in the configuration database.

Editing release cause mapping - IP

In this example the EMI protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

- SMPP
- EMI
- SIP

Follow these steps to edit a release mapping for a protocol.

Step	Action
1	From the Action and Error Codes screen, click the required protocol tab to edit the release mapping for. Result: The <i>Protocol</i> tab shows all the release cause and error mappings currently defined for the protocol. The top table on the tab displays the release cause mappings.

- | Step | Action |
|------|---|
| 2 | In the Release Cause Mappings table on the tab, select the record to edit. |
| 3 | To the right of Release Cause Mappings label at the top of the release cause mappings panel, click Edit.... |
- Result:** The Edit Release Cause Mapping screen opens.

- | | |
|---|---|
| 4 | Change the text in the field, if required. The name of the field varies according to the protocol: <ul style="list-style-type: none"> • SMPP - SMPP command status. See <i>SMPP fields</i> (on page 146). • EMI - EMI error code. See <i>EMI fields</i> (on page 147). • SIP - SIP Status. See <i>SIP fields</i> (on page 153). |
| 5 | Click Save to save the cause mapping record in the configuration database. |

Editing release cause mapping - MAP, IS-41

In this example the MAP protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

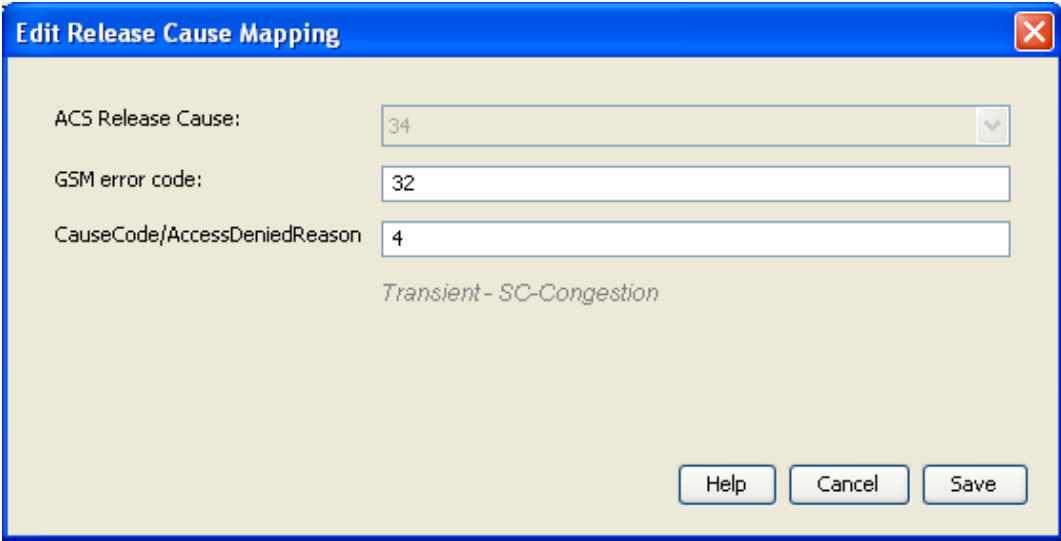
- MAP
- IS-41

Follow these steps to edit a release mapping for a protocol.

- | Step | Action |
|------|--|
| 1 | From the Action and Error Codes screen, click the required <protocol> tab to edit the release mapping for.

Result: The <i>Protocol</i> tab shows all the release cause and error mappings currently defined for the protocol. The top table on the tab displays the release cause mappings. |
-
- | ACS Release C... | Error Type | GSM Error Code | CauseCode/Ac... | Last Updated | By |
|------------------|------------|----------------|-----------------|--------------------|-----------|
| 1 | Transient | 34 | | 04/Jan/2008 03:... | MMX_ADMIN |
| 2 | Transient | 34 | | 04/Jan/2008 03:... | MMX_ADMIN |
| 3 | Transient | 34 | | 04/Jan/2008 03:... | MMX_ADMIN |
- Release Cause Mappings New... Edit... Delete...

- | | |
|---|--|
| 2 | In the Release Cause Mappings table on the tab, select the record to edit. |
|---|--|

- | Step | Action |
|------|--|
| 3 | To the right of Release Cause Mappings , click Edit .
Result: The Edit Release Cause Mapping screen opens. |
- 
- | | |
|---|--|
| 4 | Change the text in the fields, if required. The names of the fields vary according to the protocol: <ul style="list-style-type: none"> • MAP - see <i>MAP fields</i> (on page 149). • IS-41 - see <i>IS-41 fields</i> (on page 151). |
| 5 | Click Save to save the cause mapping record in the configuration database. |

Deleting release cause mapping

In this example the EMI protocol has been used. The delete release mapping procedure is identical for all protocols.

Follow these steps to delete a release mapping from a protocol.

- | Step | Action |
|------|---|
| 1 | From the Action and Error Codes screen, click the required protocol tab to delete the release cause mapping from.
Result: The <i>Protocol</i> tab shows all the release cause and error code mappings currently defined for the protocol. The top table on the tab displays the release cause mappings. |
- | Context | ACS Release C... | Error Type | EMI Error Code | Last Updated | By |
|---------|------------------|------------|----------------|--------------------|-----------|
| General | 38 | Transient | 4 | 04/Jan/2008 03:... | MMX_ADMIN |
| General | 65 | Permanent | 4 | 04/Jan/2008 03:... | MMX_ADMIN |
| General | 37 | Permanent | 3 | 04/Jan/2008 03:... | MMX_ADMIN |
| General | 64 | Transient | 3 | 04/Jan/2008 03:... | MMX_ADMIN |
| General | 36 | Permanent | 23 | 04/Jan/2008 03:... | MMX_ADMIN |
- Release Cause Mappings
- | | |
|---|---|
| 2 | In the Release Cause Mappings table on the tab, select the record to delete. |
| 3 | To the right of Release Cause Mappings , click Delete .
Result: The Delete Release Cause Mapping 'Cause_Number' screen opens. |
| 4 | Click Delete to delete the record from the configuration database. |
- Note:** This does not delete the error code, just the release mapping.

Error Mapping

Introduction

The names of the fields, except the release cause field, on the following screens, are different, depending on the protocol selected.

Adding error mapping - IP

In this example the EMI protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

- SMPP
- EMI
- SIP

Follow these steps to add an error mapping to a protocol.

Step

Action

1

From the Action and Error Codes screen, click the required protocol tab to add the release mapping to.

Result: The *Protocol* tab shows all the release cause and error mappings currently defined for the protocol. The bottom table on the tab displays the error mappings

Context	EMI Error Code	ACS Release C...	Error Type	Last Updated	By	
General	37	125	Transient	04/Jan/2008 03:...	MMX_ADMIN	⬆
General	14	78	Permanent	04/Jan/2008 03:...	MMX_ADMIN	⬆
General	36	125	Transient	04/Jan/2008 03:...	MMX_ADMIN	⬆
General	13	77	Permanent	04/Jan/2008 03:...	MMX_ADMIN	⬆
General	35	125	Transient	04/Jan/2008 03:...	MMX_ADMIN	⬆

Error Mappings

New...

Edit...

Delete...

- 2 To the right of **Error Mappings**, click **New**.
- Result:** The New Error Mapping screen opens.

New Error Mapping

EMI error code:

ACS Release Cause:

You must select a Release Cause.

Help

Cancel

Save

Step	Action												
3	Enter the protocol error code to map to in the top field. The name of the field varies according to the protocol: <table><tr><th>Protocol</th><th>Field name</th><th>More information</th></tr><tr><td>SMPP</td><td>SMPP command status</td><td>See <i>SMPP fields</i> (on page 146).</td></tr><tr><td>EMI</td><td>EMI error code</td><td>See <i>EMI fields</i> (on page 147).</td></tr><tr><td>SIP</td><td>SIP Status</td><td>See <i>SIP fields</i> (on page 153).</td></tr></table> Note: Must be a unique release code for this protocol.	Protocol	Field name	More information	SMPP	SMPP command status	See <i>SMPP fields</i> (on page 146).	EMI	EMI error code	See <i>EMI fields</i> (on page 147).	SIP	SIP Status	See <i>SIP fields</i> (on page 153).
Protocol	Field name	More information											
SMPP	SMPP command status	See <i>SMPP fields</i> (on page 146).											
EMI	EMI error code	See <i>EMI fields</i> (on page 147).											
SIP	SIP Status	See <i>SIP fields</i> (on page 153).											
4	Select the global release cause to map with from the ACS Release Cause drop down list. Result: The error type and description of the release cause are displayed below the fields. Refer to <i>Global fields</i> (on page 143). ACS Release Cause: 3 <i>Transient - Network failure</i>												
5	Click Save to save the new release mapping record in the configuration database.												

Adding error mapping - MAP, IS-41

In this example the MAP protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

- MAP
- IS-41

Follow these steps to add an error mapping to a protocol.

Step

Action

1

From the Action and Error Codes screen, click the required protocol tab to add the release mapping to.

Result: The *Protocol* tab shows all the release cause and error mappings currently defined for the protocol. The bottom table on the tab displays the error mappings.

GSM Error Code	CauseCode/Ac...	ACS Release C...	Error Type	Last Updated	By	
1		92	Permanent	04/Jan/2008 03:...	MMX_ADMIN	▲
5		91	Permanent	04/Jan/2008 03:...	MMX_ADMIN	☰
6	1	95	Transient	04/Jan/2008 03:...	MMX_ADMIN	▼

Error Mappings

New...

Edit...

Delete...

2

To the right of **Error Mappings**, click **New**.

Result: The New Error Mapping screen opens.

Step	Action
New Error Mapping GSM error code: CauseCode/AccessDeniedReason ACS Release Cause: Help Cancel Save	

- 3
- Enter the protocol error codes to map to in the top two fields. The names of the fields vary according to the protocol:
 - MAP - see *MAP fields* (on page 149).
 - IS-41 - see *IS-41 fields* (on page 151).**Note:** Must be a unique release code for this protocol.
- 4
- Select the global release cause to map to from the **ACS Release Cause** drop down list.
Result: The error type and description of the release cause are displayed below the field. Refer to *Global fields* (on page 143).

ACS Release Cause:

3

Transient - Network failure

- 5
- Click **Save** to save the error mapping record in the configuration database.

Editing error mapping - IP

In this example the EMI protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

- SMPP
- EMI
- SIP

Follow these steps to edit a release mapping for a protocol.

Step	Action
1	From the Action and Error Codes screen, click the required <protocol> tab to edit the release mapping for. Result: The <i>Protocol</i> tab shows all the release cause and error mappings currently defined for the protocol. The bottom table on the tab displays the error mappings

Step	Action
------	--------

Context	EMI Error Code	ACS Release C...	Error Type	Last Updated	By
General	37	125	Transient	04/Jan/2008 03:...	MMX_ADMIN
General	14	78	Permanent	04/Jan/2008 03:...	MMX_ADMIN
General	36	125	Transient	04/Jan/2008 03:...	MMX_ADMIN
General	13	77	Permanent	04/Jan/2008 03:...	MMX_ADMIN
General	35	125	Transient	04/Jan/2008 03:...	MMX_ADMIN

Error Mappings

2 In the Error Mappings table on the tab, select the record to edit.

3 To the right of **Error Mappings**, click **Edit**.

Result: The Edit Error Mapping screen opens.

Edit Error Mapping
✕

EMI error code:

ACS Release Cause:

22
▼

Permanent - Syntax error

Note: The name of the field varies according to the protocol:

Protocol	Field name	More information
SMPP	SMPP command status	See <i>SMPP fields</i> (on page 146).
EMI	EMI error code	See <i>EMI fields</i> (on page 147).
SIP	SIP Status	See <i>SIP fields</i> (on page 153).

4 Change the ACS Release Cause, if required.

5 Click **Save** to save the error mapping record in the configuration database.

Editing error mapping - MAP, IS-41

In this example the MAP protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

- MAP
- IS-41

Follow these steps to edit a release mapping for a protocol.

Step	Action
------	--------

1	From the Action and Error Codes screen, click the required <protocol> tab to edit the release mapping for. Result: The <i>Protocol</i> tab shows all the release cause and error mappings currently defined for the protocol. The bottom table on the tab displays the error mappings
---	---

Step

Action

GSM Error Code	CauseCode/Ac...	ACS Release C...	Error Type	Last Updated	By	
1		92	Permanent	04/Jan/2008 03:...	MMX_ADMIN	▲
5		91	Permanent	04/Jan/2008 03:...	MMX_ADMIN	≡
6	1	95	Transient	04/Jan/2008 03:...	MMX_ADMIN	▼

Error Mappings

New...

Edit...

Delete...

2 In the Error Mappings table on the tab, select the record to edit.

3 To the right of **Error Mappings**, click **Edit**.

Result: The Edit Error Mapping screen opens.

Note: The names of the top two fields vary according to the protocol:

- MAP - see *MAP fields* (on page 149).
- IS-41 - see *IS-41 fields* (on page 151).

4 Change the ACS Release Cause, if required.

5 Click **Save** to save the error mapping record in the configuration database.

Deleting error mapping

In this example the EMI protocol has been used. The delete error mapping procedure is identical for all protocols.

Follow these steps to delete an error mapping from a protocol.

Step	Action
1	From the Action and Error Codes screen, click the required protocol tab to delete the release cause mapping from. Result: The <i>Protocol</i> tab shows all the release cause and error code mappings currently defined for the protocol. The bottom table on the tab displays the error mappings

Step		Action				
Context	EMI Error Code	ACS Release C...	Error Type	Last Updated	By	
General	37	125	Transient	04/Jan/2008 03:...	MMX_ADMIN	▲
General	14	78	Permanent	04/Jan/2008 03:...	MMX_ADMIN	☰
General	36	125	Transient	04/Jan/2008 03:...	MMX_ADMIN	
General	13	77	Permanent	04/Jan/2008 03:...	MMX_ADMIN	
General	35	125	Transient	04/Jan/2008 03:...	MMX_ADMIN	▼
Error Mappings						New... Edit... Delete...

2 In the Error Mappings table on the tab, select the record to delete.

3 To the right of **Error Mappings**, click **Delete**.

Result: The Delete Error Mapping 'Cause_Number' screen opens.\

4 Click **Delete** to delete the record from the configuration database.

Note: This does not delete the error code, just the error mapping.

Messaging Manager Routing Scheme Edit Control

Overview

Introduction

This chapter explains how to manage routing scheme components.

In this chapter

This chapter contains the following topics.

Routing Scheme Edit Control 165

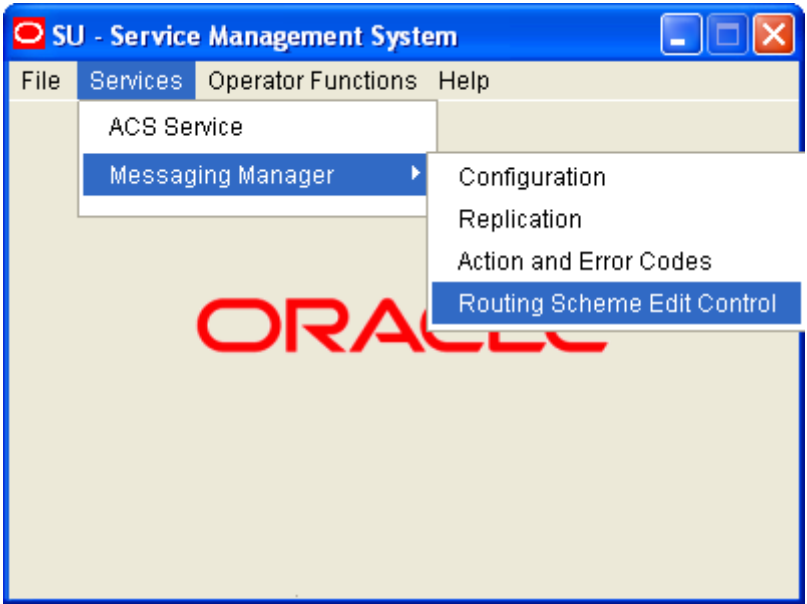
Routing Scheme Edit Control

Introduction

This tab controls which routing components can be configured using the Messaging Manager GUI.

Accessing Routing Scheme Edit Control

Follow these steps to open the Messaging Manager Routing Scheme Edit Control screen.

