Oracle® Communications Network Charging and Control

Messaging Manager Help

Release 15.1
G14416-01
April 2025

ORACLE

Oracle Communications Network Charging and Control Messaging Manager Help, Release 15.1

G14416-01

Contents

1 Messaging Manager Configuration Screen

8 XMS Parameters Feature Nodes

1

Messaging Manager Configuration Screen

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

This chapter contains the following topics.

Messaging Manager Configuration Screen

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

- Schemes
- Nodes
- Networks
- SMSCs
- ASP Parameters
- ASP Groups
- ASPs

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

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.

Topics:

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.

Field	Description
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 Schemes. **Note:** Default value is **(Unspecified)**.
Interface	Interface record used by this node. 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.

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.
4. Click **Save**.

Related topic

Nodes

Editing IP addresses

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

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, IP address fields.
4. Click **Save**.

Related topic

Nodes

Removing IP addresses

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

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.

Related topic

Nodes

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*.

Related topic

Nodes

Editing nodes

Follow these steps to edit an existing node record.

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.
3. Edit the fields with the changes to make.

   For more information about the fields on this screen, see Nodes fields.

   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.

Related topic

Nodes

Deleting nodes

Nodes cannot be deleted using the configuration screens.

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

Related topic

Nodes

Schemes

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 Messaging Manager Schemes.

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.

Topics:

Configuration options

Schemes columns

Schemes buttons

Opening schemes

Copying schemes

Scheme fields

Adding schemes

Editing schemes

Deleting schemes

Configuration options

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

Function	Description	More information
Adapters	Configure protocol adapters.	Adapters
Interfaces	Configure network interfaces.	Interfaces
Paths	Configure the paths associated with adapters.	Paths
Connections	Configure connections used by paths.	Path Connections
Screening rules	Configuring screening and anti-spam rules.	Screening
Addressing rules	Configure address categorization rules.	Addressing
Throttling rules	Configure throttling rules.	Throttling
Triggering rules	Configure triggering rules.	Triggering
Routing rules	Configure outbound routing rules.	Routing

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 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
Copy...	Copies the currently selected scheme and all associated data to a new scheme. See Copying schemes.
Open...	Displays the selected scheme details for editing. See Opening schemes.

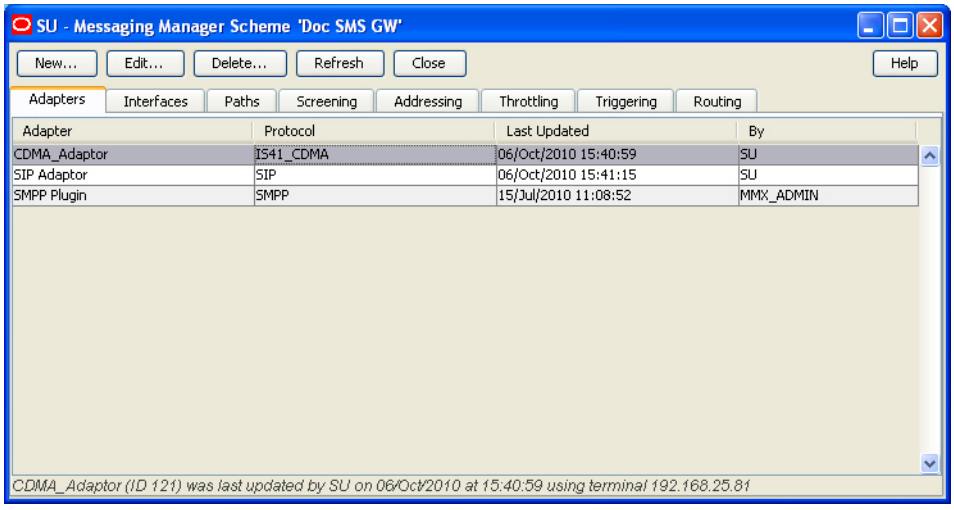
Opening schemes

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

Follow these steps to open a scheme:

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.

Related topic

Schemes

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.

1. In the table on the **Schemes** tab, select the record to copy.
2. Click **Copy**.

   Result: The Copy Scheme '*Scheme_Name*' screen appears.
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.

Related topic

Schemes

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.

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*

Related topic

Schemes

Editing schemes

Follow these steps to edit an existing scheme record.

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.
3. Configure this record by entering data in the fields on this screen.

   For more information about the fields on this screen, see Scheme fields.
4. Click **Save** to save the updated scheme record in the configuration database.

Related topic

Schemes

Deleting schemes

Follow these steps to delete an existing Scheme record.

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

   Result: One of the following dialogs appears:
   - Delete Scheme '*Scheme_Name*'
   - Scheme In Use
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.

Related topic

Schemes

Networks

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

Topics:

Networks columns

Networks fields

Editing networks

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.
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 (IMSIs 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.

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**
3. **Result:** The Edit Network '*Network_Name*' screen appears.
4. 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.
5. When generating temporary MSIDs for IMSIs, enter the country code to use in the **IMSI MCC** field.
6. When generating temporary MSIDs for IMSIs, enter the network code to use in the **IMSI MNC** field.
7. When generating temporary MSIDs for IMSIs, enter the fixed initial digits part of the MSIN in the **MSIN prefix** field.
8. 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.
9. 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.
10. Enter the network description in the **Description** field.
11. Click **Save** to save the updated network record in the configuration database.

Related topic

Networks

SMSCs

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.

Topics:

SMSCs fields

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.

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 SMSCs fields.

   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.

Related topic

SMSCs

Editing SMSCs

Follow these steps to edit an existing SMSC.

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**
3. **Result:** The Edit SMSC screen appears.
4. You can change the **Service centre address** for the SMSC, as required.
5. Click **Save**.

Related topic

SMSCs

Deleting SMSCs

Follow these steps to delete an existing SMSC record.

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**.

Related topic

SMSCs

ASP Parameters

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.

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).

Field	Description
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 *ACS User's Guide*.
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 *protocol* 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 ASP groups and parameter defaults.
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`

Titles for ASP configuration screens

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.

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.

2. 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
   - ASP accounts, see ASP Groups and Parameters

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

Related topic

ASP Parameters

Editing ASP parameters

Follow these steps to edit an existing ASP parameter.

1. In the table on the **ASP Parameters** tab, select the parameter to edit.
2. Click **Edit...**.

   Result: The Edit ASP Parameters '*asp_Parameter_Name*' screen opens.

   This screen enables you to edit existing ASP parameters used in the ASP account screens. For more information about ASP accounts, see ASP Groups and Parameters.

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.

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

Related topic

ASP Parameters

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.

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 ASP Groups and Parameters.
3. Click one of:
   - **Delete** to delete the ASP Parameter from the configuration database
   - **Don't Delete** to cancel the delete

Related topic

ASP Parameters

ASP Groups

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.

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 ASP Parameters.

Adding ASP groups

Follow these steps to add a new ASP group.

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 ASP Groups and Parameters.

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.

Related topic

ASP Groups

Editing ASP groups

Follow these steps to edit an existing ASP group.

1. In the table on the **ASP Groups** tab, select the group to edit.
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 ASP Groups and Parameters.

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.

Related topic

ASP Groups

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.

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 ASP Groups and Parameters.

3. Click **Delete** to delete the ASP group from the configuration database.

Related topic

ASP Groups

ASPs

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

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 ASP Groups tab. This field is required.

Note: This screen will have other configuration on later panels. This configuration is defined in the ASP Parameters 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.

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 ASP Groups and Parameters.

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.

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

Related topic

ASPs

Editing ASP accounts and templates

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

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 '*asp_Account_Name*' screen opens.
   - If the record was an ASP template, the Edit ASP template '*asp_Template_Name*' screen opens.
3. 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.
4. 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.
5. Click **Save** to save the updated ASP account or template in the configuration database.

Related topic

ASPs

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.

1. In the table on the **ASPs** tab, select the record to delete.
2. Click **Delete...**.

   Result: The Delete ASP confirmation prompt appears.

   This prompt enables you to delete an existing ASP account or ASP account template. For more information about ASP groups, see ASP Groups and Parameters.
3. Click **Delete** to delete the ASP account or template from the configuration database.

Related topic

ASPs

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 Schemes 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 Adapters 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.

Field	Description
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. 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.

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.

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.

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.

Related topic

ASPs

Editing IP connections in ASPs

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

1. In the table on the **ASPs** tab, select the record to edit.
2. Click **Edit...**.

   The Edit *protocol* Connection *'Connection_Name*' 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:
   - IP Connections for more information about configuring IP connections and for information about the connection fields for the different connection protocols
   - Paths for general information about paths and connections
4. Click **Save** to save the updated IP connection in the configuration database.

Related topic

ASPs

Deleting IP connection in ASPs

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

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 Paths and Connections.

   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.

Related topic

ASPs

2

Messaging Manager Schemes

This chapter explains the functionality of the Oracle Communications Network Charging and Control (NCC) 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.

This chapter contains the following topics.

Messaging Manager Scheme Screen

You access the Messaging Manager Scheme screen through the **Schemes** tab of the Messaging Manager Configuration screen. For details, see Opening schemes.

Scheme tabs

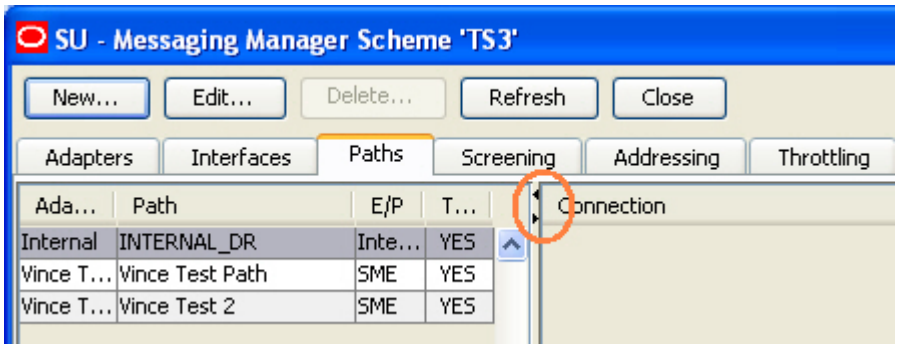
The Scheme screen allows you to configure the details of a scheme.

This table describes the tabs on the screen.

Tab	Description	See
Adapters	Defines the adapters which route traffic to and from the scheme.	Adapters
Interfaces	Defines the interfaces which are available to the scheme.	Interfaces
Paths	Defines the paths available to the scheme.	Paths
Screening	Defines the anti-spam rules for the scheme.	Screening
Addressing	Defines the addressing rules for the scheme.	Addressing
Throttling	Reports summary of all the domain throttling values.	Throttling
Triggering	Defines the triggering rules for the scheme.	Triggering
Routing	Defines the routing rules for the scheme.	Routing

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.

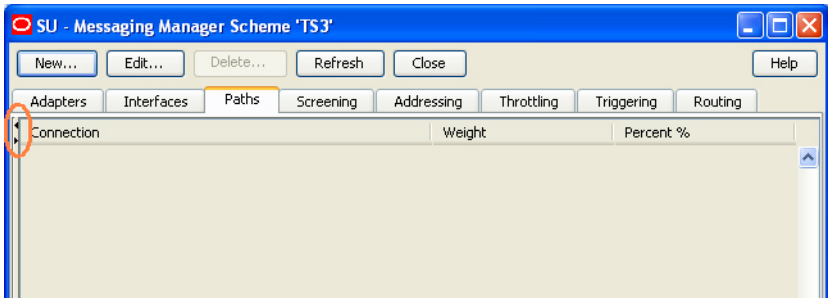


The following describes how to adjust the display:

- **To Display only the right hand panel:**

  Click the arrow which points left.

  Result: Only the right hand panel is displayed.



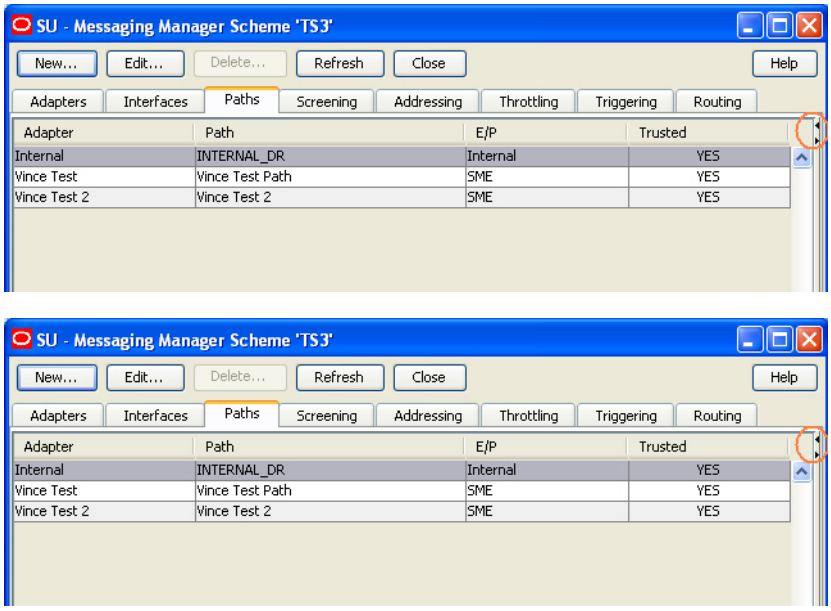
- **To Display both panels when only the right hand panel is displayed**

  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

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.