Step	Action
1	Select the Services menu from the SMS main screen.
	
2	Select Messaging Manager .

Step	Action
3	Select Routing Scheme Edit Control . Result: You see the Messaging Manager Routing Scheme Edit Control screen.

For more information about:

- The screen's content and how to enter configuration information, see the other topics in this chapter.
- How all the information works together to create the Messaging Manager configuration, see *Configuration Scenarios* (on page 169).
- Logging into the Service Management System screen, see *SMS User's Guide*.

Routing Scheme Edit Control tab

Here is an example **Routing Scheme Edit Control** tab.

SU - Routing Scheme Edit Control

New... Edit... Delete... Refresh Close Help

Routing Scheme Edit Control

*Use this screen to enable/disable edit access to selected parts of the Routing Scheme.
Unlicensed components can be disabled to prevent edit access and improve configuration ease of use.
This screen does not control licensing: all licenses are controlled separately by node configuration files.*

Group	Component	Used For These Functions	Enabled
Adapters	API	Define adapters for service control applications	☒
	CDMA	Define IS41/CDMA adapters for SS7 connections	☒
	EMI	Define UCP/EMI adapters for IP connections	☒
	MAP	Define MAP adapters for SS7 connections	☒
	SIP	Define adapters for SIP connections	☒
	SMPP	Define SMPP adapters for IP connections	☒
	TDMA	Define IS41/TDMA adapters for SS7 connections	☒
Gateways	MO SMS	Receive MO SMS from the network	☒
	MT SMS	Receive MT SMS from the network	☒
	VAS SMS	Send/Receive SMS from IP connections	☒
Options	SAS	Allow SMS Anti-spam Screening controls	☒
	EDR	Allow Express Delivery Routing and retries	☒
	MCP	Allow triggering to Message Control Pack	☒

Apply

Columns

This table describes the contents of each column of the **Routing Scheme Edit Control** tab.

Column	Description
Group	Identifies which component group the other columns relate to.

Column	Description
Component	Identifies the component within the group.
Used for these Functions	Describes which functions use this component.
Enabled	Indicates if the component is available for configuration (selected check box).

Editing scheme controls

Follow these steps to edit the scheme controls.

Step	Action
1	Open the Messaging Manager Routing Scheme Edit Control screen.
2	Go through the listed components and perform one of the following actions: • Select the Enabled check box to allow use of the component • Deselect the Enabled check box to bar the use of the component
3	Click Apply to save the flag information to the database. Result: SMS will perform Messaging Manager configuration replication for all the selected nodes.

Configuration Scenarios

Overview

Introduction

This chapter explains how Messaging Manager configuration is completed through the use of several scenarios.

In this chapter

This chapter contains the following topics.

Mobile to SMSC Messaging	169
Application to Mobile Messaging	179
Mobile to Application Messaging	194
Mobile to Mobile triggering to ACS	215
Instant Messaging	229
Email	235

Mobile to SMSC Messaging

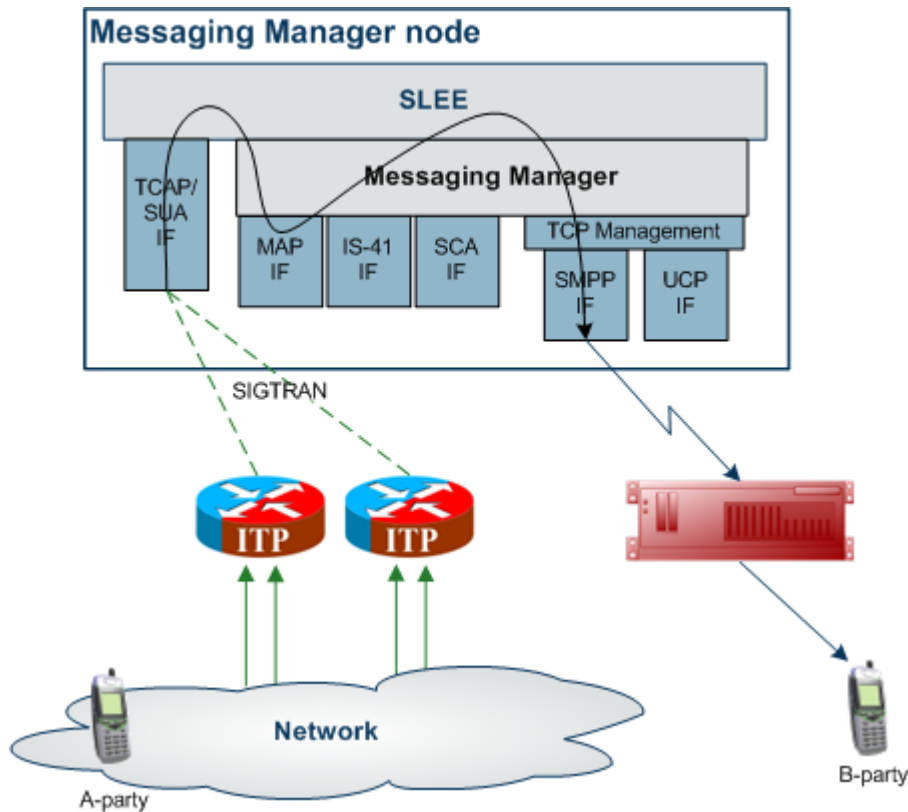
Description

The Mobile to SMSC messaging (MO SMS) service allows subscribers to send short messages from their mobile phone to the SMSC, for delivery to another mobile phone.

This example covers creating a routing scheme to route messages to an SMSC through IP. Each set of steps for this example follow in the order presented.

MO SMS diagram

Using only the Messaging Manager base module, MM can be configured to provide an MO SMS service. In this example we will receive mobile originating MAP messages and deliver to the SMSC over TCP/IP using the SMPP protocol. The following diagram shows the modules required.



Process overview

This table lists the procedures that you need to follow to complete this scenario.

Step	Action
1	Create MAP adapter (on page 170)
2	Create routing scheme (on page 171)
3	Create message center (on page 172)
4	Create SMPP adapter (on page 173)
5	Create SMSC path (on page 174)
6	Create SMSC connection (on page 175)
7	Create domain (on page 176)
8	Create submit routing rule (using MAP domain out to SMSC path)

Create MAP adapter

The adapter name in the GUI *must* match exactly the `adapterName` parameter in the `eserv.config` for the MAP protocol.

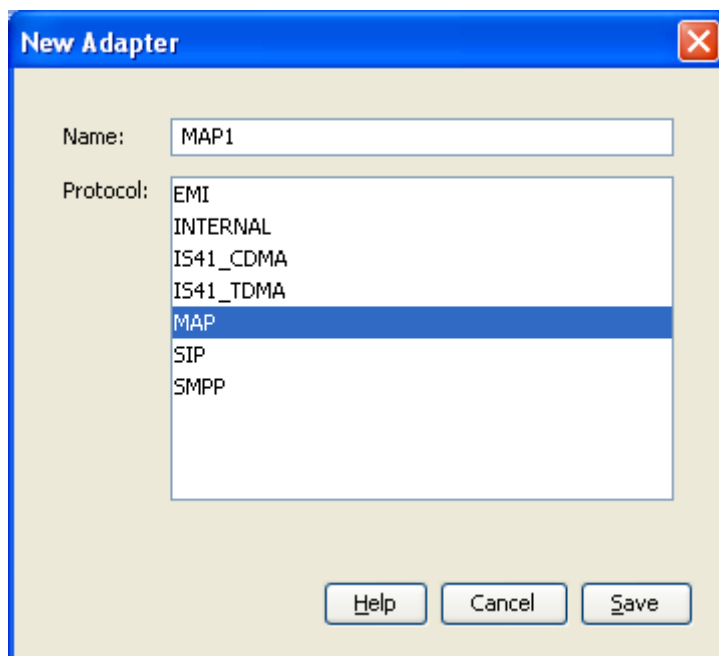
For this example we assume the `eserv.config` has the following:

```
# Adapter definitions
adapters = [
```

```
# First adapter (MAP)
{
    # adapter identifier.
    #
    adapterName = "MAP1"
    .
    .
}
```

Follow these steps to configure a MAP adapter, which will be used for receiving inbound SMSs.

Step	Action
1	Configure the MAP adapter in the MM eserv.config file. For more information, see <i>MM Technical Guide</i> .
2	On the Configuration screen, Adapters tab, click New . Result: The New Adapter screen opens.
3	In the Name field, enter MAP1 .
4	In the Protocol field, select MAP . Result: The screen should look like this:



- 5 Click **Save** to save the new adapter record in the configuration database.

Create Routing Scheme

Follow these steps to create a new routing scheme.

Step	Action
1	On the Configuration screen, Schemes tab, click New . Result: The New Scheme screen opens.
2	In the Name field, enter Mobile2SMSC Result: The Save button becomes available.
3	Ensure the Default network field is set to Default .

Step	Action
4	In the Description field, enter a description for this scheme. Example: Scheme for Mobile to SMSC messaging.
5	Ensure the Also create default domain check box is selected. Result: The screen should now look like this:

New Scheme

Name:

Default network:

Description:

☒ Also create default domain

- 6 Click **Save** to save the new scheme record in the configuration database.
Result: Messaging Manager automatically generates an MC (to/from an SMSC) and an SME (to from an MSC/HLR) path for the MAP1 adapter created in step 1.

Create Message Center

Follow these steps to create a Message Center.

Step	Action
1	On the Configuration screen, Message Centres tab, click New . Result: The New Message Centre screen opens.
2	In the Message Centre Name field, enter <code>Message Centre 1</code>
3	In the Service centre address field you would normally enter the global title of the service center to be used. For IP service centers, this is not used, but something has to be entered. Result: The Save button will appear.

New Message Centre

Message centre name:

Service centre address:

Step	Action
4	Click Save to save the new record to the database.

Create SMPP adapter

The adapter name in the GUI *must* match exactly the `adapterName` parameter in the `eserv.config` for the SMPP protocol.

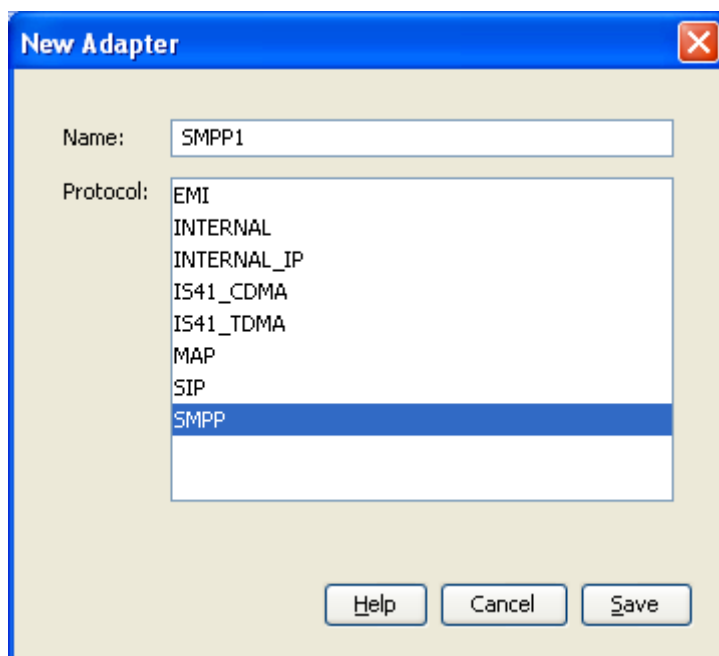
For this example we assume the `eserv.config` has the following:

```
# Adapter definitions
adapters = [

    # Third adapter (SMPP)
    {
        # adapter identifier.
        #
        adapterName = "SMPP1"
        .
        .
    }
]
```

Follow these steps to configure an SMPP adapter, which will be used for submitting SMSs to the SMSC.

Step	Action
1	On the Configuration screen, Adapters tab, click New . Result: The New Adapter screen opens.
2	In the Name field, enter <code>SMPP1</code>
3	In the Protocol field, select <code>SMPP</code> . Result: The screen should look like this.



4	Click Save to save the new adapter in the configuration database.
---	--

Create SMSC path

Configure one or more outbound paths to the SMSC over the SMPP protocol.

Follow these steps to add the required paths.

Step	Action
1	In the grid on the Configuration screen, Schemes tab, click on the <code>Mobile2SMSC</code> scheme to add the outbound paths to and click Open . Result: The Messaging Manager Scheme 'Mobile2SMSC' screen opens.
2	Select the Paths tab and click New . Result: The New Path screen opens.
3	In the Name field, type <code>Mobile2SMSC SMPP SMSC</code>
4	From the Adapter drop down list, select <code>SMPP1</code> . Result: The Save button becomes available.
5	From the Endpoint type drop down list, select <code>MC</code> . Result: The screen should now look like this:

Note: Where the message is being sent using SMPP to an SMSC, we select MC as the endpoint. Where the message is being sent to an ASP, we select SME as the endpoint.

- 6 Click **Save** to save the new Path to the configuration database.
- 7 Repeat steps 3 to 8, adding the `Mobile2SMSC SMPP ASP` path with and Endpoint of SME.

Create SMSC connection

Follow these steps to add a connection to the outbound path.

Step	Action
1	In the table on the Paths tab, select the <code>Mobile2SMSC SMPP SMSC</code> path.
2	Click Add Connection . Result: The New SMPP Connection panel opens.
3	In the Name field, enter <code>Mobile2SMSC SMSC Connection 1</code> .
4	In the Weighting field, enter <code>10</code>
5	Select the Preopen , RX and TX check boxes to allow the receiving and sending of transmissions.
6	In the Remote username field, enter <code>msgout</code>
7	In the Remote password field, enter <code>msgout</code>
8	In the Remote listen field, enter <code>205.100.97.53</code>
9	In the Remote Listen Port field, enter <code>5000</code> .

Result: The screen should now look like this.

New SMPP Connection

This routing scheme is currently deployed on 2 SCPs

Name:

Weighting:

☒ Preopen ☒ RX ☒ TX

		IP address / host name	Port
Local username:		Local listen: NIC_A	
Local password:		Local source: NIC_A	
Remote username:	msgout	Remote listen: 205.100.97.53	5000
Remote password:	msgout	Remote source:	

Connections allowed:

SMPP Options

SMPP version: 3.4	Max. concurrent transactions: 1024
System ID: eSG_MMX	Outgoing timeout: 10
System type: MMX	Idle timeout: 0
Correlation ID:	Heartbeat interval: 0

- 10 Click **Save** to save the new connection to the configuration database.

Step	Action
11	In the table on the Paths tab, select <code>Mobile2SMSC SMPP ASP</code> path and click New Connection .
12	In the Name field, enter <code>Mobile2SMSC ASP Connection 1</code> .
13	In the Weighting field, enter 10.
14	Select the RX and TX check boxes.
15	In the Local Username and Local Password fields, enter <code>lclout</code> .
16	In the Remote Username and Remote Password fields, enter <code>msgout</code> .
17	In the Remote Listen field, enter <code>205.100.97.53</code> .
18	In the Port field, enter 5000.

Result: The screen should look like this:

New SMPP Connection

This routing scheme is currently deployed on 2 SCPs

Name:

Weighting:

☐ Preopen ☒ RX ☒ TX

Local username: Local listen:

Local password: Local source:

Remote username: Remote listen:

Remote password: Remote source:

Connections allowed:

SMPP Options

SMPP version: Max. concurrent transactions:

System ID: Outgoing timeout:

System type: Idle timeout:

Correlation ID: Heartbeat interval:

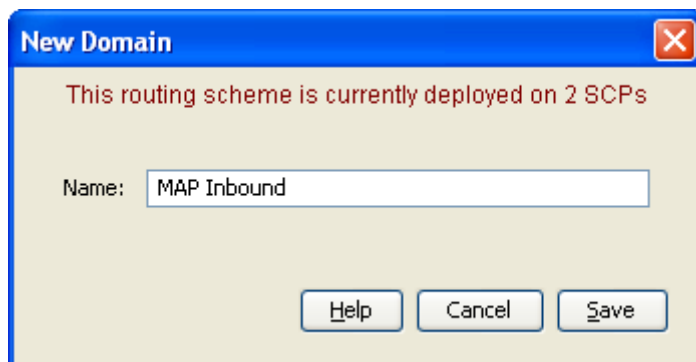
- 19 Click **Save** to save the new connection to the configuration database.