Topics:

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 `adapterName` 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 *Messaging Manager Technical Guide*.
Protocol	List of available protocols that an adapter can use.

Adding adapters

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

1. From the **Adapters** tab, click **New**.

   The New Adapter dialog displays.

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.

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.

Related topic

Adapters

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.

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.

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.

3. Click **Save**.

Related topic

Adapters

Deleting adapters

Follow these steps to delete an existing adapter record.

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.

Related topic

Adapters

Interfaces

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 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.

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

Related topic

Interfaces

Editing interfaces

Follow these steps to edit an existing interface name.

For more information about interfaces, see Interfaces and nodes.

1. On the **Interfaces** tab, select the record to edit.
2. Click **Edit**.

   Result: The Edit Routing Interface '*Interface_Name*' screen opens.

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

Related topic

Interfaces

Deleting interfaces

Follow these steps to delete an existing interface record.

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.

Related topic

Interfaces

Paths

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

Topics:

Paths tab columns

Paths tab buttons

Path screen fields

Adding paths

Editing paths

Deleting paths

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.
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 All	Selects all the paths for this scheme.
Select None	De-selects any selected paths for this scheme. This button is available whenever a path is selected.
Copy	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 Weights...	Opens the Adjust Connection Weights on Path *Path_Name* screen.
Add Connection...	Opens a new screen with blank connection record fields.
Edit...	Opens the Edit Connection screen for the selected connection.
Remove...	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
Remove... Don't Remove	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**.
Equalise Weights	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.
ASP account	The ASP account that is associated with this path. This list is populated by the ASPs 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 SMSCs for an explanation of the association. **Notes:** • This field is disabled (grayed out) if you select `MC` for the endpoint type. • If you have selected `SME` for the endpoint type, this field is required.

Field	Description
Statistics category	The text entered in this field will be added to the DETAIL column of the SMF_STATISTICS database table. This field is optional. For more information, see *MM Technical Guide*. **Note:** For delivery reports this value will automatically be **INTERNAL_DR**.
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:** • 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.

1. From the **Paths** tab, click **New**.

   Result: The New Path screen appears.

2. Fill in the **Name**, **Adapter** and **Endpoint type** fields.

   For more information about the fields in this screen, see Path screen fields.

3. 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
4. Configure any remaining fields to complete the path.
5. Click **Save** to save the new path record in the configuration database.

Related topic

Paths

Editing paths

Follow these steps to edit an existing path:

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 Path screen fields.
4. Click **Save** to save the path record in the configuration database.

Related topic

Paths

Deleting paths

Follow these steps to delete an existing path.

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.

Related topic

Paths

Path Connections

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.

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.

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

Topics:

About user authorization for local and remote connections

Adjust connection weightings

Deleting connections

About user authorization for local and remote connections

NCC 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 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.

1. From the **Paths** tab, click **Adjust Weights...**.

   Result: The Adjust Connection Weights on Path '*Path_Name*' 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.
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.

Related topic

Path Connections

Deleting connections

Follow these steps to delete an existing connection.

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 '*Connection_Name*' confirmation prompt will appear.
3. If the connection can be deleted, click **Delete** to delete the record from the configuration database.

Related topic

Path Connections

IP Connections

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.

Field	Description
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
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.

Field	Description
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.

1. From the **Paths** tab, click **Add Connection**.

   Result: The New EMI Connection screen appears.

2. Complete the fields as required in the top part of the screen. See IP Connections.

   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.

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.

Related topic

IP Connections

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

Field	Description
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 *EDR Reference Guide*.
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.

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 '*Connection_Name*' screen opens, where *Connection_Name* is the name of the selected connection.
3. Update the fields as required. See IP Connections and EMI connection fields for information about the available connection fields.
4. Click **Save** to save the connection record in the configuration database.

Related topic

IP Connections

Adding SMPP connections

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

1. From the **Paths** tab, click **Add Connection...**.

   Result: The New SMPP Connection screen appears.
2. Complete the fields as required in the top part of the screen. See IP Connections.

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.
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.

Related topic

IP Connections

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. **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 enquire_link message is sent. The connection will be closed if an enquire_link_resp (or any other kind of message) within the time specified by outgoingTimeout 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.

Field	Description
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 smscCorrelationId 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 *MM Technical Guide*.
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.

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 '*Connection_Name*' screen opens, where *Connection_Name* is the name of the selected connection.
3. Update the fields as required. See IP Connections and SMPP connection fields for more information about the available fields.
4. Click **Save** to save the connection record in the configuration database.

Related topic

IP Connections

Changing connection passwords

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

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 *protocol* Connection '*Connection_Name*' 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.

Related topic

IP Connections

SS7 Connections

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

1. From the **Paths** tab, click **Add Connection...**.

   Result: The New SS7 Connection screen appears.

2. Enter a name for the connection.

3. 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.

4. Complete the fields as required See SS7 connection fields 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.

5. 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.

Related topic

SS7 Connections

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. **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:

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 '*Connection_Name*' screen appears.

3. Change the fields as required. See SS7 connection fields.
4. Click **Save** to save the new connection record in the configuration database.

Related topic

SS7 Connections

Screening

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.

Topics:

Monitoring screening rules

Screening tab columns

Screening rule fields

Screening rule list

Calling Party Filter

Delivery Sequence Correlation

Destination Address Screening

Isolated Delivery

Layer Address Correlation

Originating Address Screening

Roaming Location Validation

Adding Screening rules

Editing Screening rules

Deleting 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*.

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:** • 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 Monitoring screening rules.
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 Screening rule list.

Field	Description
Action	The action the rule will perform when invoked, selected from a configured list. **Allowed values:** 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 Action and Error Codes.
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 Monitoring screening rules.
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
Calling Party Filter	Y	Y	Y	Y
Delivery Sequence Correlation	NA	Y	Y	NA
Destination Address Screening	Y	Y	Y	Y
Isolated Delivery	NA	Y	Y	NA
Layer Address Correlation (GSM only)	Y	Y	Y	Y
Originating Address Screening	Y	Y	Y	NA
Roaming Location Validation	Y	NA	NA	NA

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.

- 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 is 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 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 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 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 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 panel is displayed in the bottom part of the screen.

Adding Screening rules

Follow these steps to add a screening rule.

1. From the **Screening** tab, select the transaction type for the required rule from the **Transaction Type** drop down list.

   Note: The **New** button is unavailable when all allowable rules have been added for the transaction type. No more rules can be added.

2. From the **Screening** tab, click **New**.

   Result: The New SAS Rule screen appears with the selected transaction type pre-populated.

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.

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 Action and Error Codes.

6. Complete the rest of the fields on the screen.

   For more information about the rest of the fields on this screen, see Screening rule fields.

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

Related topic

Screening

Editing Screening rules

Follow these steps to edit a screening rule.

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.

Related topic

Screening

Delete Screening rules

Follow these steps to delete a screening rule.

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.

Related topic

Screening

Global Title Screening Rules

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.

Topics:

Rules buttons

Finding a rule

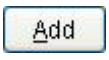
Adding a rule

Removing a rule

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.

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.

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.

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 'G*lobal_Title*' confirmation prompt appears.
3. Click **Delete** to delete the record from the configuration database.

SCA Consistency Rules

The SCA consistency rules are available when Layer Address Correlation 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.

Topics:

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.
Find	Locates a rule containing the entered digits.
Remove Selected	Deletes the selected rule.

Finding SCA Consistency Rules

Follow these steps to find SCA consistency rules.

1. Type the prefix number string to find in the **Country 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 SCA Consistency Rules

Follow these steps to add new SCA consistency rules.

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.

Related topic

SCA Consistency Rules

Editing SCA Consistency Rules

Follow these steps to edit SCA consistency rules.

1. Locate and select the SCA consistency rule to edit. Use either the scroll bar or the Finding SCA Consistency Rules procedure.
2. Click **Edit...**.

   Result: The Edit SCA Consistency Rule '*Country_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 SCA consistency rule record in the database.

Related topic

SCA Consistency Rules

Deleting SCA Consistency Rules

Follow these steps to delete a SCA consistency rule.

1. Locate and select the SCA consistency rule to delete. Use either the scroll bar or the Finding SCA Consistency Rules procedure.
2. Click **Remove Selected**.

   Result: The Remove SCA Consistency Rule '*country prefix*' confirmation prompt appears.
3. Click **Delete** to delete the record from the configuration database.

Related topic

SCA Consistency Rules

Screening Rules

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.

Topics:

Screening rule panel buttons

Screening rule fields

Adding Screening rules

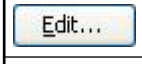
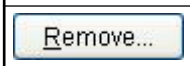
Editing screening rules

Deleting screening rules

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
Path_Direction path name prefix	The path prefix filter.
Path_Direction 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** of the Action and Error Codes screen.

Adding Screening rules

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

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 *Address_Type* Screening Rule screen appears.

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.

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.

Related topic

Screening Rules

Editing screening rules

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

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.

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.

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

Related topic

Screening Rules

Deleting screening rules

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

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.

Related topic

Screening Rules

RLV Prefix Rules

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.

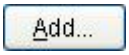
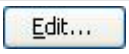
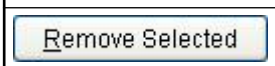
When doing the roaming location validation check, MM will compare the MSC address from the HLR against the configured prefixes to determine how many digits to match.

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.

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 RLV Prefix Rules

Follow these steps to find RLV prefix rules.

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.

1. Click **Add...**.

   Result: The New RLV Prefix Rule screen appears.

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.

Related topic

RLV Prefix Rules

Editing RLV Prefix Rules

Follow these steps to edit RLV prefix rules.

1. Locate and select the RLV prefix rule to edit. Use either the scroll bar or the Finding RLV Prefix Rules procedure.

2. Click **Edit...**.

   Result: The Edit RLV Prefix Rule 'P*refix*' 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.

Related topic

RLV Prefix Rules

Deleting RLV Prefix Rules

Follow these steps to delete an RLV prefix rule.

1. Locate and select the RLV prefix rule to delete. Use either the scroll bar or the Finding RLV Prefix Rules procedure.

2. Click **Remove Selected**.

   Result: The Remove RLV Prefix Rule '*Prefix*' confirmation prompt appears.

3. Click **Delete** to delete the record from the configuration database.

Related topic

RLV Prefix Rules

Addressing

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).

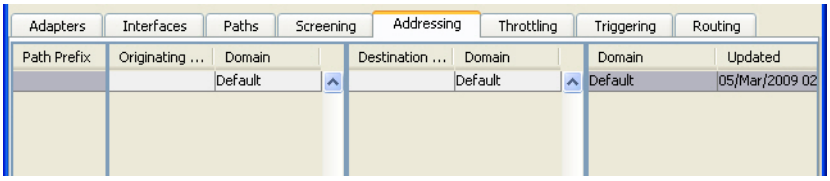
An address is considered to be a member of the set defined by the rule if the leading characters of the address match the address prefix and the message type matches the specified type.

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.

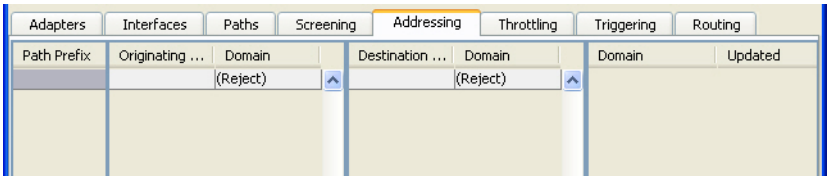
Pre-populated screen areas

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 for details.

Removing a Path Prefix

Follow these steps to remove a path prefix.

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.
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 before you add a rule.

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.
3. In the **Domain** field, select the domain to map the rule against.

   Note: If the domain is not in the list, you need to click **Cancel** and Adding domains 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).

Related topic

Addressing

Editing address rules

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

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 Adding Address rules.

   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.

Related topic

Addressing

Removing Address rules

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

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.

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

Related topic

Addressing

Adding domains

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

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.

Related topic

Addressing

Editing domains

Follow these steps to edit an existing domain.

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.

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.

Related topic

Addressing

Deleting domains

Follow these steps to delete an existing domain:

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.

Related topic

Addressing

Throttling

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.

Topics:

Throttling rules fields

Adding Throttling rules

Editing Throttling Rules

Deleting Throttling Rules

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 Transaction Types. 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.

Adding Throttling rules

Follow these steps to add throttling rules.

1. From the **Throttling** tab, click **New**.

   Result: The New Throttling Rule screen appears.
2. Select values required in each field as described in Throttling rules fields.
3. Click **Save** to save the record in the configuration database.

Related topic

Throttling

Editing Throttling Rules

Follow these steps to edit an existing Throttling Rule

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.

3. Change the fields, as described in Throttling rules fields, as required.
4. Click **Save** to save the Throttling rule in the configuration database.

Related topic

Throttling

Deleting Throttling Rules

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

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.

Related topic

Throttling

Triggering

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.

Topics:

Trigger control

Triggering fields

Adding Triggering rules

Editing Triggering rules

Deleting Triggering rules

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 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 Transaction Types for details.
Originating Domain	Trigger rule applies to messages which have this originating domain. For more information, see Screening Rules. **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.
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 Screening Rules. **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.

Field	Description
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 Triggering.
Release cause	If you set **Perform action** to `Reject`, then select the release cause to send back to the switch from the **Release cause** list. **Note:** You configure the release causes listed in this field on the **Global tab** of the Action and Error Codes screen.

Field	Description
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 `Deliver`, `Notification` and `Submit` detection points support these routing classes: • Deliver • FDA • Submit The default `Routing Info` detection point supports only the Locate routing class. For more information about routing classes, see Routing Class.
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 Combo boxes.
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 Combo boxes.

Adding Triggering rules

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

1. On the **Triggering** tab, select the **Detection Point** that the trigger rule is to apply to and click **New**.

   Result: The New Trigger Rule screen appears. For a 'Deliver', 'Notify' or 'Route Info' Detection Point, the screen includes the Destination Domain and Destination Address prefix fields. For a 'Submit' Detection Point the New Trigger Rule screen has the Originating Domain and Originating Address prefix fields instead.

2. Select or enter the fields, as described in Triggering fields, as required.
3. Click **Save** to save the new Triggering rule in the configuration database.

Related topic

Triggering

Editing Triggering rules

Follow these steps to update an existing Triggering rule.

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

   Result: The Edit Trigger Rule screen appears.
3. Select or complete the fields, as described in Triggering fields, as required.
4. Click **Save** to save the Triggering rule in the configuration database.

Related topic

Triggering

Deleting Triggering rules

Follow these steps to delete an existing Triggering rule.

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

   Result: The Delete Trigger Rule *'Rule_Name*' confirmation prompt appears.
3. Click **Delete** to delete the record from the configuration database.

Related topic

Triggering

Routing

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

Topics:

Routing fields

Adding Routing rules

Editing Routing rules

Deleting Routing rules

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

Field	Description
SMSC	The SMSC to use for this outbound route. **Note:** This field is only available when a Submit Routing class is selected.
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:

1. On the **Routing** tab, select the **Routing class** that the routing rule is to apply to and click **New**.

   Result: A version of the New Routing Rule screen appears; the contents vary based on the *Routing class.*

2. Select or enter the fields, as described in Routing fields, 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.

Related topic

Routing

Editing Routing rules

Follow these steps to edit an existing routing rule:

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 Routing fields, as required.
5. Click **Save** to save the routing rule to the configuration database.

Related topic

Routing

Deleting Routing rules

Follow these steps to delete an existing routing rule:

1. In the table in the **Routing** tab, select the record to delete.
2. Click **Delete**.

   Result: The Delete Routing Rule '*Route_Name*' confirmation prompt appears.
3. Click **Delete** to delete the record from the configuration database.

Related topic

Routing

3

Messaging Manager Replication Screen

Replication is the process used to ensure several instances of databases are kept synchronized. This chapter explains the Messaging Manager replication process.

This chapter contains the following topics.

Messaging Manager Replication

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

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.

1. Select the **Services** menu from the SMS main screen.
2. Select **Messaging Manager**.
3. Select **Replication**.

   Result: The Messaging Manager Replication screen displays.

Replication

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.

1. Open the Messaging Manager Replication screen.
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.

4

Messaging Manager Action and Error Codes

This chapter explains how to configure the reject action error codes.

This chapter contains the following topics.

Action and Error Codes

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.

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.
- 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.

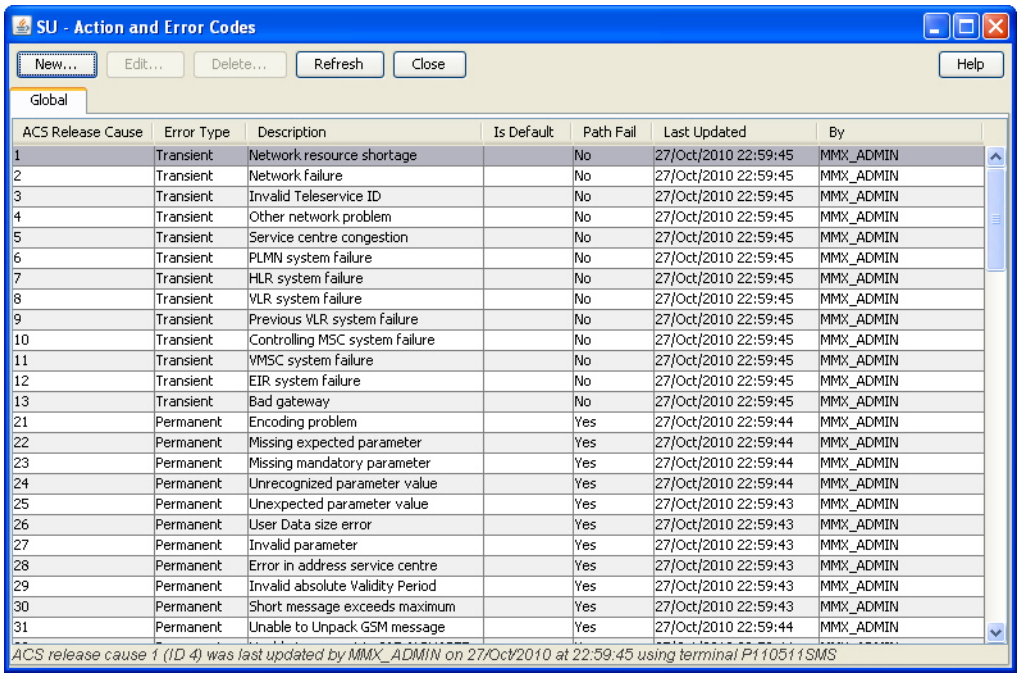
Global Action and Error Codes

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.

Topics:

Global tab

Here is an example **Global** tab.



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 retires 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.

1. From the **Global** tab screen, click **New**.

   Result: The New Release Cause screen opens.

   See Global fields for a description of each field.

2. In the **ACS Release Cause** field, enter the release cause number.

   Note: Must be a unique number, less than 118.

3. Enter the description for the release cause in the **Description** field.
4. Select the type of error for this release cause from the **Error Type** drop down list.
5. Select the **Path Failure** check box if you wish this release cause to be a path failure.
6. 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.

7. Click **Save** to save the new release cause record in the configuration database.

Related topic

Global Action and Error Codes

Editing Global Release Cause

Follow these steps to edit a global error code.

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.
3. Change the fields as required. See Global fields for a description of each field.
4. Click **Save** to save the release cause record in the configuration database.

Related topic

Global Action and Error Codes

Deleting Global Release Cause

Follow these steps to delete a Global Release Cause.

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.

Related topic

Global Action and Error Codes

SMPP

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

Topics:

SMPP fields

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**.
Error Type	The type of error the ACS release cause number represents. **Note:** This is defined on the **Global tab**.

EMI

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

Topics:

EMI fields

This table describes the content of each column.

Field	Description
Context	The circumstances in which this mapping will be applied.
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**.
Error Type	The type of error the ACS release cause number represents. **Note:** This is defined on the **Global tab**.

MAP

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

Topics:

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.

Field	Description
CauseCode/Access 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**.
Error Type	The type of error the ACS release cause number represents. **Note:** This is defined on the **Global tab**.

Actions available

From this tab, for a release cause mapping you can:

- Adding release cause mapping - MAP, IS-41
- Editing release cause mapping - MAP, IS-41
- Deleting release cause mapping

For an error mapping you can:

- Adding error mapping - MAP, IS-41
- Editing error mapping - MAP, IS-41
- Deleting error mapping

IS-41

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

Topics:

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	*Not used for IS-41*

Field	Description
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
- Editing release cause mapping - MAP, IS-41
- Deleting release cause mapping

For an error mapping you can:

- Adding error mapping - MAP, IS-41
- Editing error mapping - MAP, IS-41
- Deleting error mapping

SIP

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

Topics:

SIP fields

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**.
Error Type	The type of error the ACS release cause number represents. **Note:** This is defined on the **Global tab**.

Release Cause Mapping

The names of the fields, except the release cause field, on the following screens, are different, depending on the protocol selected.

Topics:

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.

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 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...**.

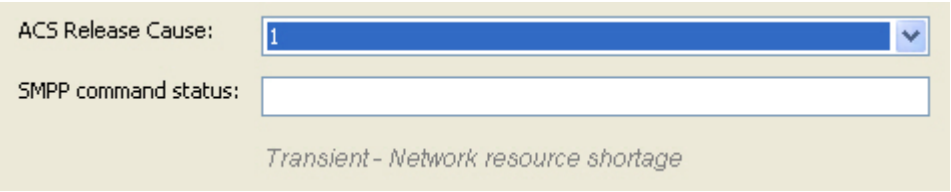
   Result: The New Release Cause Mapping screen opens.

   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.

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.

   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 Global fields.



5. Enter the protocol error code to map to in the bottom field. The name of the field varies according to the protocol:

Protocol	Field name	More information
SMPP	SMPP command status	See SMPP fields.
EMI	EMI error code	See EMI fields.
SIP	SIP Status	See SIP fields.

Note: Must be a unique release code for this protocol.

6. Click **Save** to save the new release cause mapping record in the configuration database.

Related topic

Release Cause Mapping

Adding release cause mapping - MAP, IS-41

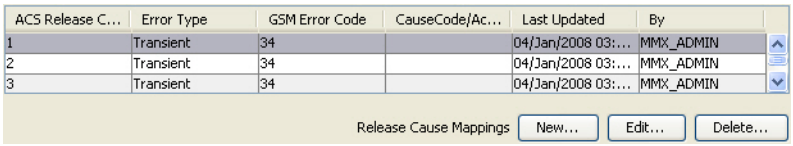
In this example the MAP protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

- MAP
- IS-41

Follow these steps to add a release mapping to a protocol.

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 top table on the tab displays the release cause mappings.

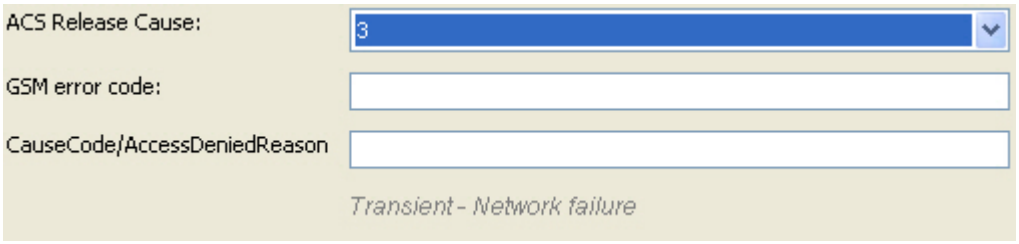


2. To the right of **Release Cause Mappings**, click **New**.

   Result: The New Release Cause Mapping screen opens.

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.



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.
   - IS-41 - see IS-41 fields.
5. **Note:** Must be a unique release code for this protocol.

6. Click **Save** to save the cause mapping record in the configuration database.

Related topic

Release Cause Mapping

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.

1. From the Action and Error Codes screen, click the required protocol tab to edit the release mapping for.

   Result: The *Protocol* 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. 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:
   - SMPP - **SMPP command status**. See SMPP fields.
   - EMI - **EMI error code**. See EMI fields.
   - SIP - **SIP Status**. See SIP fields.
5. Click **Save** to save the cause mapping record in the configuration database.

Related topic

Release Cause Mapping

Editing release cause mapping - MAP, IS-41

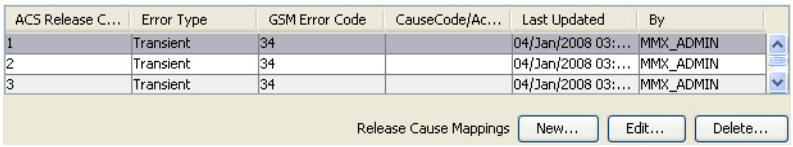
In this example the MAP protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

- MAP
- IS-41

Follow these steps to edit a release mapping for a protocol.

1. From the **Action and Error Codes** screen, click the required <protocol> tab to edit the release mapping for.

   Result: The *Protocol* 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. In the Release Cause Mappings table on the tab, select the record to edit.
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:
   - MAP - see MAP fields.
   - IS-41 - see IS-41 fields.
5. Click **Save** to save the cause mapping record in the configuration database.

Related topic

Release Cause Mapping

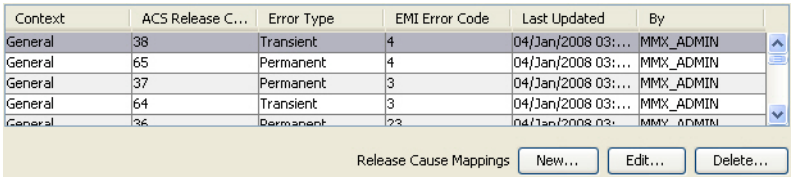
Deleting release cause mapping

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.

1. From the Action and Error Codes screen, click the required protocol tab to delete the release cause mapping from.

   Result: The *Protocol* 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.



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.