Create domain

Identify the domains that are wanted to route to the SMSC through IP.

Follow these steps to add routing address prefixes:

Step	Action
1	In the table on the Configuration screen, Schemes tab, click on the <i>Mobile2SMSC</i> routing scheme and click Open . Result: The Messaging Manager Scheme 'Mobile2SMSC' screen opens.
2	Select the Domains tab and click New .
3	In the Name field, enter <i>MAP Inbound</i> . Result: The screen should now look like this:



- | | |
|---|---|
| 4 | Click Save .
Result: The Domain will be saved and be selected in the table. |
| 5 | Select the Screening tab and select the Originating Address Screening rule. |
| 6 | Click Add . |
| 7 | In the Incoming path name prefix field, enter <i>MAP Inbound</i> . |
| 8 | In the Originating address prefix field, enter <i>033</i> . |
| 9 | Select MAP Inbound from the Allocate domain drop-down list.
Result: The screen should now look like this: |

Step	Action
------	--------

Add Originating Screening Rule

This routing scheme is currently deployed on 2 SCPs

Screening selection criteria

Incoming path name prefix:

Originating address prefix:

Screening response

☒ Allocate domain:

☐ Perform action:

☐ Release cause:

- 10 Click **Save**.
- 11 Steps 7 to 11 can be repeated to build up a list of routing address prefixes for this routing scheme.

Create Submit routing rule

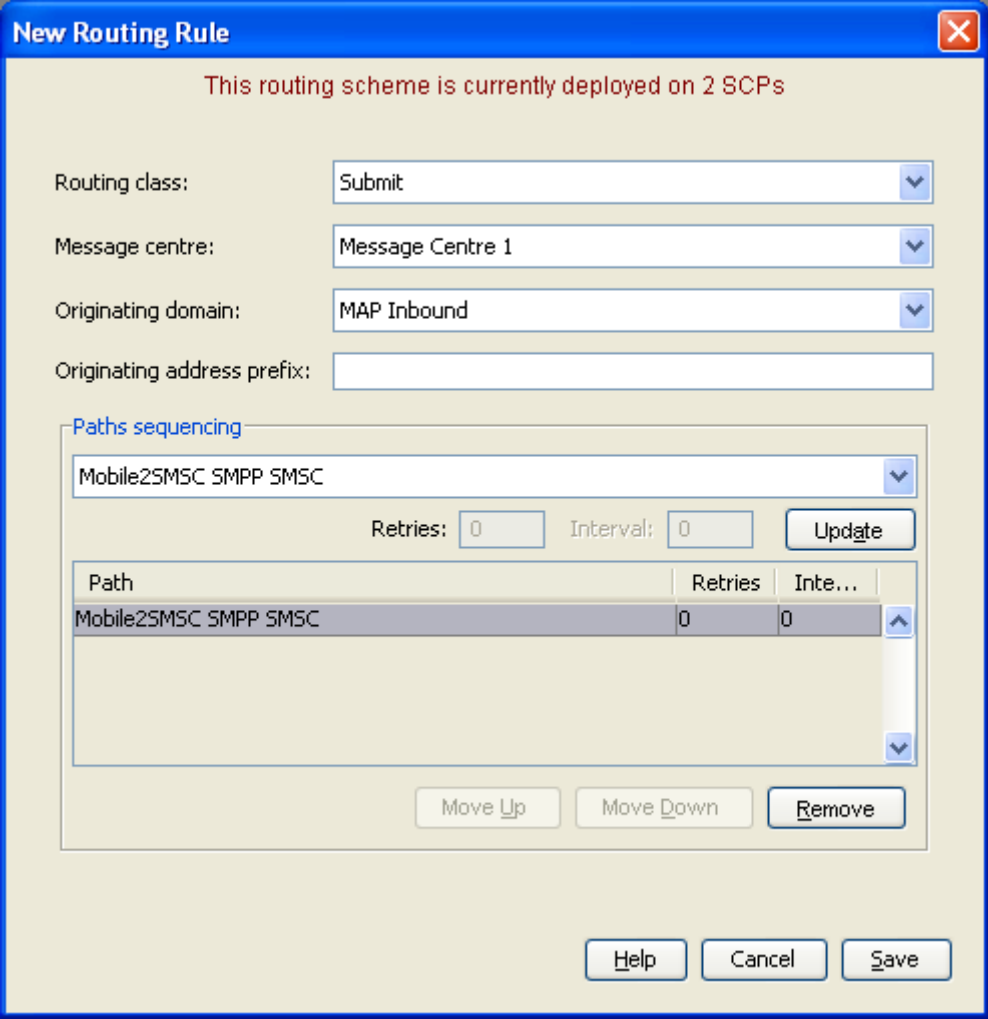
The Routing rules enable Messaging Manager to have a list of paths to attempt routing over. Messaging Manager will attempt routing using the first path, second and so on down the list. Follow these steps to establish a list of paths.

Step	Action
------	--------

- 1 In the table on the Configuration screen, **Schemes** tab, click on the `Mobile2SMSC` scheme and click **Open**.
Result: The Messaging Manager Scheme 'Mobile2SMSC' screen opens.
- 2 Select the **Routing** tab and click **New**.
- 3 In the **Routing Class** drop down list, select `Submit`.
- 4 In the **Message centre** drop down list, select `Message Centre 1`.
- 5 In the **Originating domain** drop down list, select `MAP Inbound`.
- 6 From the **Paths sequencing** drop down list, select `Mobile2SMSC SMPP SMSC`.
- 7 Click **Add**.
Result: The screen should look like this.

Step

Action



New Routing Rule [X]

This routing scheme is currently deployed on 2 SCPs

Routing class: Submit

Message centre: Message Centre 1

Originating domain: MAP Inbound

Originating address prefix:

Paths sequencing

Mobile2SMSC SMPP SMSC

Retries: 0 Interval: 0 [Update]

Path	Retries	Inte...
Mobile2SMSC SMPP SMSC	0	0

[Move Up] [Move Down] [Remove]

[Help] [Cancel] [Save]

8

Click **Save**.

Application to Mobile Messaging

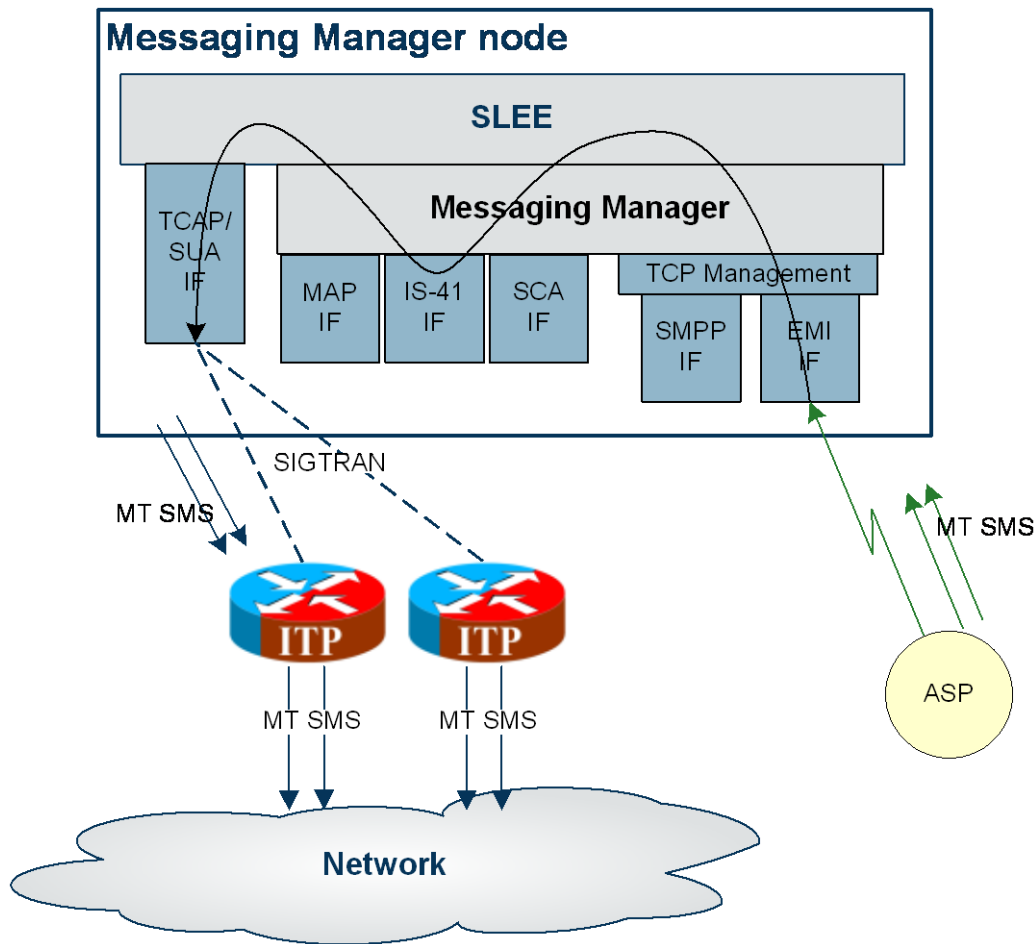
Description

Application to mobile is a simple service that provides basic delivery of SMSs to a mobile phone.

Application to Mobile diagram

Using only the Messaging Manager Base module, MM can be configured to provide an application to mobile service. In this example we will receive EMI protocol messages from ASPs and deliver them to an SMSC over SS7 using the IS-41 protocol.

The following diagram shows the modules required:



Process overview

This table lists the procedures that you need to follow to complete this scenario.

Step	Action
1	Create EMI adapter (on page 181)
2	Create routing scheme (on page 182)
3	Create EMI SMSC path (on page 182)
4	Create EMI SMSC connection (on page 183)
5	Create EMI ASP path (on page 184)
6	Create EMI ASP connection (on page 185)
7	Create address range (on page 186)
8	Create throttling rule (on page 189)
9	Configure trigger rule (on page 190)
10	Configure routing rule (on page 191)
11	Configure (on page 193) Messaging Manager node (on page 193)

Create EMI Adapter

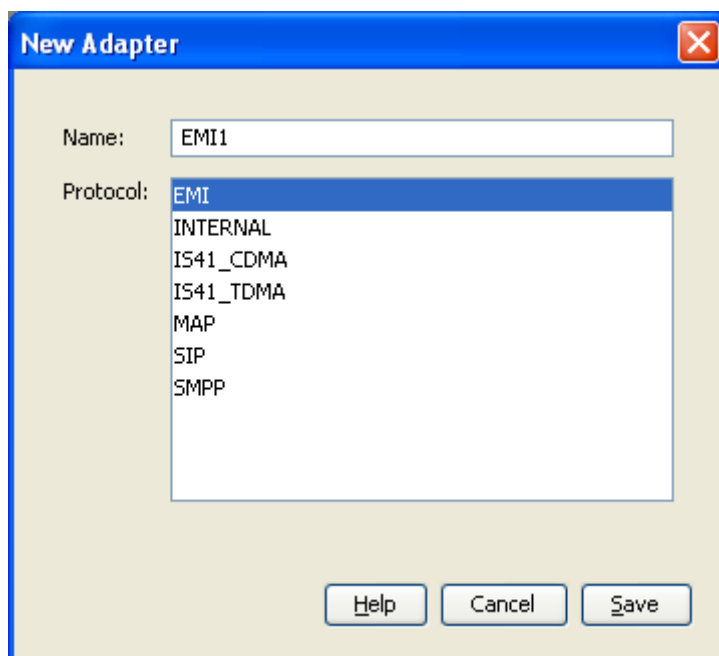
The adapter name in the GUI *must* match exactly the `adapterName` parameter in the `eserv.config` for the EMI protocol.

For this example we assume the `eserv.config` has the following:

```
# Adapter definitions
adapters = [
    # Second Adapter (EMI)
    {
        # adapter identifier.
        #
        adapterName = "EMI1"
        .
        .
    }
]
```

Follow these steps to configure an EMI adapter, which will be used for receiving inbound SMSs:

Step	Action
1	Configure the EMI Adapter in the Messaging Manager eserv.config file. For more information, see the <i>MM Technical Guide</i> .
2	On the Configuration screen, Adapters tab, click New... Result: The New Adapter screen opens.
3	In the Name field, type <code>EMI1</code> .
4	In the Protocol field, select <code>EMI</code> . Result: The screen should look like this:



- 5 Click **Save** to save the new Adapter record in the configuration database.

Create Routing Scheme

Follow these steps to create a new routing scheme.

Step	Action
1	On the Configuration screen, Schemes tab, click New . Result: The New Scheme screen opens.
2	In the Name field, type <code>App2Mobile</code> Result: The Save button becomes available.
3	In the Description field, type a description for this scheme.
4	Ensure the Also create default domain check box is ticked. Result: The screen should now look similar to this:

The screenshot shows a 'New Scheme' dialog box with a blue title bar and a red close button. Inside, there are three input fields: 'Name' with the text 'App2Mobile', 'Default network' with a dropdown menu showing 'Default', and 'Description' with a text area containing 'Scheme for Application to Mobile messaging'. Below these fields is a checked checkbox labeled 'Also create default domain'. At the bottom of the dialog are three buttons: 'Help', 'Cancel', and 'Save'.

5	Click Save to save the new Scheme record in the configuration database.
---	--

Create EMI SMSC path

Follow these steps to create a default routing path to an SMSC via EMI:

Step	Action
1	In the grid on the Schemes tab, click on the <code>App2Mobile</code> scheme.
2	Click Open .
3	Select the Paths tab and click New . Result: The New Path screen opens.
4	In the Name field, type <code>EMI SMSC</code> Note: The Name can be generic since this path can also be used by other paths as their default routing path.
5	From the Adapter drop down list, select <code>EMI Adapter</code> . Result: the Save button becomes available.
6	From the Endpoint type field, select <code>MC</code> . Result: The screen should now look similar to this:

Step	Action
------	--------

New Path

This routing scheme is currently deployed on 2 SCPs

Name:

EMI SMSC

Adapter:

EMI1

Endpoint type:

MC

Default routing path:

Message centre:

Statistics category:

Max messages/sec:

☒ This is a trusted path

Help

Cancel

Save

7 Click **Save** to save the new Path to the configuration database.

Create EMI SMSC connection

Follow these steps to create and configure an EMI SMSC connection:

Step	Action
1	In the grid on the Paths tab, click on the EMI SMSC path.
2	Click Add Connection . Result: The New EMI Connection screen displays.
3	In the Name field, type EMI SMSC Connection. Result: The Save button becomes available.
4	In the Weighting field, type 10.
5	Tick the Preopen , RX and TX check boxes to allow the receiving and sending of transmissions.
6	In the Local username and Local password fields, type local.
7	In the Port fields, type 5000.
8	The EMI Options will have default values assigned. These can be changed as required. For instance, select Allow Alternative Source Address and force a Session Timeout of 60 seconds. Result: The screen should now look similar this:

Step	Action
9	Click Save to save the new Connection to the configuration database.

New EMI Connection

This routing scheme is currently deployed on 2 SCPs

Name:

Weighting:

☒ Preopen ☒ RX ☒ TX

		IP address / host name	Port
Local username:	local	Local listen: NIC_A	5000
Local password:	local	Local source: NIC_A	5000
Remote username:		Remote listen:	
Remote password:		Remote source:	

Connections allowed:

EMI Options

Window size:	100	Alert poll time:	-1
Max window queue length:	1024	Alert address:	
Login orig. type of number:	International number	Alert protocol ID:	PC appl via abbrev. no.
Login orig. number plan ID:	E.164 address	Session timeout:	-1
Default source address:		Response timeout:	4
Allow alt. source address:	☒	Response poll time:	2
Provide VMSC in HPLMN:	☐	Default protocol ID:	0
Allow user time zones:	☐		
CDR information:			

Create EMI ASP path

Follow these steps to create and configure the inbound ASP path:

Step	Action
1	In the grid on the Schemes tab, click on the App2Mobile scheme.
2	Click Open .
3	Click the Paths tab and click New . Result: The New Path panel opens.
4	In the Name field, type <code>Stock Quotes</code>
5	From the Adapter drop down list, select <code>EMI1</code> Result: The Save button becomes available.
6	From the Endpoint type drop down list, select <code>SME</code> .