Related topic

Release Cause Mapping

Error Mapping

The names of the fields, except the release cause field, on the following screens, are different, depending on the protocol selected.

Topics:

Adding error mapping - IP

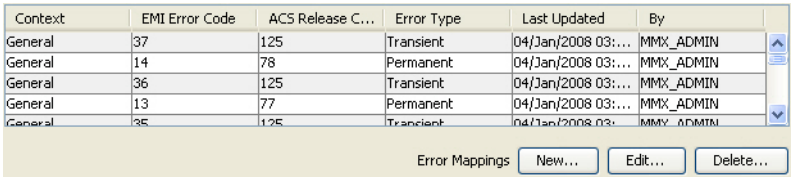
In this example the EMI protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

- SMPP
- EMI
- SIP

Follow these steps to add an error mapping to a protocol.

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



2. To the right of **Error Mappings**, click **New**.

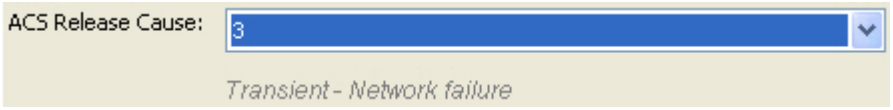
   Result: The New Error Mapping screen opens.

3. Enter the protocol error code to map to in the top field. The name of the field varies according to the protocol:

Protocol	Field name	More information
SMPP	SMPP command status	See SMPP fields.
EMI	EMI error code	See EMI fields.
SIP	SIP Status	See SIP fields.

   Note: Must be a unique release code for this protocol. Select the global release cause to map with from the ACS Release Cause drop down list.

4. **Result:** The error type and description of the release cause are displayed below the fields. Refer to Global fields.



5. Click **Save** to save the new release mapping record in the configuration database.

Related topic

Error Mapping

Adding error mapping - MAP, IS-41

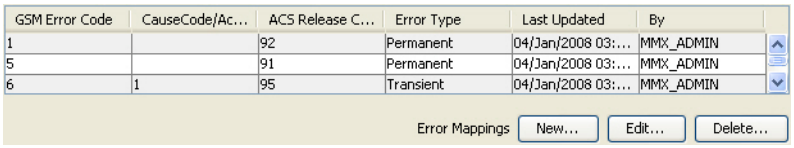
In this example the MAP protocol has been used. Apart from the different error code names, the add procedure is identical for the following protocols:

- MAP
- IS-41

Follow these steps to add an error mapping to a protocol.

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.



2. To the right of **Error Mappings**, click **New**.

   Result: The New Error Mapping screen opens.

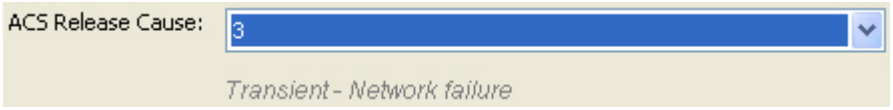
3. Enter the protocol error codes to map to in the top two fields. The names of the fields vary according to the protocol:

   - MAP - see MAP fields.
   - IS-41 - see IS-41 fields.

   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.



5. Click **Save** to save the error mapping record in the configuration database.

Related topic

Error Mapping

Editing error mapping - IP

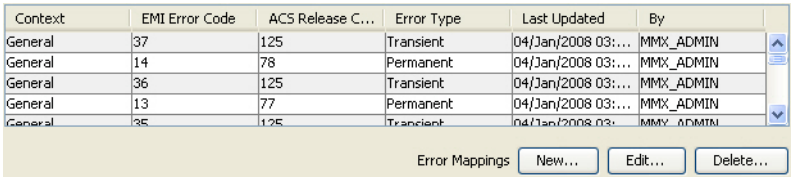
In this example the EMI protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

- SMPP
- EMI
- SIP

Follow these steps to edit a release mapping for a protocol.

1. From the **Action and Error Codes** screen, click the required <protocol> tab to edit the release mapping for.

   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



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 name of the field varies according to the protocol:

Protocol	Field name	More information
SMPP	SMPP command status	See SMPP fields.
EMI	EMI error code	See EMI fields.
SIP	SIP Status	See SIP fields.

4. Change the ACS Release Cause, if required.
5. Click **Save** to save the error mapping record in the configuration database.

Related topic

Error Mapping

Editing error mapping - MAP, IS-41

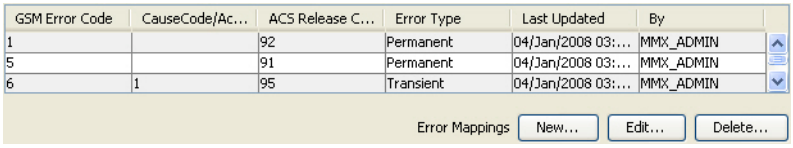
In this example the MAP protocol has been used. Apart from the different error code names, the edit procedure is identical for the following protocols:

- MAP
- IS-41

Follow these steps to edit a release mapping for a protocol.

1. From the **Action and Error Codes** screen, click the required <protocol> tab to edit the release mapping for.

   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



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.
- IS-41 - see IS-41 fields.

4. Change the ACS Release Cause, if required.
5. Click **Save** to save the error mapping record in the configuration database.

Related topic

Error Mapping

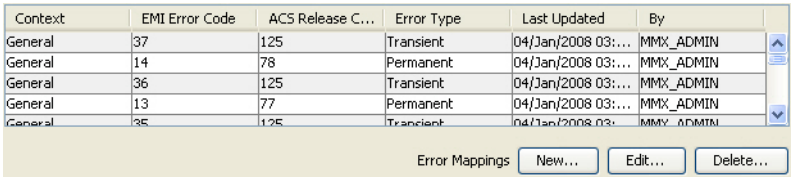
Deleting error mapping

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.

1. From the **Action and Error Codes** screen, click the required protocol tab to delete the release cause mapping from.

   Result: The *Protocol* 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



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.

Related topic

Error Mapping

5

Messaging Manager Routing Scheme Edit Control

This chapter explains how to manage routing scheme components.

This chapter contains the following topics.

Routing Scheme Edit Control

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.

1. Select the **Services** menu from the SMS main screen.
2. Select **Messaging Manager**.
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.
- Logging into the Service Management System screen, see *SMS User's Guide*.

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.
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.

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.

6
XMS Content Feature Nodes

This chapter describes the Oracle Communications Network Charging and Control (NCC) Messaging Manager XMS Content feature nodes.

This chapter contains the following topics.

Extract Content

The Extract Content feature node extracts a part of a profile field, or incoming SMS message, and stores it in a specified profile field.

Note: The part extracted is a string (that can represent a number or text) delimited by a white space character. For the various white space characters used by the supported alphabets see www.unicode.org.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The required section of the SMS was extracted and stored.

Exit	Cause	Description
2	Error	The section of SMS could not be extracted, for the following reasons: • The input type expected was numeric but the extracted section contained non numeric digits for the alphabet in use. • The input type expected was numeric but "+" found after the start of the extracted section. • The content did not match the expected content type. • There are not enough words in the source to match the word number extraction criteria.

Configuring the node

Follow these steps to edit the node configuration.

1. For the source, you can select either a profile, or the SMS buffer. To select:
   - A profile, select the **Source Location** and **Source Field**
   - SMS buffer content, select the **Use SMS Payload** check box
2. In the **Word number** field, enter the number of the word, or range of words, to extract from the source.

   Note: The Word number can be positive, zero or negative.

   Suppose the message reads "`It was the best of times`".

   - A positive number means that you count from the left-hand side, or start, of the message.

     Example: 3 would extract "`the`".
   - 0 or 1 means select the first word on the left-hand side, or start, of the message.

     Example: 1 would extract "`It`".
   - A negative number means count back from the right-hand side, or end, of the message.

     Example: -2 would extract "`of`".
   - a number followed by a colon means from that numbered word to the end.

     Example: 3: would extract "`the best of times`".
   - A colon followed by a number means from the beginning (word 1) to the number word specified.

     Example: :4 would extract "`It was the best`"
   - A negative followed by a colon means count back from the right then all to the end.

     Example: -3: would extract "`best of times`".

- Two numbers separated by a colon means a range of first specified word to the last specified.

  Example: 3:5 would extract "`the best of`".

- Two negative numbers separated by a colon mean first number from the right to the second number from the right.

  Example: -4:-2 would extract "`the best of`"

- Just a colon (that is, ":") means the entire string.

Note: Some ranges, such as 3:-7 for this example will just produce a blank string in the target field and will exit from the Error branch because there are not enough words.

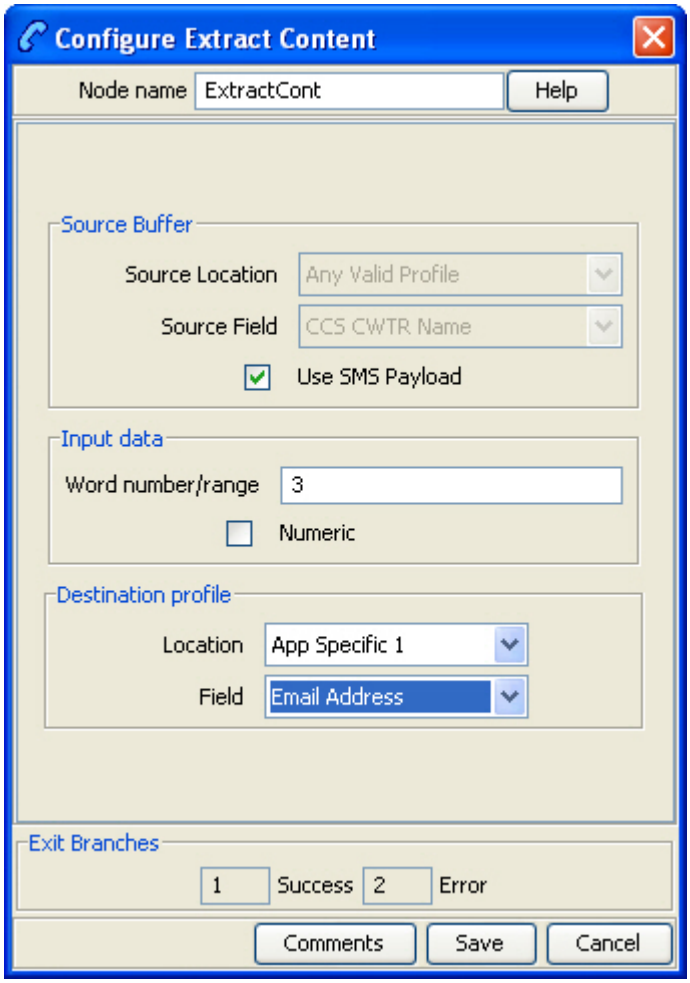
3. If the extracted word needs to be validated as a number, select the **Numeric** check box. The node will exit from the Error branch if the selection is not numeric.
4. Select the extracted content store location from the **Location** drop down list.
5. Select the store location field from the **Field** drop down list.
6. Click **Save**.

Example

Here is an example of the process, using the Extract Content node to extract the email forwarding address.

1. Users can enable forwarding by sending an SMS, for example:

   Fwd on joe.bloggs@telco.com
2. The control plan would use the Format Text node to check if it was a valid message.
3. The Extract Content node is configured as shown below.



Result: This node would store the third word (that is, 'joe.bloggs@telco.com') in the user's profile under the 'Email Address' tag.

Extract Number

The Extract Number feature node extracts the MSISDN from business card data held in either the SMS TEXT context or configured profile field, and then stores the MSISDN in a profile field.

The node will process the provided text to extract a valid MSISDN. Non-numeric numbers will be ignored unless they constitute part of the number.

The following examples demonstrate valid formats:

- "(012) 345 6789"
- "0123,456,789"
- "+44-123-456"
- "+44 123 456789"
- "(+44)123-456789"

Note: The business card data must contain only one MSISDN. The MSISDN will be extracted without normalization.

Node exits

This node has one entry and three exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	MSISDN successfully extracted and stored in the specified profile field
2	Too Many Numbers	Unable to extract the MSISDN as there was more: • Than one number in the SMS context/profile field • Digits than the maximum allowed
3	Error	Either of the following: • An error occurred reading the business card data, for example. The business card did not contain an MSISDN or it was an invalid number. • Less than the minimum expected digits

Configuring the node

Follow these steps to configure the node.

1. Select the **Business Card Source**:
   - **From Profile** to locate the card in a profile
   - **From SMS** to locate the card in a message (the Source Profile section will be grayed out)
2. For a profile location, select the **Source Profile** from the **Source Data Type, Location and Field** drop down lists.
3. select the **Destination Profile** where the extracted MSISDN will be stored from the **Destination Data Type, Location and Field** drop down lists.

   Warning: Unexpected behavior encountered if the source and destination profiles are the same.
4. In the **Minimum** field, type the minimum length allowed for the MSISDN.

   Note: The error branch will be followed if the length of the extracted MSISDN is less than the defined minimum length.
5. In the **Maximum** field, type the maximum length allowed for the MSISDN.

   Note: The too many numbers branch will be followed if the length of the extracted MSISDN is greater than the defined maximum length.
6. Click **Save**.

Format Text

The Format Text feature node enables a buffer to be populated with a formatted string based on a static string that may include place holders for the contents of other selectable buffers.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The formatting was successful.
2	Error	There is something wrong with the format string and it cannot be formatted. The output buffer will be unchanged.

Configuring the node

Follow these steps to configure the node.

1. In the Target Buffer area, select the buffer to store the formatted string. You can:
   - Select a **Target Location** and **Target Field**
   - Select the **Use SMS Payload** check box to populate the SMS buffer
2. If you wish to add the text created in this node to the end of the existing contents of the target buffer, select the **Append to target** check box.
3. The **Format** field is where you supply the format of the string. This is free-form and allows any text. The variables starting with $ will be substituted at run time by the text in the source buffer specified by the number, for example $1 is the 1st Source, $2 the 2nd Source.

   Note: The only valid characters to follow the $ are 1, 2, 3, 4, 5, and $. Anything other than these values will result in the node exiting the Error exit.

   If you wish to use the dollar sign in the string, you must prefix it with $, that is, $$.
4. There are 5 source areas available. In each of the required source areas, select the **Source Location** and **Source Field**. These buffers can be strings, integers, prefix trees, or dates.

   Note: If the source buffer is a date, then a date format can be supplied. This is in the format *field* followed by {} containing the formatting values, for example, $4{%d/%m/%y}. If no format is specified then the system locale date format will be used.

Example

Here is an example of the process, using the Format Text node to store the blacklist contents of a user's profile to send to them.

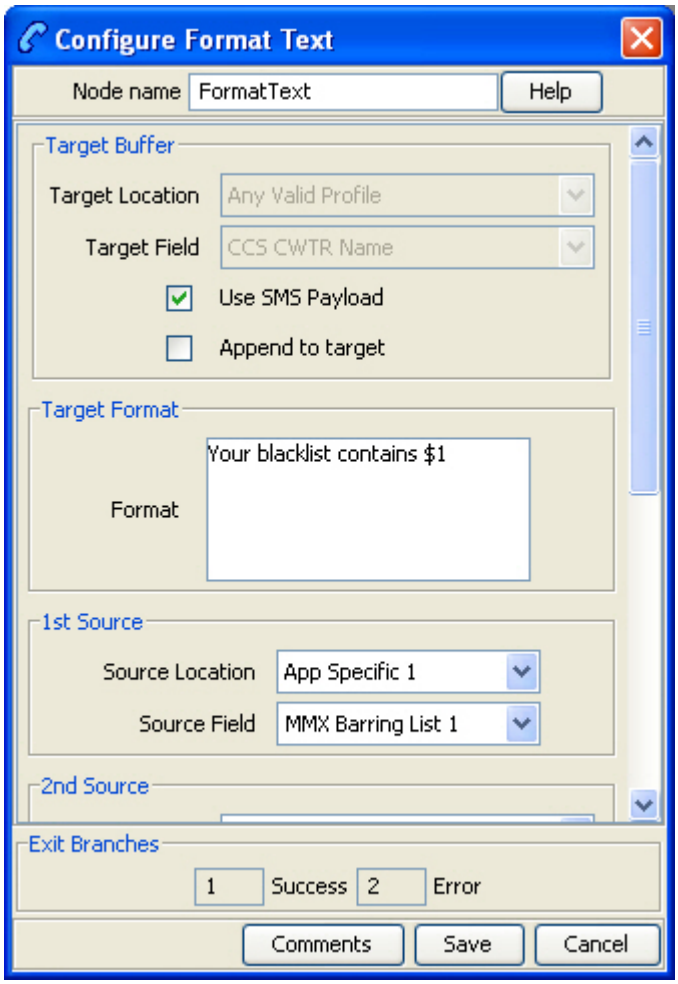
The user's blacklist contains the following numbers:

1230001

1230015

1230004

You can use the Format Text node to create a string containing the blacklist by configuring the node as shown below.



Result: The formatted string is:

"Your blacklist contains 1230001 1230015 1230004"

This is stored in the SMS payload target buffer. It can then be sent using another node in the control plan.

Keyword Search and Replace

The Keyword Search and Replace node branches, depending on whether or not a particular word was matched in the message.

The node allows up to five different keywords to be searched for in the short message and will branch according to the word that was matched. It is also possible to replace the word that was matched in the message with something else.

Node exits

This node has one entry and seven exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Matched 1	The keyword specified as Pattern 1 was matched in the message.
2	Matched 2	The keyword specified as Pattern 2 was matched in the message.
3	Matched 3	The keyword specified as Pattern 3 was matched in the message.
4	Matched 4	The keyword specified as Pattern 4 was matched in the message.
5	Matched 5	The keyword specified as Pattern 5 was matched in the message.
6	Not Matched	None of the patterns specified in the node were matched
7	Bypass	NA

Configuring the node

Follow these steps to edit the Keyword Search and Replace node.

1. Enter the patterns that are to be searched for in the message.
2. Enter the replacement values for each searchable pattern.
3. Select the **Case Sensitive** check box to make search patterns case sensitive.
4. Select the **Bypass Concatenated** check box to not check for the patterns in concatenated messages.
5. Click **Save**.

   Note: The node will search the message for the patterns to be matched in order, and once a match is made will not search any further.

Message Data Branching

The Message Data Branching node branches depending on whether the current message contains text or data, according to the data coding scheme.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Text Message	The message is text encoded.
2	Data Message	The message is data encoded.

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

Text Content Branching

The Text Content Branching node branches depending on the content of the short message.

It takes the regular expressions entered into the node and tries to match these expressions to the content of the short message. Matches are done in the order that they appear in the node, as soon as a match is made the branch corresponding to that expression will be taken. The node does not do a "best match", but looks for and takes the first match found.

When a match is found, it branches accordingly; if no match is found the node exits the "Not Matched" exit.

Node exits

This node has one entry and seven exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Match 1	Short message received matches regular expression 1.
2	Match 2	Short message received matches regular expression 2.
3	Match 3	Short message received matches regular expression 3.
4	Match 4	Short message received matches regular expression 4.
5	Match 5	Short message received matches regular expression 5.
6	Not Matched	None of the regular expressions matched the short message.
7	Exception	Exceptions thrown while matching the expressions from content of short message.

Configuring the node

Follow these steps to edit the Text Content Branching node.

1. Determine whether the regular expressions that are to matched against the short messages are to be case sensitive; if so, select the check box.
2. Enter up to five regular expressions that the short message is to be matched against.
3. Click **Save**.

7

XMS Control Feature Nodes

This chapter describes the Oracle Communications Convergent Charging Controller Messaging Manager XMS Control feature nodes.

This chapter contains the following topics.

Accept

The Accept node is used to instruct Messaging Manager to perform an Accept action.

This node should be used in preference to the Disconnect Call node specifying 127.

Node exits

This node has one entry and one exit. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The Release Code has been sent.

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

Attempt Delivery Pending

The Attempt Delivery Pending (ADP) feature node attempts to deliver the message. This feature node has no billing engine interaction, and will attempt the delivery of the short message with no account balance check.

This feature node also monitors for message delivery and returns a message delivery status.

Node exits

This feature node has one entry and five exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Delivery Failure	SMS delivery failed.
2	Queued	SMS sent to SMSC, no further monitoring.
3	Notified	Successful delivery of the message to an SME.
4	Abort/Abandon	An abort was received from the network, or message abandoned.
5	Node Failure	Failure due to an internal error, or result message being either unknown, or not of the right type.

Editing the node

Follow these steps to configure the Attempt Delivery Pending feature node.

1. Select the action for Messaging Manager to take. To cause a:
   - Route action, select **Route**
   - Relay action, select **Relay**
   - Route Unchanged, select **Route Unchanged**
2. For more information about the different actions, see the discussion on triggering rules in *Messaging Manager User's Guide*.
3. Click **Save**.

Branch on Domain

The Branch on Domain node allows a service plan to act differently depending on the domains assigned to the message origination or destination domains.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Match	The configured regular expression matches the indicated domain.
2	No Match	The regular expression does not match the domain.

Configuring the node

Follow these steps to edit the Branch on Domain node.

1. Select which **Domain** to match on.
2. Enter the **Pattern** to match against.
3. Click **Save**.

Discard

The Discard node is used to tell Messaging Manager to perform a discard action.

Node exits

This node has one entry and one exit. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The Release Code has been sent.

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

MMX EDR

The MMX EDR node takes a literal string for the EDR tag, and a profile buffer for the EDR value. Thus, any profile buffer can be written to an MMX EDR. The node stores the string as a profile buffer. This buffer will then be examined by the service loader, and passed back to Messaging Manager as an extension with the tag SM_TAG_CDR_INFO.

EDRs specified by the MMX EDR nodes will appear in the final EDR in alphabetical order instead of following the processing order in the control plan.

The MMX EDR node does not interact with EDR tags from other sources and will not affect or overwrite any of these EDR tags. Therefore, the final EDR record may have duplicated EDR tags if the same EDR tag is defined and used by the MMX EDR node and other different sources.

Supported profile data types

The profile data types supported by the MMX EDR node are limited to the following types:

- STRING
- NSTRING
- LNSTRING
- SHORT
- UINTEGER
- INTEGER
- BYTE

For other types, you need to use the Format Text node to format the data and save the formated string into a profile buffer, then configure the profile buffer as the source buffer in the MMX EDR node.

Node exits

This node has one entry and three exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Value successfully retrieved from profile.
2	Value not Found	Value not found in profile.
3	Failure	General failure condition.

Configuring the node

Follow these steps to configure the node.

1. Enter an EDR Tag in the field.

   Note: When using the MMX EDR node to build a control plan, you need to make sure all given EDR tags are unique across the control plan. If there are any duplicated EDR tags, the last occurrence will overwrite previous ones.

2. Select a profile location and field to retrieve.
3. Click **Save**.

Reject

The Reject node is used to send a specified (in this node) ACS release cause to Messaging Manager.

This node should be used in preference to the Disconnect Call node specifying the release cause.

Node exits

This node has one entry and one exit. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The ACS release cause has been sent to MM.

Configuring the node

Follow these steps to edit the node configuration.

1. Select the Reject cause to use from the **Release cause** drop down list.
2. Click **Save**.

Send Short Message Notification

Use the Send Short Message Notification (SSMN) feature node to construct and send an INTERNAL short message from Messaging Manager that you specify either in the feature node, or by using a notification template defined in ACS.

You select the message originator and destination from the following options:

- A fixed number or alphanumeric address. If the address is alphanumeric, the message must be routed through the protocol that supports it, such as EMI, SMPP, or SIP.
- Any existing ACS context digit field, including:
  - The caller or message originator of the current call or SMS.
  - The called party or message destination of the current call or SMS.
- A profile tag containing a comma separated list of destinations.

If required, you can override NPI and TON values in the outgoing message by using a Set, or a Copy feature node before the SSMN feature node in the control plan. You use the Set, or the Copy feature node to set the override values in one or more of the following profile fields:

- SSMN Originating TON Override
- SSMN Destination TON Override
- SSMN Originating NPI Override
- SSMN Destination NPI Override

See the section on "NPI and TON Override Profile Fields" in *Feature Nodes Reference Guide* for more information.

Note: You can use the SSMN feature node in any service control plan. Although the SSMN feature node is installed with Messaging Manager, you can use it in non-Messaging Manager service control plans. The SSMN feature node does not require the use of the Messaging Manager service library.

Important: To use this feature node in a service control plan, an INTERNAL adapter must be configured in the system.

Node exits

This feature node has one entry and eight exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Message sent successfully.
2	Send Failure	Cannot send SLEE event to wrapper.

Exit	Cause	Description
3	Params Unavailable	The token specified cannot be found. For example <SMS_TEXT> token, if message text is not available or cannot be converted to Latin-1.
4	Node Failure	Internal node error. Message not sent.
5	Timeout	Did not get the expected response within the Timeout number of seconds.
6	Temporary Error	The returned cause code maps to a temporary error.
7	Permanent Error	The returned cause code maps to a permanent error.
8	Abort	The returned cause code maps to an abort error.

Note: The temporary, permanent and abort errors are all configured in the Messaging Manager Action and Error Codes screens. From the main SMS screen, see **Services > Messaging Manager> Action and Error Codes** and the **Error Type** column.

Configuring the node

Follow these steps to edit the Send Short Message Notification feature node.

Message Addresses - Source

1. Select the **Type** of source address from the list.

   Result: The fields requiring data for the type selected are made available.

2. If available, enter the characters or digits for the source address in the **Chars/Digits** field.

   Tip: This is a text string representing the sender of the notification. It can be either a telephone number or an alphanumeric address.

   If it contains any characters other than 0-9, it will be regarded as an alphanumeric address and will have TON (type of number) set to alphanumeric, otherwise TON will be set to unknown. NPI (number plan indicator) will always be set to unknown.

3. If available, from the **Profile Block** drop down list, select the profile block for the source address.

4. If available, enter in the **Tag** field, the location of the source address within the selected profile block.

   Tip: Valid tags for the profile block can be found in the ACS configuration screens. From main SMS screen, select menu options **Services > ACS Services**, then **Configuration**. The profile block and tag names are available under the **Profile Tag Mapping** tab, and the tag value for the tag name under the **Profile Tag Details** tab (**Profile Tag** column).