Step	Action
------	--------

- 7 From the **Default routing path** drop down list, select **EMI SMSC**.

Result: The screen should now look similar to this:

- 8 Click **Save** to save the new Path to the configuration database.

Create EMI ASP connection

Follow these steps to create and configure an EMI connection to the ASP:

Step	Action
------	--------

- 1 In the grid on the **Paths** tab, click on the **Stock Quotes** path.
- 2 Click **Add Connection** to add a Connection to the selected path.
Result: The New EMI Connection screen displays.
- 3 In the **Name** field, type **Stock Quote 1**.
Result: The Save button becomes available.
- 4 In the **Weighting** field, type **10**.
- 5 Select the **RX** and **TX** check boxes to allow the receiving and sending of transmissions.
- 6 In the **Local username** and **Local password** fields, type **stock**.
- 7 In the **Local listen port** field, type **5000**.
In the **Local source port** field, type **1512**

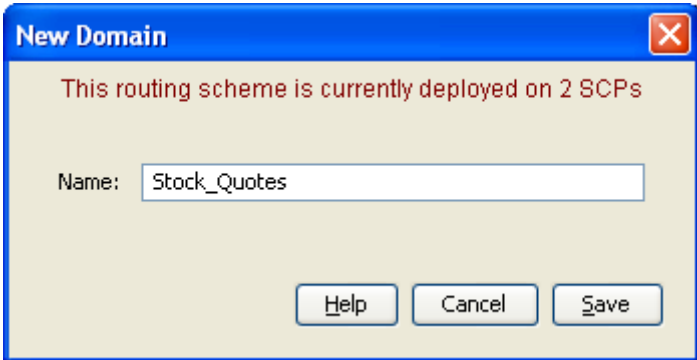
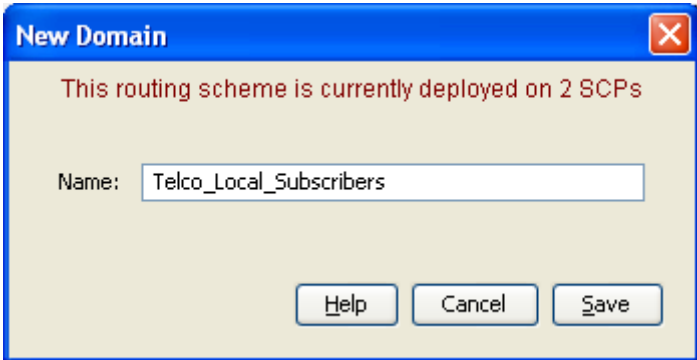
Step	Action
8	The EMI Options will have default values assigned. These can be changed as required. For instance, select Allow alt. source address and force a Session timeout of 60 seconds. Result: The screen should now look similar this:

- 9 Click **Save** to save the new Connection to the configuration database.

Create address range

Identify the domains that will be used to route from the ASP (short code 123) to a mobile phone. Follow these steps to add new domains:

Step	Action
1	On the Schemes tab, select the <code>App2Mobile</code> routing scheme.
2	Click Open .
3	Select the Domains tab and click New....

Step	Action
4	In the Name field, type <code>Stock_Quotes</code>. Result: The screen should now look similar to this: 
5	Click Save. The Domain will be saved and be selected in the grid.
6	Click New...
7	In the Name field, type <code>Telco_Local_Subscribers</code>. Result: The screen should now look similar to this: 
8	Click Save. The Domain will be saved and be selected in the grid.
9	Select the Screening tab and select the Originating Address Screening rule.
10	Click Add...
11	In the Incoming path name prefix field, type <code>Stock Quotes</code>
12	In the Originating address prefix field, type <code>123</code>.
13	Select Stock_Quotes from the Allocate domain drop-down list. Result: The screen should now look like this:

Step	Action
------	--------

Add Originating Screening Rule

This routing scheme is currently deployed on 2 SCPs

Screening selection criteria

Incoming path name prefix:

Originating address prefix:

Screening response

☒ Allocate domain:

☐ Perform action:

☐ Release cause:

- 14 Click **Save**.
 - 15 Select the **Destination Address Screening** rule.
 - 16 Click **Add...**
 - 17 In the **Incoming path name prefix** field, type Stock Quotes.
 - 18 In the **Destination address prefix** field, type 056.
 - 19 Select Telco_Local_Subscribers from the **Allocate domain** drop-down list.
- Result:** The screen should now look like this:

Step	Action
------	--------

Add Destination Screening Rule

This routing scheme is currently deployed on 2 SCPs

Screening selection criteria

Incoming path name prefix: Stock Quotes

Destination address prefix: 056

Screening response

☒ Allocate domain: Telco_Local_Subscribers

☐ Perform action:

Release cause:

Help

Cancel

Save

- 20 Click **Save**.
- 21 Steps 16 to 20 can be repeated to build up a list of address prefixes for the domain.

Create Throttling Rule

Follow these steps to set the throttling values for the path. Traffic from the ASP will only be accepted if the system is running below 50% capacity:

Step	Action
------	--------

- 1 Select the **Throttling** tab and click **New**.
- 2 In the **Detection point** field, select **Submit**.
- 3 In the **Originating domain** field select **Stock_Quotes**.
- 4 In the **Throttle** field, type 50
- Result: The screen should look like this:

Step	Action
------	--------

- 5 Click **Save**.

Configure Trigger Rule

Follow these steps to configure a trigger rule:

Step	Action
------	--------

- 1 On the **Triggering** tab, click **New**.
- 2 From the **Detection point** drop down list, select `Submit`
- 3 From the **Originating Domain** drop down list, select `Stock_Quotes`.
- 4 Select the **Route** action from the **Perform action:** drop down list.
- 5 Select the **Set routing class** check box and from drop down list, select `Deliver`

Result: The screen should look like this:

Step

Action

New Trigger Rule ✖

This routing scheme is currently deployed on 2 SCPs

Trigger Selection Criteria

Detection point:

Originating Domain:

Originating Address prefix:

Trigger Processing

☒ Perform action:

Release cause:

☒ Set routing class:

☐ Trigger a call plan in ACS

☐ Use scheduled call plan if present

☐ Use this named call plan

ACS customer: ?

Call plan: ?

Please press ENTER after keying customer or call plan names.
This will cause the value entered to be retrieved and validated.
You can search in either field by entering partial names.

Note that a limit of 100 rows is returned in each list. If you cannot find the item you're looking for, please narrow your search criteria.

6

Click **Save**.

Configure routing rule

The Routing rules enable Messaging Manager to have a list of paths to attempt routing over. Messaging Manager will attempt routing using the first path, second and so on down the list.

Follow these steps to establish a list of paths:

- | Step | Action |
|------|---|
| 1 | Create <i>CDMA Adapter</i> (on page 197) as in the Mobile to Application Messaging scenario if it doesn't already exist. |
| 2 | On the Routing tab, from the Routing class drop down list, select <i>Deliver</i> . |
| 3 | Click New....
Result: The New Routing Rule screen will open. The Routing class field will be populated with <i>Deliver</i> . |
| 4 | From the Destination domain drop down list, select <i>Telco_Local_Subscribers</i> . |
| 5 | From the Originating domain drop down list, select <i>Stock_Quotes</i> . |
| 6 | From the Paths sequencing drop down list, select <i>IS41_CDMA_SME_CDMA Adapter</i> . |
| 7 | Click Add .
Results: <ul style="list-style-type: none"> The path will be added to the Paths sequencing list. The screen should now look similar to this: |

New Routing Rule

This routing scheme is currently deployed on 2 SCPs

Routing class:

Destination domain:

Destination address prefix:

Originating domain:

Originating address prefix:

Paths sequencing

Retries: Interval:

Path	Retries	Inte...
IS41_CDMA_SME_IS41_CDMA_SME_CDMA Adapter	0	0

- 8 Click **Save**.

Configure Messaging Manager node

To enable loading of a routing scheme by Messaging Manager, the scheme is associated with the node listed in the **eserv.config** file.

Follow these steps to associate the scheme just configured with the SCP01 node:

Step	Action
1	From the table on the Nodes tab, select the node, in this example, SCP01 .
2	Click Edit . Result: The Edit Node screen opens.
3	From the Scheme list, select APP2Mobile. Result: The screen will look similar to this:

Edit Node 'SCP01'

Name: SCP01

IP Address: 192.168.15.117

Redirection Port: 4377

Description: Created from Python

Scheme: (Unspecified)
a
App2Mobile
AT32_rc
Autotest312
Autotest32
Autotest321
Autotest322

NIC A: 192.168.15.117

NIC B: 192.168.15.117

Concatenation Group: 43

Help Cancel Save

- 4 Click **Save**.
- 5 Click **Close**.
Result: This example configuration is now complete.

Mobile to Application Messaging

Description

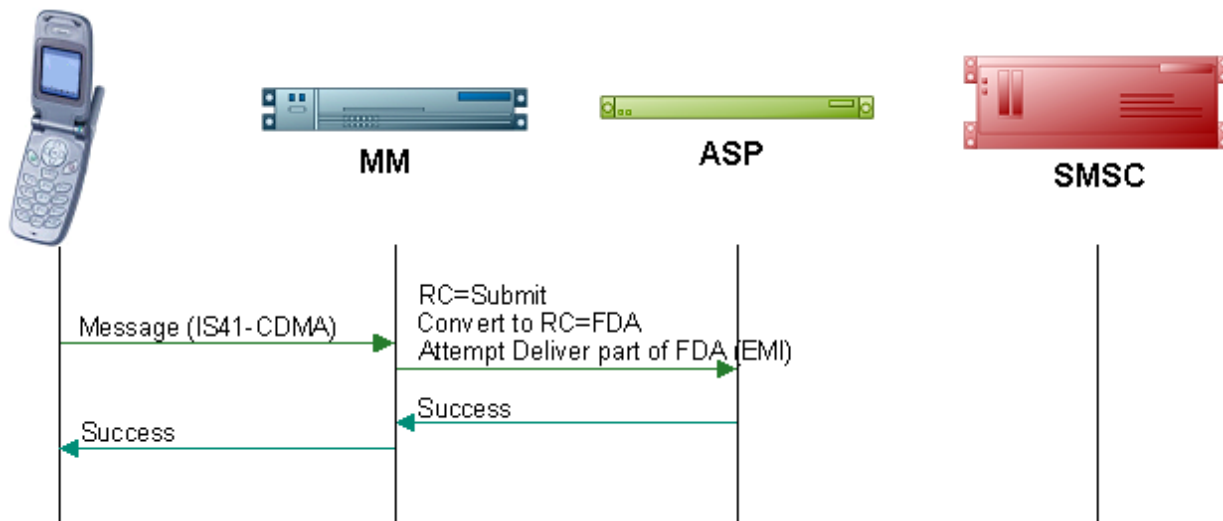
The mobile to application to service provides delivery of SMSs that originated on a mobile phone to an ASP.

Messaging Manager will attempt to deliver the SMS directly to the ASP, falling back to an SMSC if the direct delivery (FDA) fails.

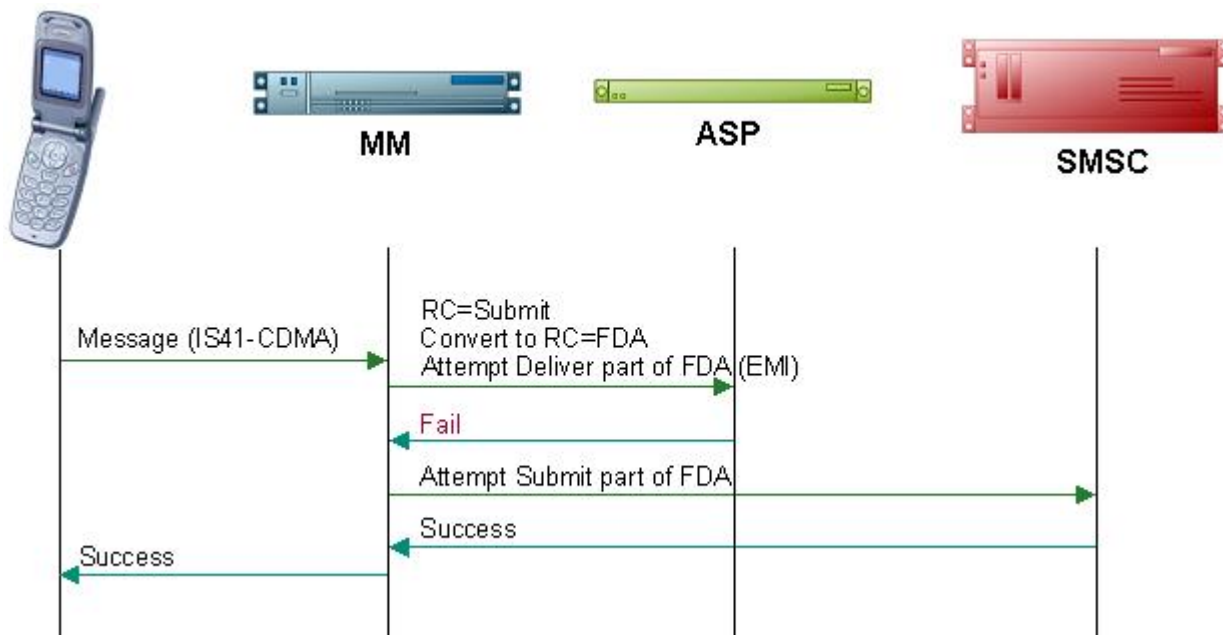
Setting the scene

This example covers the configuration required for the following flows:

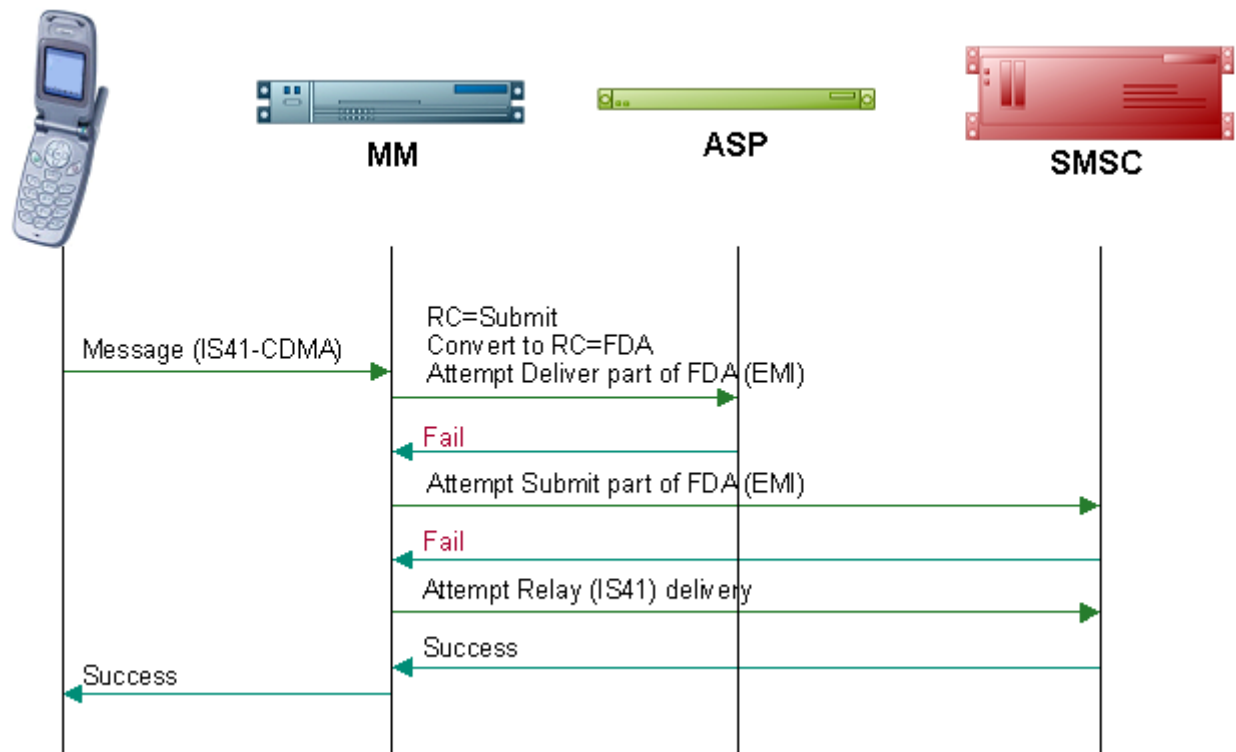
FDA deliver attempt success



FDA submit attempt success

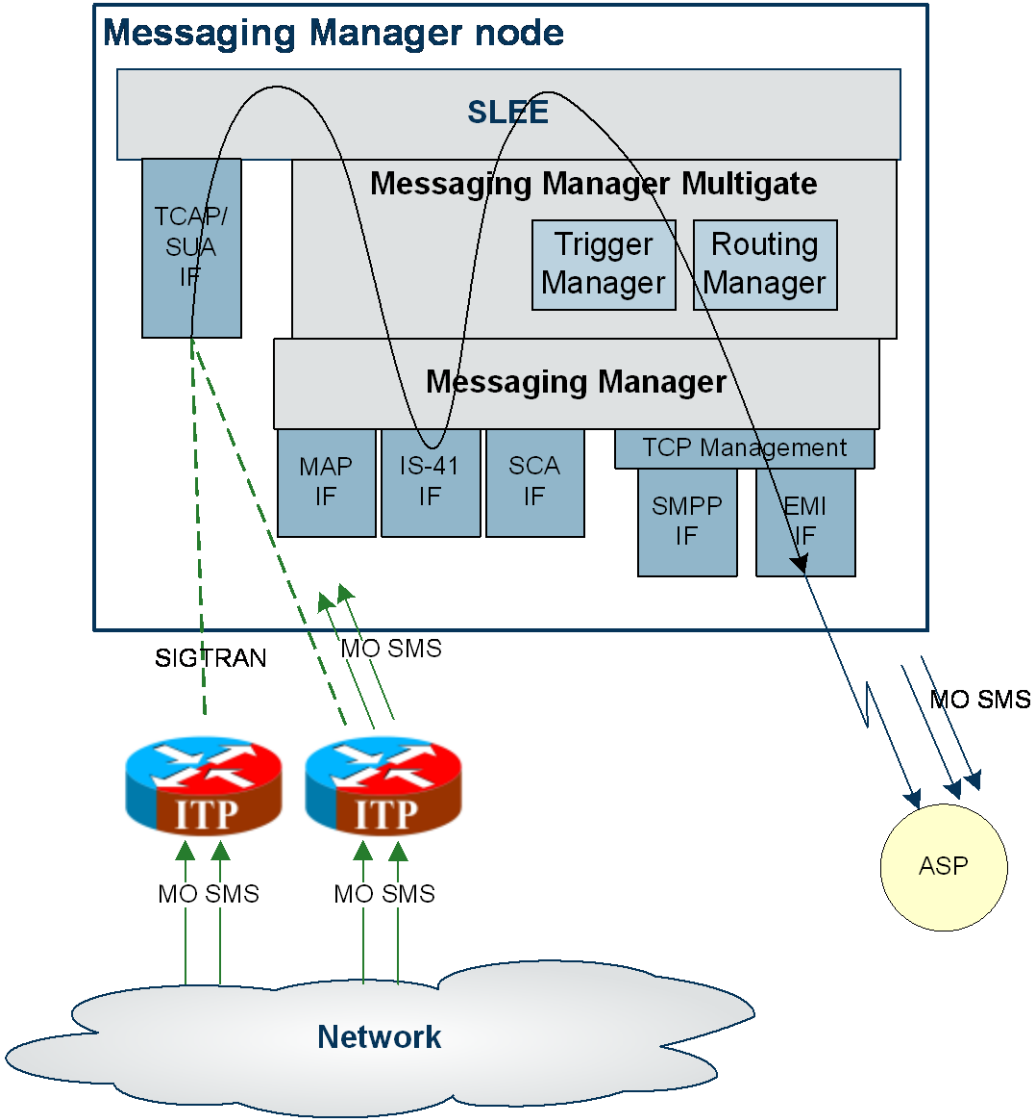


Default routing path attempt success



Mobile to Application diagram

Using the Messaging Manager Multigate and the Messaging Manager Director modules, MM can be configured to provide a Mobile to Application service. In this example we will receive mobile originating IS-41 messages and deliver them to ASPs over EMI using FDA. This diagram shows the modules required.



Process overview

This table lists the procedures that you need to follow to complete this scenario.

Step	Action
1	Create a CDMA adapter (on page 197)
2	Create routing scheme (on page 198)
3	Create SMSC path (on page 199)
4	Configure SS7 SMSC path connection (on page 200)
5	Assign default routing path to inbound CDMA path (on page 201)
6	Create outbound path (on page 202)

Step	Action
7	Configure outbound path EMI connection (on page 203)
8	Create EMI SMSC path (on page 204)
9	Configure inbound path EMI connection (on page 205)
10	Create originating domain (on page 207)
11	Configure originating domain rule (on page 208)
12	Create destination domain (on page 207)
13	Configure destination domain rule (on page 208)
14	Create throttling rule (on page 209)
15	Configure trigger rule (on page 210)
16	Configure deliver routing rule (on page 211)
17	Configure submit routing rule (on page 212)
18	Configure Messaging Manager node (on page 214)Messaging Manager

Create CDMA Adapter

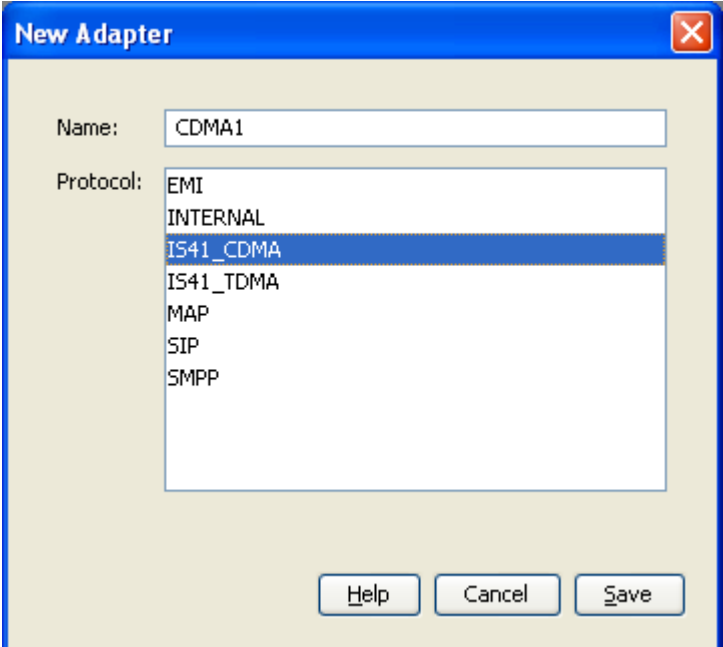
The adapter name in the GUI *must* match exactly the `adapterName` parameter in the `eserv.config` for the IS41 CDMA protocol.

For this example we assume the `eserv.config` has the following:

```
# Adapter definitions
adapters = [
    # IS-41 CDMA Adapter
    {
        # adapter identifier.
        #
        adapterName = "CDMA1"
        .
        .
    }
]
```

Follow these steps to configure a CDMA adapter, which will be used for receiving inbound SMSs:

Step	Action
1	Configure the CDMA adapter in the Messaging Manager <code>eserv.config</code> file. For more information, see <i>MM Technical Guide</i> .
2	On the Configuration screen, Adapters tab, click New.... Result: The New Adapter screen opens.
3	In the Name field, enter <code>CDMA1</code>
4	From Protocol list, select <code>IS41_CDMA</code> . Result: The screen should now look like this:

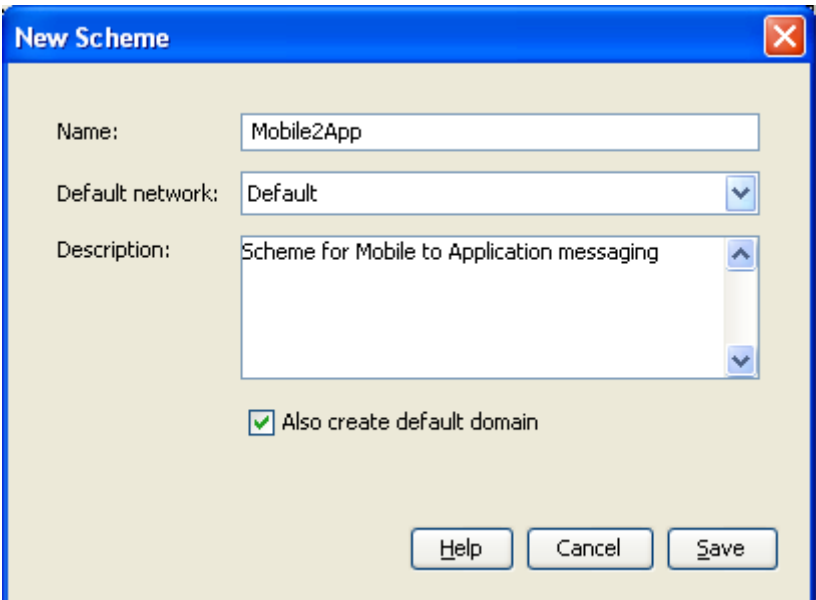
Step	Action
	

- 5 Click **Save** to save the new adapter record in the configuration database.

Create Routing Scheme

Follow these steps to create a new routing scheme.

Step	Action
1	On the Configuration screen, Schemes tab, click New . Result: The New Scheme screen opens.
2	In the Name field, type <code>Mobile2App</code> . Result: The Save button becomes available.
3	In the Description field, enter a description.
4	Ensure the Also create default domain check box is selected. Result: The screen should now look similar to this:

Step	Action
	

- 5 Click **Save** to save the new scheme record in the configuration database.

Create SMSC path

Follow these steps to create a CDMA SMSC path.

Step	Action
1	In the table on the Schemes tab, select the <code>Mobile2App</code> scheme to add the default routing path to.
2	Click Open .
3	Select the Paths tab and click New.... Result: The New Path screen opens.
4	In the Name field, enter <code>CDMA SMSC</code> Note: The Name can be generic since this path can be used many times by other schemes/ paths as their relay path.
5	From the Adapter drop down list, select <code>CDMA1</code> .
6	From the Endpoint type drop down list, select <code>MC</code> .
7	Select the This is a trusted path check box. Result: The screen should now look similar to this:

Step	Action
------	--------

- 8 Click **Save** to save the new path to the configuration database.

Configure SS7 SMSC path connection

Follow these steps to add a SS7 connection to the SMSC path.

Step	Action
------	--------

- 1 In the table on the **Paths** tab, select the `CDMA SMSC` path.
- 2 Click **Add Connection**.
Result: The New SS7 Connection screen opens.
- 3 In the **Name** field, enter `SMSC Connection1`
- 4 Select the **Outbound** check box.
- 5 In the **SS7** field, enter `021`
- 6 In the **GT** field, enter `071234567`
Note: When adding a new connection the Save button becomes available after entering either PC or GT and SS7 fields.
- 7 In the **Weight** field, type `1` (may need to deselect the **Failover** check box first).
Note: With a single connection, any non-zero value equates to a maximum loading.
Result: The screen should now look like this:

Step	Action
------	--------

New SS7 Connection

This routing scheme is currently deployed on 2 SCPs

Name:SMSC Connection1

☐ Inbound

Remote PC:(Any)

Match any PC

SCCP Calling Party point code (exact match)

Remote SSN:(Any)

Match any SSN

SCCP Calling Party subsystem number (exact match)

Remote GT:(Any)

Match any GT

SCCP Calling Party global title (prefix match)

☒ Outbound

PC:

SCCP Called Party point code. At least one of GT and PC is required.

SSN:

021

SCCP Called Party subsystem number (required)

GT:

071234567

SCCP Called Party global title

Weight:

1

 % ☐ Failover

Congestion threshold: messages

Congestion backoff: seconds

Help

Cancel

Save

8 Click **Save** to save the new connection to the database.

Assign default routing path to inbound CDMA path

Follow these steps to assign a default routing path to the predefined CDMA SME path. This will be used for all inbound MO traffic that has no specific routing rule defined.

Step	Action
------	--------

1

In the table on the **Paths** tab, select the inbound path IS41_CDMA_SME_CDMA1_Adapter.

2

Click **Edit**.
Result: The Edit Path 'path_name' screen appears.

3

From the **Default routing path** drop down list, select CDMA SMSC.
Result: The screen will look similar to this:

Chapter 9, Configuration Scenarios 201

Step	Action
------	--------

The screenshot shows a dialog box titled "Edit Path 'IS41_CDMA_SME_CDMA1_Adapter'". At the top, a red message states: "This routing scheme is currently deployed on 2 SCPs". Below this, there are several fields and a checkbox:

- Name:** IS41_CDMA_SME_CDMA1_Adapter
- Adapter:** CDMA1 (dropdown menu)
- Endpoint type:** SME (dropdown menu)
- Default routing path:** CDMA SMSC (dropdown menu)
- Message centre:** Default (dropdown menu)
- Statistics category:** (empty text field)
- ☒ This is a trusted path

At the bottom right, there are three buttons: "Help", "Cancel", and "Save".

- 4 Click **Save**.

Create outbound path

Follow these steps to create an outbound path to the EMI ASP.

Step	Action
------	--------

- 1 Select the **Paths** tab and click **New**.
Result: The New Path screen opens.
- 2 In the **Name** field, enter `Pop Idol`
- 3 From the **Adapter** drop down list, select `EMI1`
- 4 From the **Endpoint type** drop down list, select `SME`.
Result: The screen should now look like this:

Step	Action
------	--------

New Path

This routing scheme is currently deployed on 2 SCPs

Name:

Pop Idol

Adapter:

EMI1

Endpoint type:

SME

Default routing path:

Message centre:

Default

Statistics category:

Max messages/sec:

☒ This is a trusted path

Help

Cancel

Save

Note: Where the message is being sent using EMI to an SMSC, we select MC as the endpoint. Where the message is being sent to an ASP, we select SME as the endpoint.

- 5
- Click **Save** to save the new path to the configuration database.

Configure outbound path EMI connection

Follow these steps to create and configure an EMI ASP connection.

Step	Action
1	In the table on the Paths tab, select the path <code>Pop Idol</code> .
2	Click Add Connection . Result: The New EMI Connection screen opens.
3	In the Name field, enter <code>Pop Idol connection</code> . Note: When adding a new connection the Save button becomes available on entering the Name field.
4	In the Weighting field, enter <code>10</code> .
5	Select the Preopen check box to allow the connection to open on Messaging Manager startup/ reload.
6	Select the RX and TX check boxes to allow the receiving and sending of transmissions.
7	In the Local username and Local Password fields, enter <code>popidol</code>
8	In the Local listen Port field, enter <code>5000</code> In the Local source Port field, enter <code>1512</code>

Step	Action
9	The EMI options will have default values assigned. These can be changed as required. Result: The screen should now look like this:

New EMI Connection

Name:

Weighting:

☒ Preopen ☒ RX ☒ TX

Local username: Local listen: IP address / host name Port

Local password: Local source:

Remote username: Remote listen:

Remote password: Remote source:

Connections allowed:

EMI Options

Window size: Alert poll time:

Max window queue length: Alert address:

Login orig. type of number: Alert protocol ID:

Login orig. number plan ID: Session timeout:

Default source address: Response timeout:

Allow alt. source address: ☒ Response poll time:

Provide VMSC in HPLMN: ☐ Default protocol ID:

Allow user time zones: ☐

CDR information:

- 10 Click **Save** to save the new connection to the database.

Create EMI SMSC path

Follow these steps to add an outbound path to the SMSC via EMI.

Step	Action
1	Select the Paths tab and click New . Result: The New Path screen opens.
2	In the Name field, enter <code>SMSC via EMI</code> .
3	From the Adapter drop down list, select <code>EMI1</code> .
4	From the Endpoint type drop down list, select <code>MC</code> . Result: The screen should now look like this:

Step	Action
------	--------

New Path

Name:

Adapter:

Endpoint type:

Default routing path:

Message centre:

Statistics category:

Max messages/sec:

☒ This is a trusted path

- 5 Click **Save** to save the new path to the configuration database.

Configure inbound path EMI connection

Follow these steps to create and configure an EMI connection.