Message Addresses - Destination

1. Select the **Type** of destination address from the list.

   Result: The fields requiring data for the type selected are made available.

2. If available, enter the characters or digits for the destination address in the **Chars/Digits** field.

Tip: This is a text string representing the sender of the notification. It can be either a telephone number or an alphanumeric address.

If it contains any characters other than 0-9, it will be regarded as an alphanumeric address and will have TON set to alphanumeric, otherwise TON will be set to unknown. NPI will always be set to unknown.

3. If available, from the **Profile Block** drop down list, select the profile block for the destination address(es).
4. If available, enter in the **Tag** field, the location of the destination address(es) as a comma separated list of destinations within the selected profile block.

   Tip: Valid tags for the profile block can be found in the ACS configuration screens. From main SMS screen, select menu options **Services > ACS Services**, then click **Configuration**. The profile block and tag names are available under the **Profile Tag Mapping** tab, and the tag value for the tag name under the **Profile Tag Details** tab (**Profile Tag** column).

Options

1. To send the message as a flash message, select the **Flash Message** check box.

   Tip: Flash messages are displayed immediately on the subscriber's handset, rather than going to their in box.
2. If a response is expected, to avoid missing the response, select the **Wait for Response** check box and then enter the number of seconds to wait for the response in the **Timeout** field.

   Tip: If the check box is deselected, then the node will exit the Success exit immediately.
3. To preserve the parameters set for the original message that triggered the control plan, select the **Copy Current Message** check box.

   Result: The current message is copied and the parameters supplied in this node are applied to the internal message being constructed by this node.

   Example: If the destination domain has been specified in the Set Message Routing node earlier in the control plan, this will be copied to the new message.

Alphabet

1. Select a character encoding for the SMS message, click on the arrow against the **Alphabet** text box and pick an encoding from the drop-down list.

   Example: To send SMS text using Arabic characters, you would pick

   ```
   ISO88596, Arabic
   ```

   .

Message

1. Select one of the following
   - **Use Notification Template** to send the message using a notification template. Then select the **Application**, **Type** and **Language** for the template from the drop down lists, or
   - **Use Message** to specify the message in the feature node. Then type the text of the notification message in the **Message** field.
2. See Message content for a description of how to construct messages.

3. Click **Save**.

Message content

The **Message** field is a (UTF-8) text field. This field is tokenized when the node is initialized, so that fast construction of the message can be done during message processing. For a list of tokens, see Message tokens.

Tokens are searched for in the message text, and replaced with an appropriate value. If the value (at call-time) is null, the token is removed from the message text.

The SMS is sent to MM with the specified UTF-8 encoded text, and the desired alphabet set from the Alphabet drop down list.

Warning: Tokens are case sensitive.

Machine environment information

In addition, there is access to some of the machine's environment information, using the following tokens.

Token	Description
<DATE>	The current system time on the SLC (after conversion to GMT). Output format is described in the Configuration section. This variable may have a modifier, in number of hours to add to the time. For example: "<DATE+2:30>".
<TIME>	As above, but with a different output format. The am/pm requirement is possible through the strftime format string.
<TIME24>	As above, but with a different output format.

Example message

An SMS text is:

"Your call to <SERVICE_NUMBER> was sent on <DATE>"

This will appear (at the receiving handset) as:

"Your call to 043345335 was sent on Monday 10th December 2012".

Message tokens

Tokens are searched for in the message text, and replaced with an appropriate value. If the value (at call-time) is null, the token is removed from the message text. The token values are extracted from the ACS engine context, so a value is always expected to be available.

Here is the list of tokens:

Token	Description
<ACCOUNT_ID>	Currently only set if the service control plan was triggered with the CC service library. The format is an integer that is the CCS Account Reference ID (stored in the SMF database).

Token	Description
<ACCOUNT_NUMBER>	The normalized calling or called number. For Messaging Manager triggered service control plans, this is the calling number for XMS_Originating, and the called number for the XMS_Terminating service. For ACS_CB triggered service control plans this is the normalized calling or called number, whichever party is to be billed for the message.
<CALLED_NUMBER>	The unnormalized called number.
<CALLED_PARTY_ID>	Exactly the same as <CALLED_NUMBER>.
<CALLING_NUMBER>	The calling party's MSISDN.
<CALLING_PARTY_ID>	Exactly the same as <CALLING_NUMBER>.
<CALLING_PRIVATE_NETWORK>	Only set for service control plans that are triggered via the VPN service. In this case it will be the calling number in the private network.
<CALL_DURATION>	The current call length (set for example by the ccsATB and ccsUATB nodes).
<CALL_TIME>	Ultimately comes from the SLC time at the start of triggering to ACS. The format is determined by the node configuration for the time format.
<CALL_START_DATE>	Exactly the same as the <CALL_TIME>.
<LOCATION_NUMBER>	The location number from the IDP used to trigger ACS. For Messaging Manager triggered calls this will be the SourceLocationInformation (that is, the originating address).
<LOGICAL_CALLING_NUMBER>	A normalized version of the logical calling number. For Messaging Manager triggered service control plans this will be the MIN or MDN, depending on the switch involved.
<NETWORK_CALLING_NUMBER>	This is the MIN or MDN, depending on the switch.
<NORM_CALLED_NUMBER>	Normalized version of <CALLED_NUMBER>.
<NORM_CALLING_NUMBER>	Normalized version of <CALLING_NUMBER>.
<ORIGINAL_CALLED_NUMBER>	This is the getOriginalCalledPartyID from the IDP, which is the called party number (before any changes made by ACS).
<PIN>	Only available if a prior node in the service control plan has set the PIN (for example, the PIN Authorisation Node).
<PENDING_TERMINATION_NUMBER>	Only available if a termination attempt has previously been made in the current service control plan.

Token	Description
<PROFILE_CHAR_BLOCK*number*_TAG<tag number>> <PROFILE_INT_BLOCK*number*_TAG<tag number>>	Data stored in Profile blocks is retrieved during call processing using one of the profile tag tokens: PROFILE_CHAR_BLOCK - if value is string format PROFILE_INT_BLOCK - if value is an integer The required values are defined as: • *number* is an integer for the block number; • *tag number* is the decimal value of the profile tag. **Example:** <PROFILE_CHAR_BLOCK19_TAG7671818> is replaced by a string value taken from the field with tag 7671818 from profile block 19. For more information about profile blocks, see Profile Block list.
<REDIRECTION_NUMBER>	The redirecting party ID from the IDP used to trigger ACS. For Messaging Manager triggered service control plans, this is the SMSCAddress (DA serviceCentre).
<SERVICE_NUMBER>	The normalized called number (that is, the same as <NORM_CALLED_NUMBER>).
<SMS_TEXT>	The original incoming SMS text message.
<TERMINATION_NUMBER>	Will be set after a node which has attempted termination, for example, the ccsATBNode.
<TERMINATION_PRIVATE_NETWORK>	Will only be set if using the VPN. It is the termination number for the private network.
<USSD_RESPONSE>	Text returned from the Send USSD Message node.

Extra configuration

The Send Short Message Notification feature node requires extra configuration in both of these sections of the **eserv.config** file:

- `macroNodes`
- `Internal` adapter

For more information about these sections, see *MM Technical Guide*.

Send USSD Message

The Send USSD Message node is used to send a message to the USSD application.

Node exits

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Message sent successfully
2	USSD Failure	USSD operation sent, but an error was received from the target system.

Exit	Cause	Description
3	Timeout	USSD operation sent, but no response received from the target system before the timeout period was reached.
4	Node Failure	Node error, the message was not sent.

Configuration fields

This table describes the function of each field in the Configure Send USSD message screen.

Field	Description
Source MSISDN	This section is used to set the number that Messaging Manager pretends to be, for the purposes of sending the USSD operation.
Type	List of numbers contained in the call context.
Nature of Address	Sets the nature of address to be used. This is only available for number types that do not contain a nature of address.
SSN	Subsystem Number to use.
Digits	Used to set the digits. This is only available for the Fixed Address number type.
Target System	This section is used to set the Global Title of the system that the USSD operation is to be sent to.
GT Type	Select the Global Title Type from the list, as specified in the SCCP Q713 standard, section 3.4.2.3. The GT may be defined in any of the following formats: • "1,*noa*,*BCD_address_digits*" • "2,*Trans_Type*,*BCD_address_digits*" • "3,*Trans_Type*,*Num_Plan*,*BCD_address_digits*" • "4,*Trans_Type*,*Num_Plan*,*noa*,*BCD_address_digits*"
Message Template	This field is simply a text field. This field is tokenized when the node is initialized, so that fast construction of the message can be done during message processing. For a list of tokens, see Message tokens. **Note:** Tokens are case sensitive.
Separators	This section determines the separators that are used in the message
USSD Separators	The separators that are to be used in the USSD message. The will be substituted for the Input Separators used.
Input Separators	The separators in the input message that are to be substituted by the USSD Separator.
USSD Terminator	The symbol that is to be placed at the end of the USSD message if the **Add Terminator** check box is selected.

Field	Description
Add Terminator	Select this check box if the USSD Terminator is to be added to the end of USSD messages that do not already contain this symbol.
Timeout	The period in seconds that the node will wait for a response before taking the Timeout branch.

Configuring the node

Follow these steps to edit the Send USSD Message node.

1. Select the **Type** of source address from the list.
2. If you select the type - `Fixed Address`, you need to fill in the **Digits** field. This is a text string representing the sender of the USSD operation. It can be either a telephone number or an alphanumeric address.

   If it contains any characters other than 0-9, it will be regarded as an alphanumeric address and will have TON (Type Of Number) set to alphanumeric, otherwise TON will be set to unknown. NPI (Number Plan Indicator) will always be set to unknown.
3. Set the Global Title of the destination address.

   Depending on the **Type** and **GT Type** selected, other fields in this section will be available, if required.
4. Set the Subsystem Number to the required value in the **SSN** field.
5. Type the text of the message in the **Message** field.

   See Message content for a description of how to construct messages.
6. Add the separators required.
7. Set the timeout period for the node.
8. Click **Save**.

Message content

The **Message** field is a (UTF-8) text field. This field is tokenized when the node is initialized, so that fast construction of the message can be done during message processing. For a list of tokens, see Message content.

Tokens are searched for in the message text, and replaced with an appropriate value. If the value (at call-time) is null, the token is removed from the message text.

The SMS is sent to MM with the specified UTF-8 encoded text, and the desired alphabet set from the Alphabet drop down list.

Warning: Tokens are case sensitive.

Message tokens

Tokens are searched for in the message text, and replaced with an appropriate value. If the value (at call-time) is null, the token is removed from the message text. The token values are extracted from the ACS engine context, so a value is always expected to be available.

Here is the list of tokens:

Token	Description
<ACCOUNT_ID>	Currently only set if the service control plan was triggered with the CC service library. The format is an integer that is the CCS Account Reference ID (stored in the SMF database).
<ACCOUNT_NUMBER>	The normalized calling or called number. For Messaging Manager triggered service control plans, this is the calling number for XMS_Originating, and the called number for the XMS_Terminating service. For ACS_CB triggered service control plans this is the normalized calling or called number, whichever party is to be billed for the message.
<CALLED_NUMBER>	The unnormalized called number.
<CALLED_PARTY_ID>	Exactly the same as <CALLED_NUMBER>.
<CALLING_NUMBER>	The calling party's MSISDN.
<CALLING_PARTY_ID>	Exactly the same as <CALLING_NUMBER>.
<CALLING_PRIVATE_NETWORK>	Only set for service control plans that are triggered via the VPN service. In this case it will be the calling number in the private network.
<CALL_DURATION>	The current call length (set for example by the ccsATB and ccsUATB nodes).
<CALL_TIME>	Ultimately comes from the SLC time at the start of triggering to ACS. The format is determined by the node configuration for the time format.
<CALL_START_DATE>	Exactly the same as the <CALL_TIME>.
<LOCATION_NUMBER>	The location number from the IDP used to trigger ACS. For Messaging Manager triggered calls this will be the SourceLocationInformation (that is, the originating address).
<LOGICAL_CALLING_NUMBER>	A normalized version of the logical calling number. For Messaging Manager triggered service control plans this will be the MIN or MDN, depending on the switch involved.
<NETWORK_CALLING_NUMBER>	This is the MIN or MDN, depending on the switch.
<NORM_CALLED_NUMBER>	Normalized version of <CALLED_NUMBER>.
<NORM_CALLING_NUMBER>	Normalized version of <CALLING_NUMBER>.
<ORIGINAL_CALLED_NUMBER>	This is the getOriginalCalledPartyID from the IDP, which is the called party number (before any changes made by ACS).
<PIN>	Only available if a prior node in the service control plan has set the PIN (for example, the PIN Authorisation Node).
<PENDING_TERMINATION_NUMBER>	Only available if a termination attempt has previously been made in the current service control plan.