Step	Action
1	In the table on the Paths tab, select the path <code>SMSC via EMI</code> .
2	Click Add Connection . Result: The New EMI Connection screen opens.
3	In the Name field, enter <code>SMSC via EMI connection</code> Result: The Save button becomes available.
4	In the Weighting field, enter 10
5	Select the Preopen check box to allow the connection to open on Messaging Manager startup/ reload.
6	Select the RX and TX check boxes to allow the receiving and sending of transmissions.
7	In the Remote username and Remote password fields, enter <code>smsc</code>
8	In the Remote listen field, enter <code>200.10.20.1</code>
9	In the Remote listen Port field, enter 5000
10	The EMI options will have default values assigned. These can be changed as required. Result: The screen should look similar this:

Step	Action
New EMI Connection Name: SMSC via EMI connection Weighting: 10 ☒ Preopen ☒ RX ☒ TX Local username: Local password: Remote username: smc Remote password: smc Connections allowed: 1 Local listen: NIC_A Local source: NIC_A Remote listen: 200.10.20.1 Remote source: IP address / host name Port Window size: 100 Max window queue length: 1024 Login orig. type of number: International number Login orig. number plan ID: E.164 address Default source address: Allow alt. source address: ☒ Provide VMSC in HPLMN: ☐ Allow user time zones: ☐ CDR information: Alert poll time: -1 Alert address: Alert protocol ID: PC appl via abbrev. no. Session timeout: -1 Response timeout: 4 Response poll time: 2 Default protocol ID: 64 Help Cancel Save	

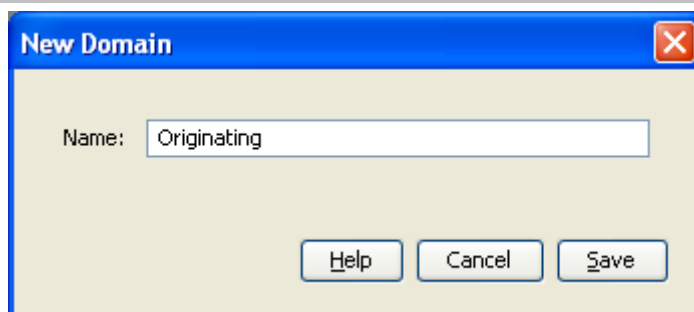
- 11 Click **Save** to save the new connection to the database.

Create originating Domain

Follow these steps to add an originating message domain.

Step	Action
1	In the table on the Schemes tab, select the <code>Mobile2App</code> routing scheme.
2	Click Open .
3	Select the Domains tab and click New . Result: The New Domain screen opens.
4	In the Name field, enter <code>Originating</code> . Result: The screen should look like this:

Step	Action
------	--------



A dialog box titled "New Domain" with a close button (X) in the top right corner. It contains a text field labeled "Name:" with the text "Originating" entered. At the bottom, there are three buttons: "Help", "Cancel", and "Save".

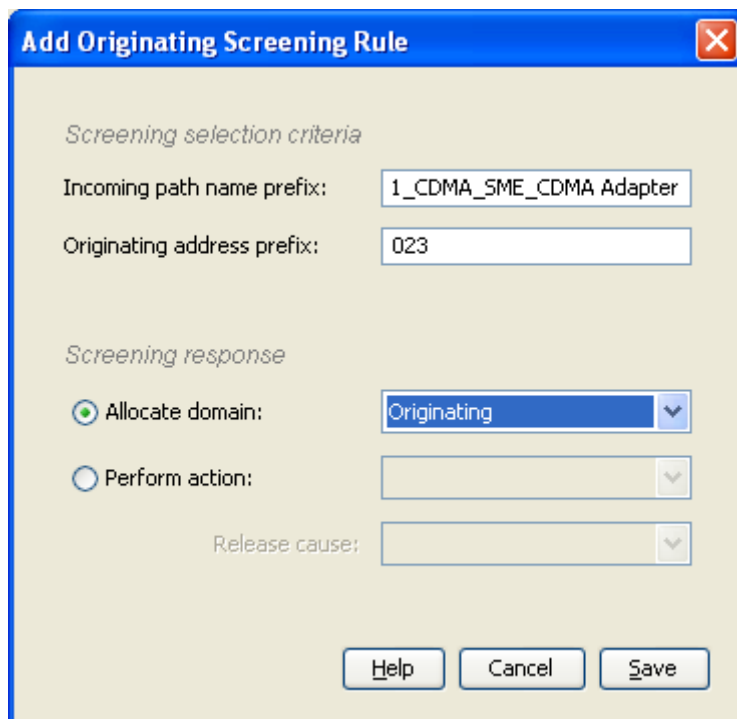
- 5 Click **Save**.

Configure originating Domain Rule

Follow these steps to add a rule to the selected address domain.

Step	Action
------	--------

- 1 On the **Screening** tab, select the **Originating Address Screening** rule and click **Add...**
Result: The Add Originating Screening Rule screen opens.
- 2 In the **Incoming path name prefix** field, enter `IS41_CDMA_SME_CDMA Adapter`
This applies the address rule to a single path - the default inbound CDMA path from a handset.
Result: The Save button becomes available.
- 3 In the **Originating address prefix** field, type `023`
- 4 From the **Allocate domain** drop-down list select `Originating`.
Result: The screen should now look like this:



A dialog box titled "Add Originating Screening Rule" with a close button (X) in the top right corner. It is divided into two sections: "Screening selection criteria" and "Screening response".

Screening selection criteria

Incoming path name prefix:

Originating address prefix:

Screening response

☒ Allocate domain:

☐ Perform action:

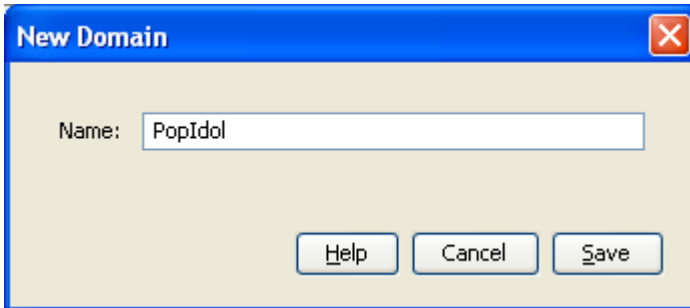
Release cause:

At the bottom, there are three buttons: "Help", "Cancel", and "Save".

- 5 Click **Save** to save the new domain rule to the configuration database.

Create destination Domain

Follow these steps to add a destination message domain.

Step	Action
1	Select the Domains tab of the Mobile2App Scheme screen, and click New . Result: The New Domain screen opens.
2	In the Name field, enter <code>PopIdol</code> Result: The screen should look like this:
	
3	Click Save .

Configure destination Domain Rule

Follow these steps to add a rule to the selected domain.

Step	Action
1	In the table on the Screening tab, select the Destination Address Screening rule and click Add.... Result: The Add Destination Screening Rule screen opens.
2	In the Incoming path name prefix field, enter <code>IS41_CDMA_MO_IN_CDMA Adapter</code> This applies the address rule to a single path - the default inbound CDMA path from a handset. Result: The Save button becomes available.
3	In the Destination Address Prefix field, enter <code>777</code>
4	Select <code>PopIdol</code> from the Allocate domain drop-down list. Result: The screen should look like this:

Step	Action
------	--------

Add Destination Screening Rule

Screening selection criteria

Incoming path name prefix: 1_CDMA_SME_CDMA Adapter

Destination address prefix: 777

Screening response

☒ Allocate domain: PopIdol

☐ Perform action:

☐ Release cause:

Help Cancel Save

- 5 Click **Save** to save the new domain rule to the configuration database.

Create Throttling Rule

Follow these steps to set the throttling values for the path.

Step	Action
------	--------

- 1 Select the **Throttling** tab and click **New**.
- 2 In the **Detection Point** field, select **Submit**.
- 3 In the **Originating domain** field, select **Originating**.
- 4 In the **Throttle** field, enter 60.

Result: The screen should look like this:

New Throttling Rule

Detection point: Submit

Destination domain:

Originating domain: Originating

Throttle at: 60 %

Help Cancel Save

Step	Action
5	Click Save .

Configure Trigger Rule

Follow these steps to configure a trigger rule.

Step	Action
1	On the Triggering tab, from the Detection point drop down list, select <code>Submit</code> .
2	Click New... Result: The New Trigger Rule screen will open. The Detection point field will be populated with <code>Submit</code> .
3	From the Originating Domain drop down list, select <code>Originating</code> .
4	Select the Route action from the Perform action: drop down list.
5	Select the Set routing class check box and from drop down list, select <code>FDA</code> . Result: The screen should look like this:

Step	Action
	New Trigger Rule <i>Trigger Selection Criteria</i> Detection point: Submit Originating Domain: Originating Originating Address prefix: <i>Trigger Processing</i> ☒ Perform action: Route Release cause: ☒ Set routing class: FDA ☐ Trigger a call plan in ACS ☐ Use scheduled call plan if present ☐ Use this named call plan ACS customer: Call plan: Please press ENTER after keying customer or call plan names. This will cause the value entered to be retrieved and validated. You can search in either field by entering partial names. Note that a limit of 100 rows is returned in each list. If you cannot find the item you're looking for, please narrow your search criteria. Help Cancel Save

6 Click **Save**.

Configure deliver Routing Rule

The Routing rules enable Messaging Manager to have a list of paths to attempt routing over. Messaging Manager will attempt delivery using the first path, second and so on down the list.

Because the FDA routing class was specified in the trigger rule above. Messaging Manager will firstly attempt routing using a Deliver routing rule, then using a Submit routing rule.

Follow these steps to establish a Deliver routing rule with a list of SME paths.

- | Step | Action |
|------|--|
| 1 | On the Routing tab, from the Routing class drop down list, select Deliver . |
| 2 | Click New....
Result: The New Routing Rule screen will open. The Routing class field will be populated with Deliver . |
| | Note: This represents the first delivery attempt for the FDA. |
| 3 | From the Destination domain drop down list, select PopIdol . |
| 4 | From the Originating domain drop down list, select Originating . |
| 5 | From the Paths sequencing drop down list, select Pop Idol and click Add .
Result: The screen should look like this: |

New Routing Rule

Routing class:

Destination domain:

Destination address prefix:

Originating domain:

Originating address prefix:

Paths sequencing

Retries: Interval:

Path	Retries	Inte...
Pop Idol	0	0

- 6 Click **Save**.

Configure submit Routing Rule

The routing rules enable Messaging Manager to have a list of paths to attempt routing over. Messaging Manager will use the paths in a Submit routing rule after the Deliver leg of FDA routing has failed.

Follow these steps to establish a Submit rule with a list of SMSC paths.

Step	Action
1	On the Routing tab, from the Routing class drop down list, select Submit .
2	Click New... Result: The New Routing Rule screen will open. The Routing class field will be populated with Submit . Note: This represents the second delivery attempt for the FDA.
3	From the Message centre drop down list, select Default .
4	From the Originating domain drop down list, select Originating .
5	From the Paths sequencing drop down list, select SMSC via EMI . Note: This represents the Submit attempt part of a failed FDA delivery.
6	Click Add .
7	From the Paths sequencing drop down list, select CDMA SMSC . Note: This represents the Default routing path attempt after a failed FDA.
8	Click Add .
9	In the Retries field, enter 3.
10	In the Interval field, enter 3. Result: The screen should look like this:

Step	Action
11	Click Save .

New Routing Rule

Routing class: Submit

Message centre: Default

Originating domain: Originating

Originating address prefix:

Paths sequencing

CDMA SMSC

Retries: 3 Interval: 3 Update

Path	Retries	Inte...
SMSC via EMI	0	0
CDMA SMSC	0	0

Move Up Move Down Remove

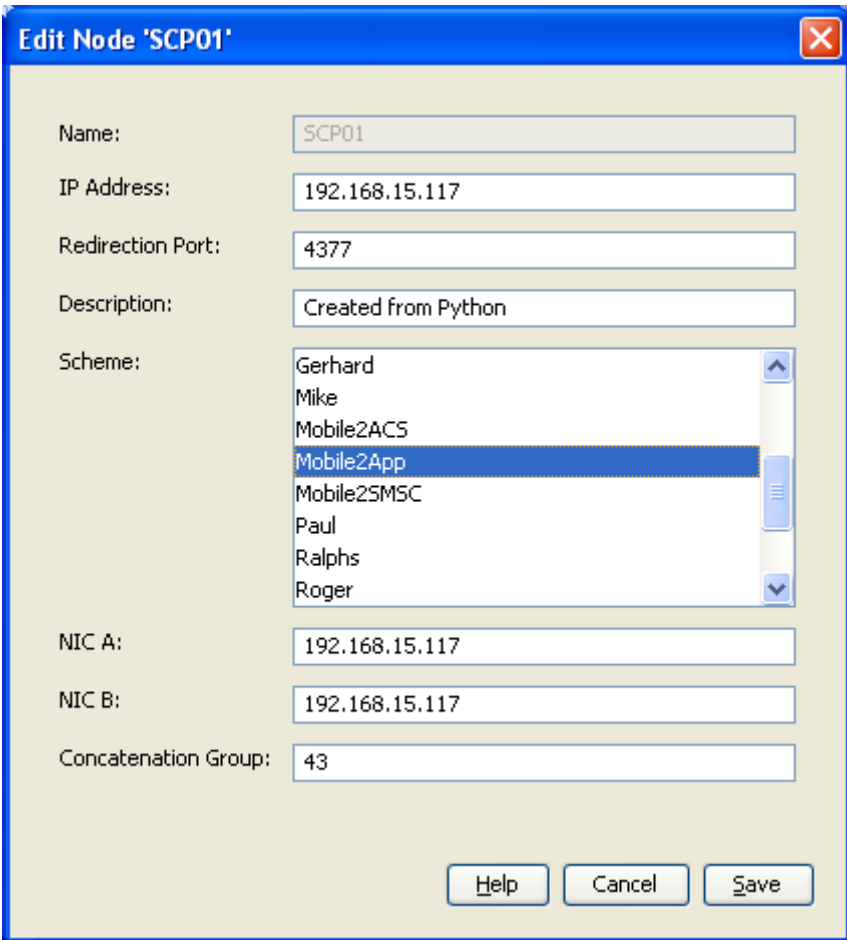
Help Cancel Save

Configure Messaging Manager node

To enable loading of a routing scheme by Messaging Manager, the scheme is associated with the node listed in the **eserv.config** file.

Follow these steps to associate the scheme just configured with the SCP01 node:

Step	Action
1	From the table on the Nodes tab, select the node, in this example, SCP01.
2	Click Edit . Result: The Edit Node screen opens.
3	From the Scheme list, select <i>Mobile2App</i> . Result: The screen will look similar to this:

Step	Action
	

4 Click **Save**.

5 Click **Close**.

Result: This example configuration is now complete.