Token	Description
<PROFILE_CHAR_BLOCK*number*_TAG<tag number>> <PROFILE_INT_BLOCK*number*_TAG<tag number>>	Data stored in Profile blocks is retrieved during call processing using one of the profile tag tokens: PROFILE_CHAR_BLOCK - if value is string format PROFILE_INT_BLOCK - if value is an integer The required values are defined as: • *number* is an integer for the block number; • *tag number* is the decimal value of the profile tag. **Example:** <PROFILE_CHAR_BLOCK19_TAG7671818> is replaced by a string value taken from the field with tag 7671818 from profile block 19. For more information about profile blocks, see Profile Block list.
<REDIRECTION_NUMBER>	The redirecting party ID from the IDP used to trigger ACS. For Messaging Manager triggered service control plans, this is the SMSCAddress (DA serviceCentre).
<SERVICE_NUMBER>	The normalized called number (that is, the same as <NORM_CALLED_NUMBER>).
<SMS_TEXT>	The original incoming SMS text message.
<TERMINATION_NUMBER>	Will be set after a node which has attempted termination, for example, the ccsATBNode.
<TERMINATION_PRIVATE_NETWORK>	Will only be set if using the VPN. It is the termination number for the private network.
<USSD_RESPONSE>	Text returned from the Send USSD Message node.

Machine environment information

In addition, there is access to some of the machine's environment information, using the following tokens.

Token	Description
<DATE>	The current system time on the SLC (after conversion to GMT). Output format is described in the Configuration section. This variable may have a modifier, in number of hours to add to the time. For example: "<DATE+2:30>".
<TIME>	As above, but with a different output format. The am/pm requirement is possible through the strftime format string.
<TIME24>	As above, but with a different output format.

Example message

An SMS text is:

"Your call to <SERVICE_NUMBER> was sent on <DATE>"

This will appear (at the receiving handset) as:

"Your call to 043345335 was sent on Monday 10th December 2012".

Send USSD Notification

The Send USSD Notification node is used to send a USSD Notification message to the MSC/handset.

Tip: This node is closely related to the Send USSD Message node.

The originator and destination for a message are selectable from one of:

- A fixed number or alpha-numeric address
- Any existing ACS context digit field, including one of:
  - The caller/message originator of the current call or SMS
  - The called party/message destination of the current call or SMS

Note: The node can be used on any service control plan. It needs to be installed with Messaging Manager, but can be used on non-Messaging Manager service plans, and does not require the use of the Messaging Manager service library.

Node exits

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	Message sent successfully.
2	USSD Failure	USSD notification sent, but an error was received from the target system.
3	Timeout	USSD notification sent, but no response received from the target system before the timeout period was reached.
4	Node Failure	Node error, the USSD notification was not sent.

Configuration fields

This table describes the function of each field in the Configure Send USSD Notification node screen.

Field	Description
Target MSISDN	This section is used to set the destination the USSD Notification is to be sent to.
Type	The list of numbers contained in the call context.
Nature of Address	Sets the nature of address to be used. This is only available for number types that do not contain a nature of address.
Digits	Sets the digits for the destination address. This is only available if Type is set to Fixed Address.
Type	The list of numbers used in the call context.

Field	Description
GT Type	Select the Global Title Type from the list, as specified in the SCCP Q.713 standard, section 3.4.2.3.
Translation Type	The translation type for the system which is sending the notification. For more information about valid types, see Q.713.
Number Plan	Number plan for source.
Nature of Address	Sets the nature of address for source. This is only available for number types that do not contain a nature of address.
SSN	Subsystem number for source address.
Digits	Sets the digits for the source address. This is only available if Type is set to Fixed Address.
Message Template	This field is simply a text field. This field is tokenized when the node is initialized, so that fast construction of the message can be done during message processing. For a list of tokens, see Message tokens. **Warning:** Tokens are case sensitive.
Timeout	The period in seconds that the node will wait for a response before taking the Timeout branch.

Configuring the node

Follow these steps to edit the Send USSD Notification node.

1. In the Target MSISDN area, select the type of number the destination address will be from the **Type** drop down list.
2. If you have selected a type which does not set an NOA, select a nature of address from the **Nature of Address** drop down list.
3. If you have selected `Fixed Address` from the **Type** drop down list, enter the address to send the notification to in the **Digits** field. It can be either a telephone number or an alphanumeric address.
4. In the Source System area, select the type of number the source address will be from the **Type** drop down list.

   Depending on the **Type** and **GT Type** selected, other fields in this section will be available, if required.
5. From the **GT Type** drop down list, select the Global Title of the source address.

   For more information about how these GTs are specified, see section 3.4.2.3 in the SCCP Q713 standard.
6. In the **Translation Type** field, enter the translation type for the system which is sending the notification.

   For more information about valid types, see Q7.13.
7. If you have selected Fixed Address or one of the Extension Digits options from the Type drop down list, select a number plan from the **Number Plan** drop down list.
8. If you have selected a type which does not set an NOA, select a nature of address from the **Nature of Address** drop down list.

9. In the **SSN** field, enter the sub system number which will be used to identify MM in sent messages.
10. If you have selected Fixed Address from the Type drop down list, enter the source address in the **Digits** field. This is a text string representing the sender of the USSD notification. It can be either a telephone number or an alphanumeric address.

    If it contains any characters other than 0-9, it will be regarded as an alphanumeric address and will have TON (Type Of Number) set to alphanumeric, otherwise TON will be set to unknown. NPI (Number Plan Indicator) will always be set to unknown.
11. In the **Message Template** field, enter the text of the message.

    See Message content for a description of how to construct messages.

    Tip: If the text (taking into account the length specifier in any PT tokens) exceeds 160 characters, the Save button will be disabled.
12. In the **Timeout** field, set the number of seconds MM will wait for a response from the MSC/handset before taking the Timeout exit.
13. Click **Save**.

Message content

The **Message** field is a (UTF-8) text field. This field is tokenized when the node is initialized, so that fast construction of the message can be done during message processing. For a list of tokens, see Message tokens.

Tokens are searched for in the message text, and replaced with an appropriate value. If the value (at call-time) is null, the token is removed from the message text.

The USSD notification is sent to MM with the specified UTF-8 encoded text.

Warning: Tokens are case sensitive.

Message tokens

Tokens are searched for in the message text, and replaced with an appropriate value. If the value (at call-time) is null, the token is removed from the message text. The token values are extracted from the ACS engine context, so a value is always expected to be available.

Here is the list of tokens:

Token	Description
<ACCOUNT_ID>	Currently only set if the service control plan was triggered with the CC service library. The format is an integer that is the CCS Account Reference ID (stored in the SMF database).
<ACCOUNT_NUMBER>	The normalized calling or called number. For Messaging Manager triggered service control plans, this is the calling number for XMS_Originating, and the called number for the XMS_Terminating service. For ACS_CB triggered service control plans this is the normalized calling or called number, whichever party is to be billed for the message.
<CALLED_NUMBER>	The unnormalized called number.
<CALLED_PARTY_ID>	Exactly the same as <CALLED_NUMBER>.

Token	Description
<CALLING_NUMBER>	The calling party's MSISDN.
<CALLING_PARTY_ID>	Exactly the same as <CALLING_NUMBER>
<CALLING_PRIVATE_NETWORK>	Only set for service control plans that are triggered via the VPN service. In this case it will be the calling number in the private network.
<CALL_DURATION>	The current call length (set for example by the ccsATB and ccsUATB nodes).
<CALL_TIME>	Ultimately comes from the SLC time at the start of triggering to ACS. The format is determined by the node configuration for the time format.
<CALL_START_DATE>	Exactly the same as the <CALL_TIME>
<LOCATION_NUMBER>	The location number from the IDP used to trigger ACS. For Messaging Manager triggered calls this will be the SourceLocationInformation (for example. the originating address).
<LOGICAL_CALLING_NUMBER>	A normalized version of the logical calling number. For Messaging Manager triggered service control plans this will be the MIN or MDN, depending on the switch involved.
<NETWORK_CALLING_NUMBER>	This is the MIN or MDN, depending on the switch.
<NORM_CALLED_NUMBER>	Normalized version of <CALLED_NUMBER>
<NORM_CALLING_NUMBER>	Normalized version of <CALLING_NUMBER>
<ORIGINAL_CALLED_NUMBER>	This is the getOriginalCalledPartyID from the IDP, which is the called party number (before any changes made by ACS).
<PIN>	Only available if a prior node in the service control plan has set the PIN (for example, the PIN Authorisation Node).
<PENDING_TERMINATION_NUMBER>	Only available if a termination attempt has previously been made in the current service control plan.

Token	Description
<PT BLOCK TAG FORMAT>	Data stored in Profile blocks is retrieved during call processing using the profile tag token. **Format:** `<PT blocktagformat[length_limit]>` **Where:** • `block` is an integer which specifies the profile block to use • `tag` is the profile tag to use (specified in decimal) • `format` specifies the format to display the value (for example "I" for integer, "L" for length (time duration), "S" for string), and • `length_limit` is an optional length specifier which limits the number of characters used to display the value. If the profile tag value is greater than this limit, the value will be truncated by removing trailing characters. **Example:** <PT 8 28200002 I5> will be replace by an integer value taken from the field with tag 2820002 in profile block 8 and the displayed value will be 5 characters long. If the profile tag value is greater than 5 characters, the first five characters will be displayed and the rest will be truncated. For more information, see Profile Block list.
<REDIRECTION_NUMBER>	The redirecting party ID from the IDP used to trigger ACS. For Messaging Manager triggered service control plans, this is the SMSCAddress (DA serviceCentre).
<SERVICE_NUMBER>	The normalized called number (for example the same as <NORM_CALLED_NUMBER>).
<TERMINATION_NUMBER>	Will be set after a node which has attempted termination, for example, the ccsATBNode.
<TERMINATION_PRIVATE_NETWORK>	Will only be set if using the VPN. It is the termination number for the private network.

Profile Block list

Here are the profile blocks accessible using the <PT> message token.

Name	Integer	Description
VPN Network Profile	1	Contains most of the information you can specify in the VPN edit network, for example: • Account Code maximum length • Outgoing barred/allowed list type • Incoming barred/allowed list type • VPN network SD no check • VPN present private address **Note:** Only relevant if you have the VPN service installed.

Name	Integer	Description
VPN Station Profile	2	Contains most of the information you can specify in the VPN edit station, for example: • Outgoing barred/allowed list type • Incoming barred/allowed list type • VPN bar all incoming • VPN bar off network incoming **Note:** Only relevant if you have the VPN service installed.
Customer Profile	3	Contains customer information, for example: • Incoming barred/allowed list type • Incoming barred/allowed list • PIN rights • Default language • Incoming barred/allowed ignore • Termination number ranges • Termination number range policy
Control Plan Profile	4	This profile contains current switch node exits only.
Global Profile	5	Contains global information, for example: • PIN rights • Multi-lingual announcements • Default language • Control plan version hiding
CLI Subscriber Profile	6	Contains most of the information you can specify in the **CLI** tab of the Numbers screen, for example: • Account code • Language • Follow me number **Note:** Only relevant to the 0800 service.
Service Number Profile	7	Contains most of the information you can specify in the **Service Number** tab of the Numbers screen, for example: • Account code • Language • Follow me number **Note:** Only relevant to the 0800 service.

Name	Integer	Description
App Specific Profile 1 App Specific Profile 2 App Specific Profile 3 App Specific Profile 4 App Specific Profile 5 App Specific Profile 6 App Specific Profile 7 App Specific Profile 8	8 9 10 11 12 13 14 15	Contains information specific to an application, for example, Messaging Manager. **Note:** Unless it is in use by a specific application, these profiles (for example, App Specific Profile 7 can be specified as a temporary profile (where nothing is written back to the database) in order to pass information from one application to another, for example between USSD and DAP).
Any Valid Profile	16	Allows you to search for tags in all profiles that have been loaded.

MOX tokens

MOX tokens are only available in some circumstances. A MOX request of the appropriate type must have been sent as the last MOX message. Also, the beServer that replied to this MOX message must be of a type that fills out the requested information (for example, balances are not available in some VWS protocols).

Token	Description
<MOX_BALANCE*n*>	Only available if the last message received from the BeClient was a RetrieveSubscriberProfileRes. Some service libraries (for example, ACS_CB) perform this on triggering to ACS; Messaging Manager does not. For MM the RSINode should be placed immediately before the SSMNode to ensure an RSP is available.
<MOX_CURRENCY*n*>	Only available if the last message received from the BeClient was a RetrieveSubscriberProfileRes. Some service libraries (for example, ACS_CB) perform this on triggering to ACS; Messaging Manager does not. For MM the RSINode should be placed immediately before the SSMNode to ensure an RSP is available.
<MOX_CALL_COST*n*>	Only available if there is a DebitUnitReq ready to send to the BeClient. This is only true if the last node using MOX was an attempt terminate with Billing (for example, cbATBNode or xmsADPBNode). The number format has two decimal places (for example, 19.19, 19.00), followed by the unit (which comes from the configured unit mappings).
<MOX_VOUCHER_NUMBER>	Only available if the last message received from the BeClient was a VoucherReserveRes. Currently, there are no call plan nodes that perform this so this token is unavailable.
<MOX_VOUCHER_REDEEMED_DATE>	Only available if the last message received from the BeClient was a VoucherReserveRes. Currently, there are no call plan nodes that perform this so this token is unavailable.