Mobile to Mobile triggering to ACS

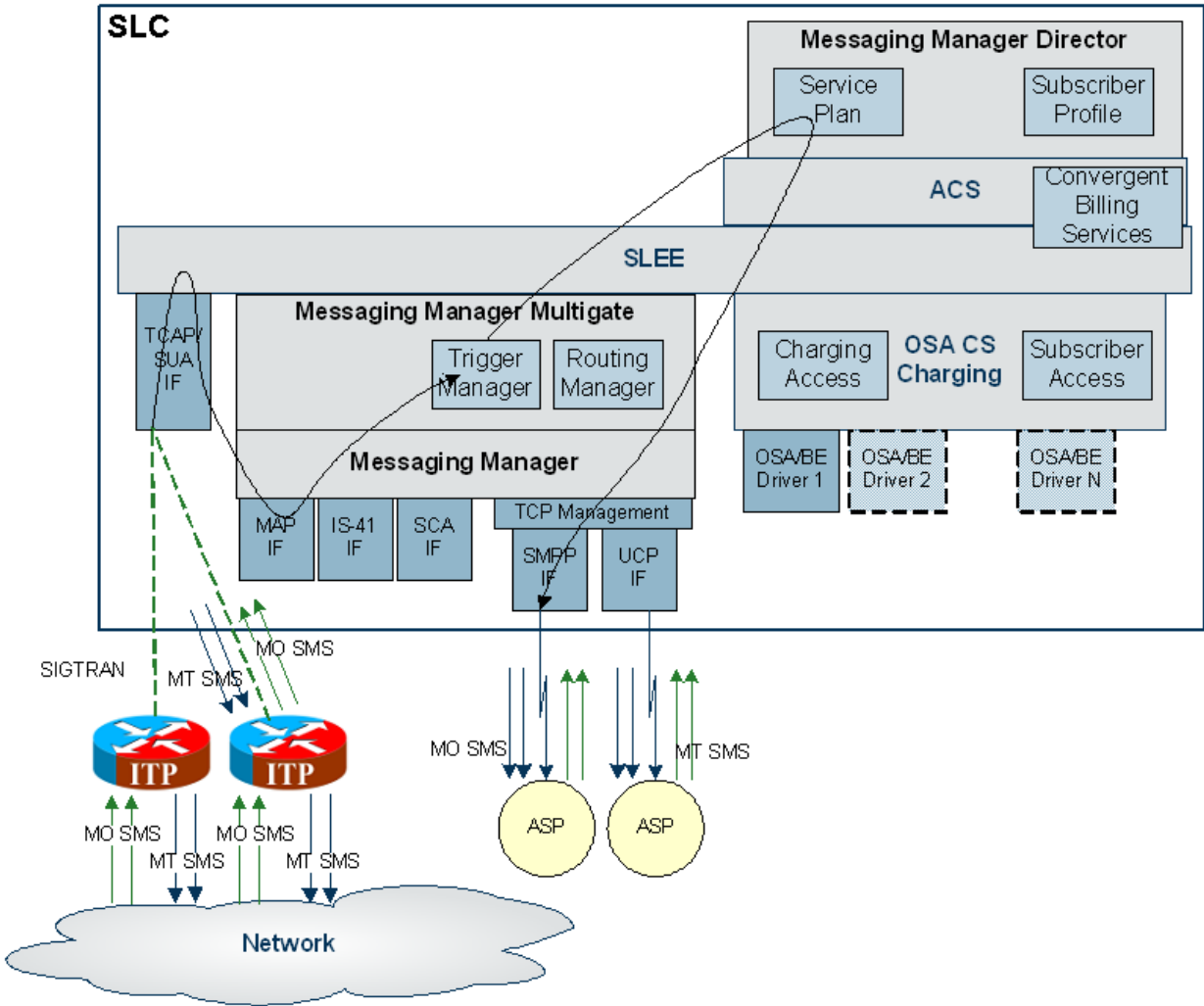
Description

The Mobile to Mobile messaging (MO SMS) service allows customers to send short messages from one mobile phone to another.

In this example messages will be triggered to an ACS control plan to route large messages to a specific SMSC.

Diagram

Using the Messaging Manager Multigate and the Messaging Manager Director modules, MM can be configured to provide a Mobile to Mobile service, triggering to ACS. In this example we will receive mobile originating MAP messages and deliver them to SMSCs over MAP having triggered them to ACS to offload all large messages to a separate SMSC. The following diagram shows the modules required:



Process overview

This table lists the procedures that you need to follow to complete this scenario.

Step	Action
1	Create MAP adapter (on page 170)
2	Create routing scheme (on page 218)
3	Create new message center (on page 219)
4	Create MC path (on page 220)
5	Create MC path SS7 connection (on page 220)
6	Create large MC path (on page 221)
7	Create large MC path connection (on page 222)
8	Create address range (on page 223)

Step	Action
9	Create control plan (on page 224)
10	Create trigger rule (on page 225)
11	Configure standard routing rule (on page 226)
12	Configure large message routing rule (on page 227)
13	Configure Messaging Manager node (on page 228)

Create MAP adapter

The adapter name in the GUI *must* match exactly the `adapterName` parameter in the `eserv.config` for the MAP protocol.

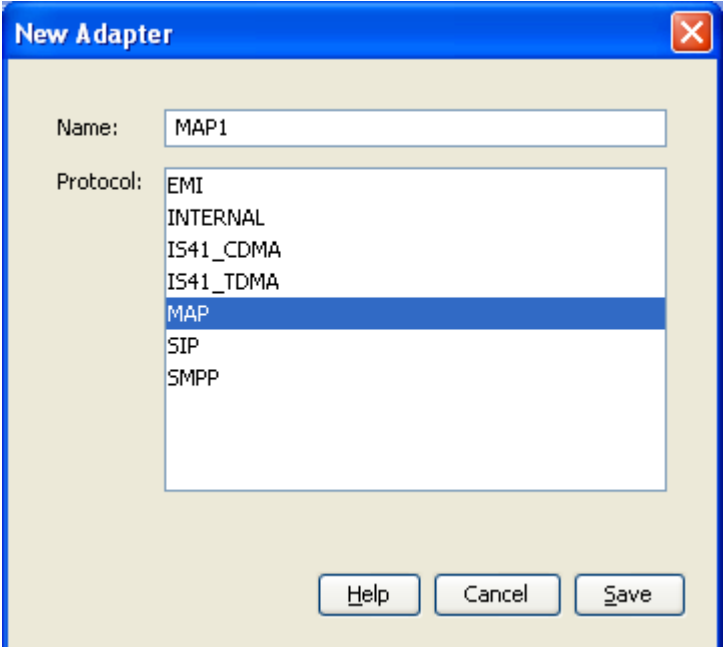
For this example we assume the `eserv.config` has the following:

```
# Adapter definitions
adapters = [

    # First adapter (MAP)
    {
        # adapter identifier.
        #
        adapterName = "MAP1"
        .
        .
    }
]
```

Follow these steps to configure a MAP adapter, which will be used for receiving inbound SMSs.

Step	Action
1	Configure the MAP adapter in the MM <code>eserv.config</code> file. For more information, see <i>MM Technical Guide</i> .
2	On the Configuration screen, Adapters tab, click New . Result: The New Adapter screen opens.
3	In the Name field, enter <code>MAP1</code> .
4	In the Protocol field, select <code>MAP</code> . Result: The screen should look like this:

Step	Action
	

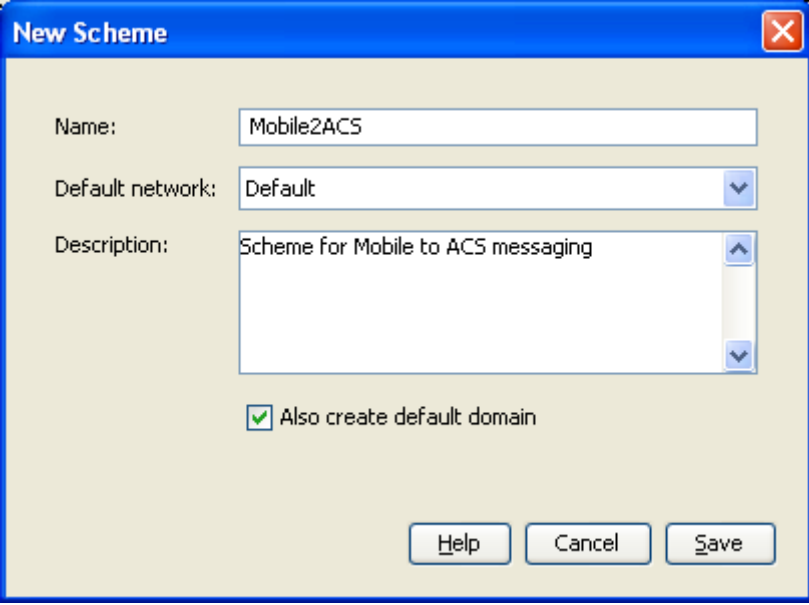
- 5 Click **Save** to save the new adapter record in the configuration database.

Create Routing Scheme

Follow these steps to create a new routing scheme:

Step	Action
1	On the Configuration screen, Schemes tab, click New... Result: The New Scheme screen opens.
2	In the Name field, enter <code>Mobile2ACS</code> . Result: The Save button becomes available.
3	In the Description field, type a description for this scheme. Example: <code>Scheme for Mobile to ACS messaging</code>
4	Ensure the Also create default domain check box is selected. Result: The screen should look like this:

Step	Action
------	--------



The 'New Scheme' dialog box has a blue title bar with a close button (X). It contains three input fields: 'Name' with the text 'Mobile2ACS', 'Default network' with a dropdown menu showing 'Default', and 'Description' with a text area containing 'Scheme for Mobile to ACS messaging'. Below these fields is a checked checkbox labeled 'Also create default domain'. At the bottom are three buttons: 'Help', 'Cancel', and 'Save'.

- 5 Click **Save** to save the new scheme record in the configuration database.
Result: All the required Messaging Manager inbound paths for the MAP protocol are automatically generated by Messaging Manager.

Create new Message Center

Follow these steps to create a separate message center for large messages.

Step	Action
------	--------

- 1 On the **Message Centres** tab, click **New....**
Result: The New Message Centre screen opens.
- 2 In the **Message centre name** field, enter `Large Message Centre`.
- 3 In the **Service centre address** field, enter `122`.
Result: The Save button will appear, and the screen should look like this:



The 'New Message Centre' dialog box has a blue title bar with a close button (X). It contains two input fields: 'Message centre name' with the text 'Large Message Centre' and 'Service centre address' with the text '122'. At the bottom are three buttons: 'Help', 'Cancel', and 'Save'.

- 4 Click **Save** to save the new message center record to the database.

Create MC path

Follow these steps to create a MAP path to the standard SMSC.

Step	Action
1	In the table on the Schemes tab, select the <code>Mobile2ACS</code> scheme to add the inbound path to.
2	Click Open .
3	Select the Paths tab and click New.... Result: The New Path screen opens.
4	In the Name field, enter <code>MAP SMSC</code> .
5	From the Adapter drop down list, select <code>CDMA1</code> . Result: The Save button becomes available.
6	From the Endpoint type drop down list, select <code>MC</code> . Result: The screen should now look similar to this:

- 7 Click **Save** to save the new path to the configuration database.

Create MC path SS7 connection

Follow these steps to add an SS7 connection to the standard SMSC path.

Step	Action
1	In the table on the Paths tab, select the <code>MAP SMSC</code> path.
2	Click Add Connection . Result: The New SS7 Connection screen opens.
3	In the Name field, enter <code>MAP SMSC connection</code> . Result: The Save button becomes available.
4	Select the Outbound check box.

Step	Action
5	In the PC field, enter 50
6	In the SSN field, enter 8
7	In the GT field, enter 6449393367
8	In the Weight field, enter 1 (may need to clear the Failover check box first).

Note: With a single connection, any non-zero value equates to a maximum loading.

Result: The screen should look similar this:

- 9 Click **Save** to save the new connection to the database.

Create large MC path

Follow these steps to create a MAP path to the SMSC for large messages.

Step	Action
1	In the table on the Schemes tab, select the Mobile2ACS scheme to add the inbound path to.
2	Click Open .
3	Select the Paths tab and click New... Result: The New Path screen opens.
4	In the Name field, enter MAP Large SMSC .
5	From the Adapter drop down list, select CDMA Adapter . Result: The Save button becomes available.
6	From the Endpoint type drop down list, select MC . Result: The screen should now look similar to this:

Step	Action
------	--------

- 7 Click **Save** to save the new path to the configuration database.

Create large MC path connection

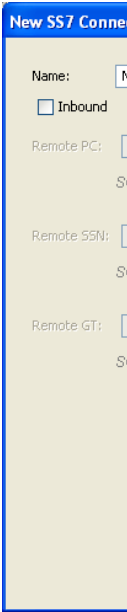
Follow these steps to add an SS7 connection to the large SMSC path.

Step	Action
------	--------

- 1 In the table on the **Paths** tab, select the `MAP Large SMSC` path.
- 2 Click **Add Connection**.
Result: The New SS7 Connection screen opens.
- 3 In the **Name** field, enter `MAP Large SMSC connection`
Result: The Save button becomes available.
- 4 Select the **Outbound** check box.
- 5 In the **PC** field, enter 51.
- 6 In the **SSN** field, enter 8.
- 7 In the **GT** field, enter 6449393368.
- 8 In the **Weight** field, enter 1 (may need to deselect the **Failover** check box first).

Note: With a single connection, any non-zero value equates to a maximum loading.

Result: The screen should look similar this:

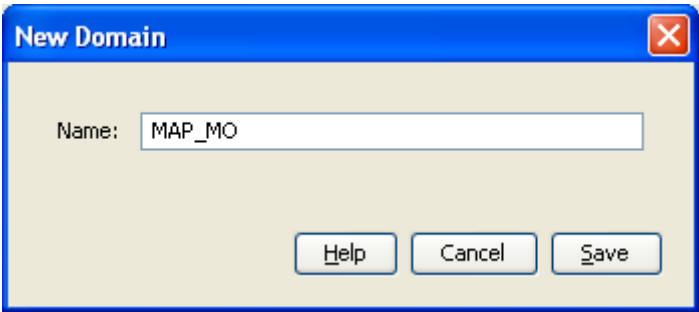
Step	Action
	

9 Click **Save** to save the new connection to the database.

Create Domain

Create a domain to identify traffic that will trigger to Messaging Manager Director.
Follow these steps to add a new domain for all MAP inbound MO traffic:

Step	Action
1	On the Schemes tab, select the <code>Mobile2ACS</code> routing scheme.
2	Click Open .
3	Select the Domains tab and click New...
4	In the Name field, enter <code>MAP_MO</code> .
Result: The screen should look like this:	

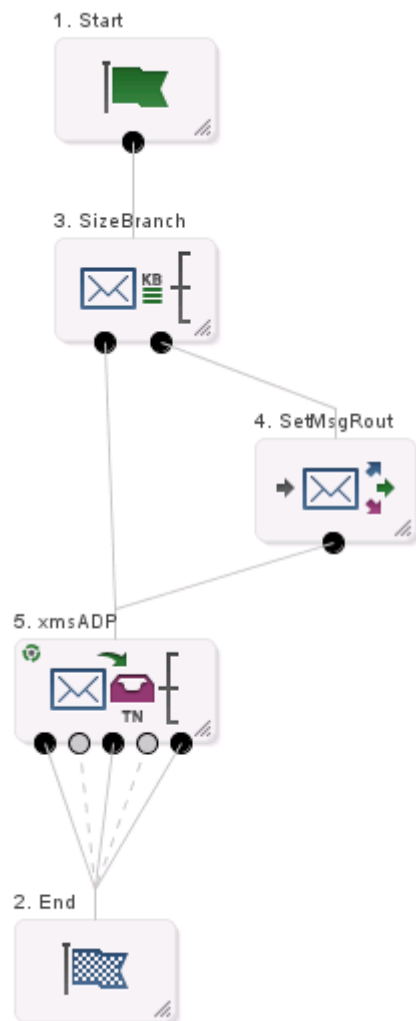


5 Click **Save**.

Create Control Plan

Follow these steps to create a Messaging Manager Director control plan.

Step	Action
1	Open the ACS Control Plan Editor. See <i>CPE User's Guide</i> for details.
2	Select the required customer.
3	Create a control plan using the following nodes: • Start • End • Content Size Branching • Set Message Routing - to set the message center to "Large Message Centre" • Attempt Delivery Pending
Result: The control plan will look similar to this:	



4 **Save** the control plan.

Create trigger rule

Follow these steps to configure a trigger rule.

Step	Action
1	On the Triggering tab, from the Detection point drop down list, select <i>Submit</i> .
2	Click New... Result: The New Trigger Rule screen will open. The Detection point field will be populated with <i>Submit</i> .
3	From the Originating Domain drop down list, select <i>SMSC Offload</i> .
4	Select the Trigger a call plan in ACS option.
5	Deselect the Use scheduled call plan if present check box.
6	Select the Use this named call plan check box.
7	Select the ACS customer and control plan named, as created and saved in <i>Create Control Plan</i> (on page 224). Result: The screen should now look like this:

Step	Action
New Trigger Rule Trigger Selection Criteria Detection point: Submit Originating Domain: SMSC Offload Originating Address prefix: Trigger Processing Perform action: Route Release cause: Set routing class: Submit Trigger a call plan in ACS Use scheduled call plan if present Use this named call plan ACS customer: Telco_Services Call plan: SMSC Offload Please press ENTER after keying customer or call plan names. This will cause the value entered to be retrieved and validated. You can search in either field by entering partial names. Note that a limit of 100 rows is returned in each list. If you cannot find the item you're looking for, please narrow your search criteria. Help Cancel Save	

8 Click **Save**.

Configure standard routing rule

Routing rules enable Messaging Manager to have a list of paths to attempt routing over. Messaging Manager will attempt routing using the first path, second and so on down the list.

Follow these steps to establish a routing rule and list of paths.

Step	Action
1	On the Routing tab, from the Routing class drop down list, select <code>Submit</code> .
2	Click New....

Step	Action
	Result: The New Routing Rule screen will open. The Routing class field will be populated with <code>Submit</code> .
3	From the Message centre drop down list, select <code>Default</code> .
4	From the Originating domain drop down list, select <code>MAP_MO</code> .
5	From the Paths sequencing drop down list, select <code>MAP_SMSC</code> and click Add .
6	In the Retries field, enter 3.
7	In the Interval field, enter 3.

Result: The screen should look like this:

New Routing Rule

Routing class:

Message centre:

Originating domain:

Originating address prefix:

Paths sequencing

Retries: Interval:

Path	Retries	Inte...
MAP_SMSC	0	0

8 Click **Save**.

Configure routing rule

If the Control Plan determined that the message was a large one, it will have set a different message center, allowing a routing rule to select a special SMSC.

Follow these steps to establish a routing rule and list of paths.

Step	Action
1	On the Routing tab, from the Routing class drop down list, select <code>Submit</code> .

Step	Action
2	Click New... Result: The New Routing Rule screen will open. The Routing class field will be populated with Submit .
3	In the Message centre drop down list, select Large Message Centre .
4	In the Originating domain drop down list, select MAP_MO .
5	From the Paths sequencing drop down list, select MAP Large SMSC and click Add .
6	In the Retries field, enter 3.
7	In the Interval field, enter 3.

Result: The screen should look like this:

- 8 Click **Save**.

Configure Messaging Manager node

To enable loading of a routing scheme by Messaging Manager, the scheme is associated with the node listed in the **eserv.config** file.

Follow these steps to associate the scheme just configured with the SCP01 node:

Step	Action
1	From the table on the Nodes tab, select the node, in this example, SCP01 . See <i>Configure Messaging Manager node</i> (on page 193).

Step	Action
2	Click Edit... Result: The Edit Node screen opens.
3	From the drop down list, select <i>Mobile2ACS</i> . Result: The screen will look similar to this:

Edit Node 'SCP01'

Name:

IP Address:

Redirection Port:

Description:

Scheme:

NIC A:

NIC B:

Concatenation Group:

4	Click Save .
5	Click Close . Result: This example configuration is now complete.

Instant Messaging

Process overview

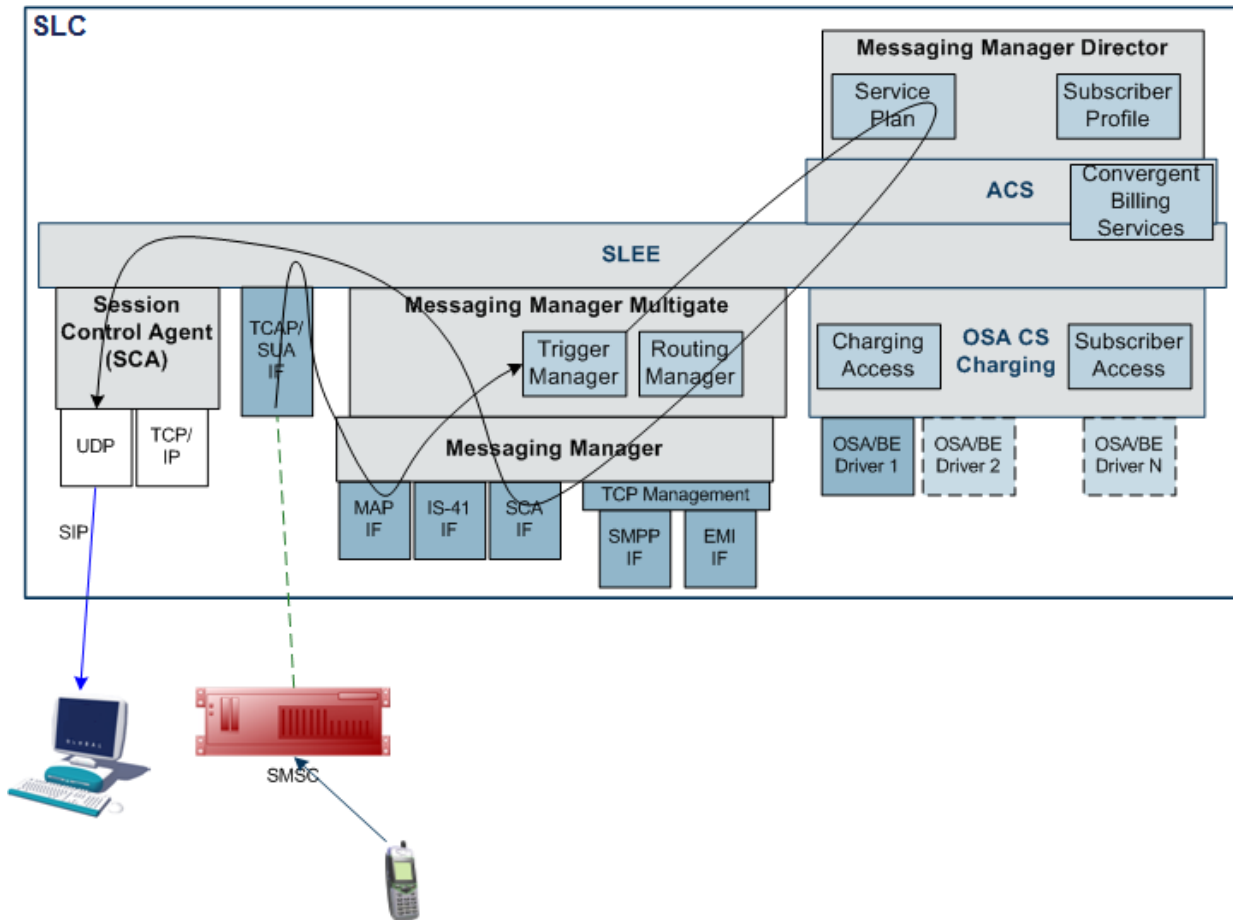
The process required is similar to the Mobile to Mobile triggering to ACS process, but the details are yet to be finalized. However, two procedures which are required for this scenario are listed in this table.

Step	Action
1	<i>Create SCA Adapter (on page 231)</i>
2	<i>Create Control Plan for SIP (on page 232)</i>

SMS forwarded to SIP

In this scenario, Tom sends a short message to Dick, who has enabled instant message forwarding using some mechanism not relevant to this design. This will forward a copy of the short messages to Dick's SIP user agent.

This is accomplished by executing a control plan that contains the Send Short Message Notification node (SSMN), which allows sending instant messages. The node specifies the destination address in URI format (for example, Dick@imdomain.com). The content and other information about the message is contained in a GenericSM event. This event is sent through the SLEE to the SCA Adapter. The SCA Adapter converts the GenericSM event to a SipSleeEvent and forwards this event to the SCA.



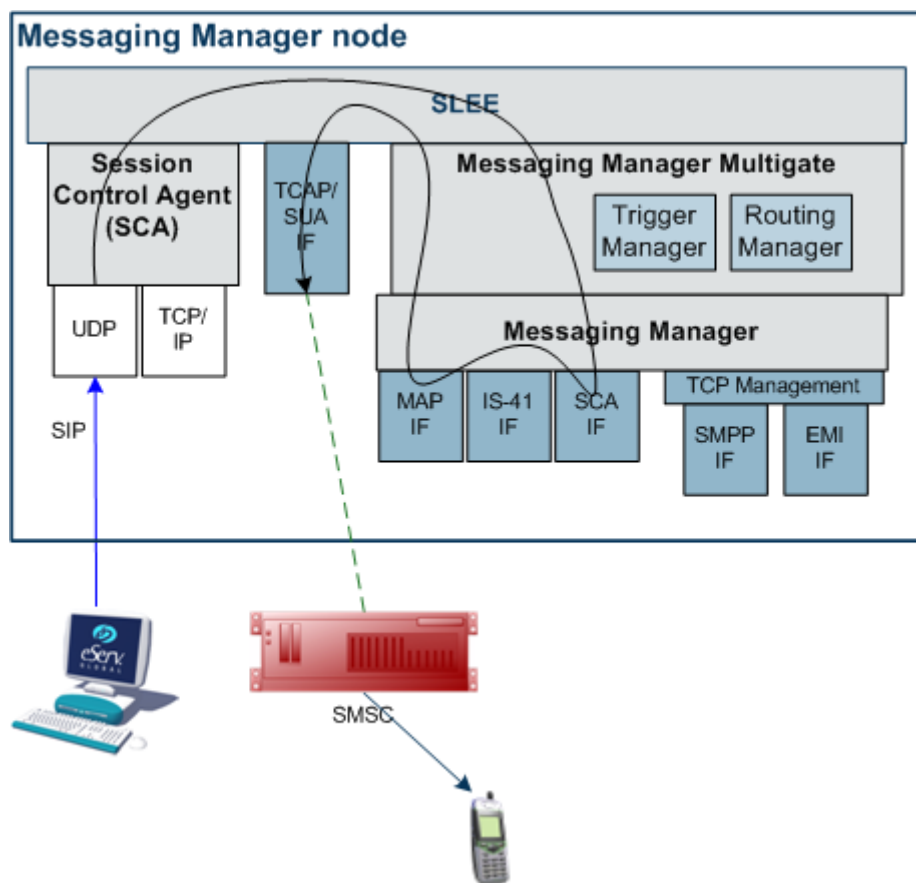
SMS to SIP

In this scenario, Tom sends a short message to a special short code (64121) that will forward the short message to Dick's instant message user agent. This scenario is similar to the scenario described above, and the path is the same as shown in that diagram, except that the destination address is specified as part of the message content (for example, "Dick@imdomain.com Watson, come here." The SSMN (or other) node extracts the destination address from the content. The short message is swallowed by MM.

SIP to SMS

In this scenario Tom sends an instant message to Dick, addressed to a handset (the E.164 telephone number - for example, 64123402). The SCA converts this message to a SipSleeEvent and passes this to the SCA Adapter. The SCA Adapter creates a GenericSM event and MM routes this to the MAP adapter. The MAP adapter sends a MAP MO-ForwardSM to the SMSC.

In this scenario, Tom uses his E.164 alias (for example, 64123570) as the originating address. This allows a reply through SMS.



Create SCA Adapter

The adapter name in the GUI *must* match exactly the `adapterName` parameter in the `eserv.config` for the SCA protocol.

For this example we assume the `eserv.config` has the following:

```
# Adapter definitions
adapters = [

    # SCA (SIP) adapter
    {
        # adapter identifier.
        #
        adapterName = "SCA1"
        .
        .
    }
]
```

Follow these steps to configure an SCA adapter, which will be used for receiving inbound SMSs.

Step	Action
1	Configure the SCA adapter in the MM <code>eserv.config</code> file. For more information, see <i>MM Technical Guide</i> .
2	On the Configuration screen, Adapters tab, click New.... Result: The New Adapter screen opens.

Step	Action
3	In the Name field, enter SCA1.
4	In the Protocol field, select SIP.

Result: The screen should look like this:

The screenshot shows a 'New Adapter' dialog box with a blue title bar and a close button (X) in the top right corner. Inside the dialog, there are two input fields: 'Name' and 'Protocol'. The 'Name' field contains the text 'SCA1'. The 'Protocol' field is a list box containing the following options: EMI, INTERNAL, IS41_CDMA, IS41_TDMA, MAP, SIP (which is highlighted with a blue background), and SMPP. At the bottom of the dialog, there are three buttons: 'Help', 'Cancel', and 'Save'.

- 5 Click **Save** to save the new adapter record in the configuration database.

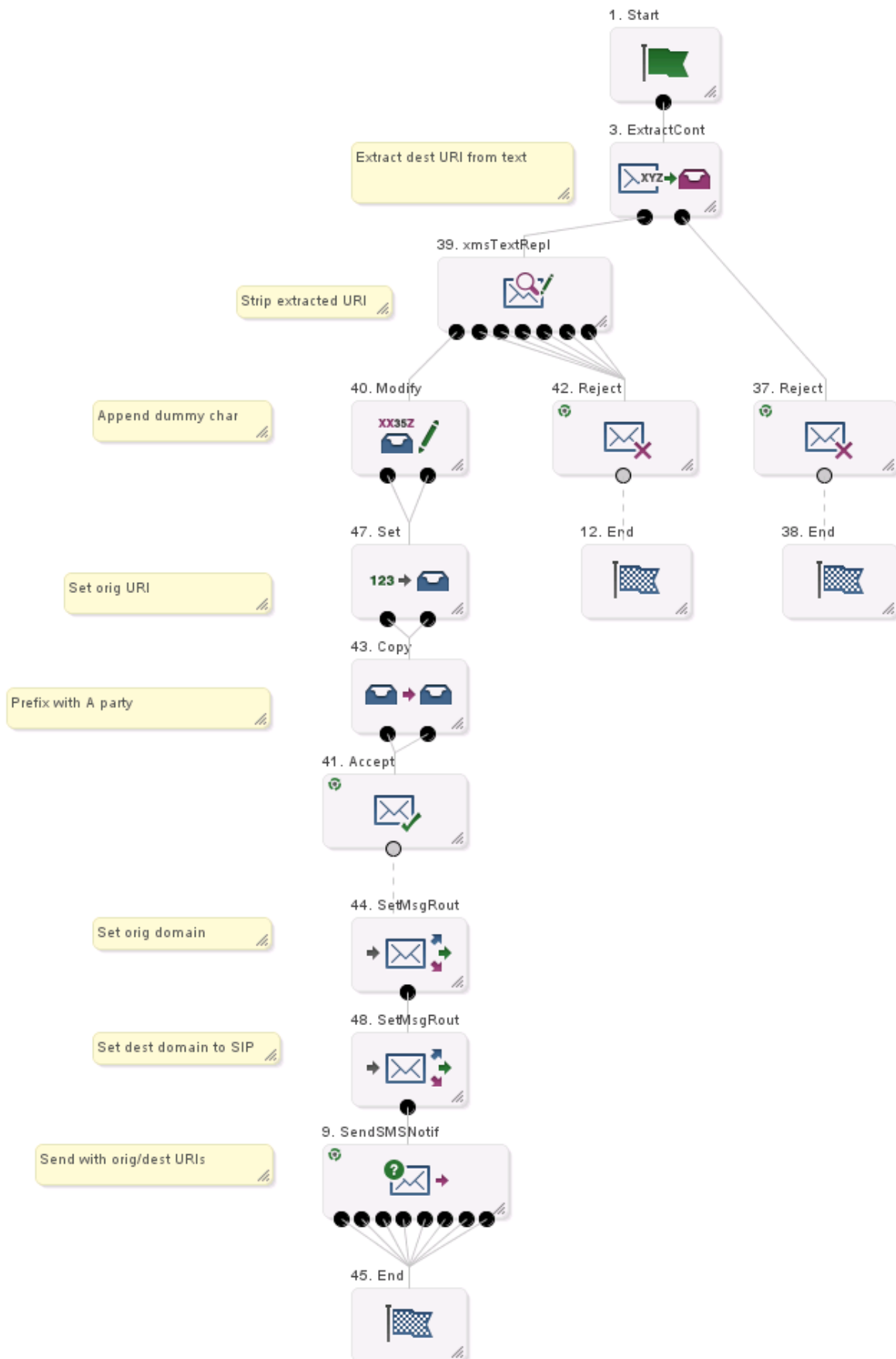
Create Control Plan for SIP

Follow these steps to create a Messaging Manager Director control plan for SIP.

Step	Action
1	Open the ACS Control Plan Editor. See <i>CPE User's Guide</i> for details.
2	Select the required customer.
3	Create a control plan using the following nodes: • Start • End • Extract Content • Configure Keyword Search and Replace • Modify • Set • Copy • Accept • Set Message Routing - to set the originating and destination domains. • Send Short Message Notification • Reject Result: The control plan will look similar to the <i>Example Control Plan for SIP</i> (on page 233)
4	Save the control plan.

Example Control Plan for SIP

Here is an example control plan for SIP.



Email

Process overview

Refer to PME Control Plan Scenarios for an explanation of how this is set up.