Token	Description
<MOX_VOUCHER_AMOUNT*n*>	Only available if the last message received from the BeClient was a VoucherReserveRes. Currently, there are no call plan nodes that perform this so this token is unavailable.
<MOX_VOUCHER_RECHARGE_ACCOUNT_TO_CREDIT>	Only available if the last message received from the BeClient was a VoucherReserveRes. Currently, there are no call plan nodes that perform this so this token is unavailable.
<MOX_VOUCHER_RECHARGE_REDEEMING_ACCOUNT>	Only available if the last message received from the BeClient was a VoucherReserveRes. Currently, there are no call plan nodes that perform this so this token is unavailable.
<MOX_CALL_START_DATE>	Only available if there is a DebitUnitReq ready to send to the BeClient. This is only true if the last node using MOX was an Attempt Terminate with Billing (for example, cbATBNode or xmsADPBNode). This time value is the same as <CALL_TIME>. The format (expressed using the time configuration format for this node) is "%G-%m-%d %T0".
<MOX_CALL_ANSWER_DATE>	Only available if there is a DebitUnitReq ready to send to the BeClient. This is only true if the last node using MOX was the cbATBNode. This is the attemptTerminateResultTime. The format is the same as for <MOX_CALL_START_DATE>, that is, "%G-%m-%d %T0".
<MOX_REDIRECTION_NUMBER>	The cbContext.normRedirectionNumber. This is the ctd_redirection_num and only available if the call plan was triggered with the ACS_CB service library.

Note: Replace the *n* in the token with the index of a balance. For example, to retrieve the first balance in a set use <MOX_BALANCE0>.

Machine environment information

In addition, there is access to some of the machine's environment information, using the following tokens.

Token	Description
<DATE>	The current system time on the SLC (after conversion to GMT). Output format is described in the Configuration section. This variable may have a modifier, in number of hours to add to the time. For example: "<DATE+2:30>".
<TIME>	As above, but with a different output format. The am/pm requirement is possible through the strftime format string.
<TIME24>	As above, but with a different output format.

Example notification

A USSD notification text is:

"Your call to <SERVICE_NUMBER> was sent on <DATE>"

This will appear (at the receiving handset) as:

"Your call to 043345335 was sent on Monday 10th December 2012".

Extra configuration

The Send USSD Notification node requires extra configuration in the `macroNodes` section in the **eserv.config** file. For more information, see Send Short Message configuration.

Set Message Routing

The Set Message Routing node allows a control plan to set routing parameters which determine the routing rule to use, and hence guides outbound path selection.

Node exits

This node has one entry and one exit. The number of exits cannot be changed.

Exit	Cause	Description
1	Message Routing Set	Message has had the new routing attributes applied.

Configuring the node

Follow these steps to edit the node.

1. To set the routing class for the message:
   - Select the **Leave Unchanged** check box
   - Select the **New Routing Class** to use from the drop-down list
2. To set the destination domain for the message:
   - Deselect the **Leave Unchanged** check box
   - Enter the name of the Domain that the Destination is to be set to in the **New Domain** field.

   Note: This must be an exact match with a Messaging Manager domain name.
3. To set the originating domain for the message:
   - Deselect the **Leave Unchanged** check box
   - Enter the name of the Domain that the Origination is to be set to in the **New Domain** field.

   Note: This must be an exact match with a Messaging Manager domain name.
4. To set the message centre for the message:
   - Deselect the **Leave Unchanged** check box
   - Enter the name of the Message Center that is to be set for the message in the **New Message Centre** field.

   Note: This must be an exact match with a Messaging Manager Message Center name.

5. Click **Save**.

Set Originating Address

The Set Originating Address node allows you to set the originating address for all messages that pass through the node to the address specified in the node.

Node exits

This node has one entry and one exit. The number of exits cannot be changed.

Exit	Cause	Description
1	Address Set	The originating address for the message has been set to the specified value.

Configuring the node

Follow these steps to edit the node.

1. Enter the address that all messages passing through the node will have set as their originating address. This field will accept numeric values, as well as the * and # symbols.
2. Click **Save**.

8

XMS Parameters Feature Nodes

This chapter describes the Oracle Communications Network Charging and Control (NCC) Messaging Manager XMS Parameters feature nodes.

This chapter contains the following topics.

Alphabet Branching

The Alphabet Branching node determines if the message text is using the alphabet specified in this node and branches accordingly.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Match	The message uses the current alphabet specified.
2	No Match	The message does not use the current alphabet specified.

Configuring the node

Follow these steps to configure the node.

1. Select the alphabet to compare the message against from the **Alphabet** drop down list.
2. Click **Save**.

Content Size Branching

The Content Size Branching node branches depending on the size of the short message (in bytes). It takes the threshold entered into the node and chooses either the small or large branch.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Small Message	The message is smaller than the specified number of bytes.
2	Large Message	The message is equal to, or larger than the specified number of bytes.

Configuring the node

Follow these steps to edit the node.

1. Specify the message size threshold, in number of bytes.
2. If you select the **Include Header** check box, then the length of the user data header is included in the message length.
3. Click **Save**.

Message Attribute Branching

Branches on the value of a message attribute. Branching is based on the result of a logical comparison between a value and the value in the corresponding message attribute.

Node exits

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Less Than	The value in the message is lower than the value configured in the node.
2	Equals	The value in the message is the same as the value configured in the node.
3	Greater Than	The value in the message is greater than the value configured in the node.
4	Not Found	An error occurred during the comparison.

Note: Strings are evaluated against ASCII order, on a character-by-character basis starting with the left-hand character.

Configuring the node

Follow these steps to configure the node.

1. Configure this record by entering data in the fields on the Configure Set Message Attribute screen.

For more information about the fields on this screen, see Configuration fields.

2. Click **Save**.

Configuration fields

This table describes the function of each field.

Field	Description
Attribute	The message attribute to compare.
Value Type	The type of value the attribute will be compared with.
Fixed	The value the message attribute will be compared with. **Note:** This field is only available if the **Value Type** field is set to `Fixed`.
Enumerated	The value the message attribute will be compared with. **Notes:** • This field is only available if the **Value Type** field is set to `Enum`. • The drop list is populated by the application. The available options cannot be changed. For more information about the available values, see Enumerated fields.
Source Location	The profile block which stores the value the message attribute will be compared with. **Notes:** • This field is only available if the **Value Type** field is set to `Profile`. • The drop down list is populated by the records on the **Profile Tag Details** tab of the ACS Configuration screen.
Source Field	The profile field which stores the value the message attribute will be compared with. **Notes:** • This field is only available if the **Value Type** field is set to `Profile`. • The drop down list is populated by the records on the **Profile Tag Details** tab of the ACS Configuration screen. The available profile fields are dependant on the profile selected in the **Source Location** drop down list.

Enumerated fields

This table describes the list of enumerated values which are available to the Message Attribute nodes.

Group Name	Value	Description
ATTRIBUTE	SRR	Status report (delivery receipt) request
ATTRIBUTE	RRR	Read-reply report request

Group Name	Value	Description
ATTRIBUTE	SMS_CLASS	SMS Message class
ATTRIBUTE	MW_TYPE	Message waiting type
ATTRIBUTE	MW_SENSE	Message waiting sense
ATTRIBUTE	MW_GROUP	Message waiting group
ATTRIBUTE	PRIORITY	NA
ATTRIBUTE	SINGLE_SHOT	Single-shot
ATTRIBUTE	RECIPIENTS	Number of recipients
ATTRIBUTE	RECIPIENT	Current recipient
ATTRIBUTE	SIZE	Message size
ATTRIBUTE	MMS_CLASS	MMS message class
ATTRIBUTE	ADAPTATION	Content adaptation
ATTRIBUTE	TIME_ZONE	NA
ATTRIBUTE	SERVICE_CODE	NA
ATTRIBUTE	BILLING_INFO	Billing Identifier
ATTRIBUTE	VP_TYPE	Validity Period Type
ATTRIBUTE	VALIDITY	Validity Period
ATTRIBUTE	MESSAGE_TYPE	NA
ATTRIBUTE	CHARGED_PARTY	NA
ATTRIBUTE	VAS_ID	NA
ATTRIBUTE	VASP_ID	NA
SRR	0	None requested
SRR	1	SME requested
SRR	2	MMX requested
SRR	3	Both requested
RRR	0	Not requested
RRR	1	Requested
SMS_CLASS	0	None
SMS_CLASS	1	Display (GSM 0)
SMS_CLASS	2	Mobile Equipment (GSM 1)
SMS_CLASS	3	SIM (GSM 2)
SMS_CLASS	4	External (GSM 3)
MW_TYPE	0	None
MW_TYPE	1	Voicemail
MW_TYPE	2	Fax
MW_TYPE	3	Email
MW_TYPE	4	Other
MW_SENSE	0	Inactive
MW_SENSE	1	Active
MW_GROUP	0	None
MW_GROUP	1	Discard
MW_GROUP	2	Store
PRIORITY	0	Normal
PRIORITY	1	Interactive
PRIORITY	2	Urgent
PRIORITY	3	Emergency

Group Name	Value	Description
SINGLE_SHOT	0	False
SINGLE_SHOT	1	True
MMS_CLASS	0	None
MMS_CLASS	1	Personal
MMS_CLASS	2	Advert
MMS_CLASS	3	Info
MMS_CLASS	4	Auto
ADAPTATION	0	False
ADAPTATION	1	True
VP_TYPE	0	Relative
VP_TYPE	1	Absolute
MESSAGE_TYPE	0	Submit
CHARGED_PARTY	0	Neither
CHARGED_PARTY	1	Sender
CHARGED_PARTY	2	Recipient
CHARGED_PARTY	3	Both
CHARGED_PARTY	0	`*/*`
CHARGED_PARTY	1	`text/*`
CHARGED_PARTY	...	NA

Segment Number Branching

The Segment Number Branching node branches, depending on if the current message is the last (or only) component in a concatenated, multi-part, message. It compares the current segment number with the total number of segments and takes the appropriate exit.

Node exits

This node has one entry and four exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Only Segment	The message contains only one segment.
2	First Segment	There is more than one segment in the message and the segment number is one.
3	Middle Segment	There is more than one segment in the message and the segment number does not match the number of segments.
4	Last Segment	There is more than one segment in the message and the segment number matches the number of segments.

Configuring the node

This node requires no configuration data. You may change the **Node name**, if required.

Set Data Coding

The Set Data Coding node sets the character set of the message to be used when the ACS Control Plan passes the message on to Messaging Manager for delivery.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The configured alphabet has been successfully selected. **Note:** The Set Data Coding node does not change the data coding in ACS, but it does define the data coding used when the message is returned to Messaging Manager. This occurs when the message is actually ready to be sent. Consequently, the TP-DCS known to ACS in the Control Plan is still the original TP-DCS, and its value does not change when leaving this node through the Success branch.
2	Failure	General error occurred.

Configuring the node

Follow these steps to edit the node configuration.

1. Select the message alphabet from the **Alphabet** drop down list.
2. Click **Save**.

Set Message Attribute

Allows the modification various attributes of the message data by overriding the options requested by a caller.

To set a message's time zone to the time zone of the user, see Set Time Zone Message Attribute.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The specified attribute was set successfully.
2	Failure	The node failed to change the specified attribute.

Configuring the node

Follow these steps to configure the node.

1. Configure this record by entering data in the fields on the Configure Set Message Attribute screen.

   For more information about the fields on this screen, see Configuration fields.

2. Click **Save**.

Configuration fields

This table describes the function of each field.

Field	Description
Attribute	The message attribute to compare.
Value Type	The type of value the attribute will be compared with.
Fixed	The value the message attribute will be compared with. **Note:** This field is only available if the **Value Type** field is set to `Fixed`.
Enumerated	The value the message attribute will be compared with. **Notes:** • This field is only available if the **Value Type** field is set to `Enum`. • The drop list is populated by the application. The available options cannot be changed. For more information about the available values, see Enumerated fields.
Source Location	The profile block which stores the value the message attribute will be compared with. **Notes:** • This field is only available if the **Value Type** field is set to `Profile`. • The drop down list is populated by the records on the **Profile Tag Details** tab of the ACS Configuration screen.

Field	Description
Source Field	The profile field which stores the value the message attribute will be compared with. **Notes:** • This field is only available if the **Value Type** field is set to `Profile`. • The drop down list is populated by the records on the **Profile Tag Details** tab of the ACS Configuration screen. The available profile fields are dependant on the profile selected in the **Source Location** drop down list.

Set Time Zone Message Attribute

Sets the message time zone attribute to the user's time zone.

To set other message attributes, see Set Message Attribute.

To branch on message attributes (including time zone), see Message Attribute Branching.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Success	The time zone was set successfully.
2	Failure	An error occurred and the time zone was not set.

Configuring the node

Follow these steps to configure the node.

1. Configure this record by entering data in the fields on the Configure Set Time Zone Message Attribute screen.

   For more information about the fields on this screen, see Configuration fields.

2. Click **Save**.

Configuration fields

This table describes the function of each field.

Field	Description
Timezone Type	The source of the timezone value.
Unix Timezone	The timezone to use from the standard unix timezone set. **Note:** This field is only available if **Timezone Type** is set to `Explicit Unix TZ`.

Test Data Coding

The Test Data Coding node checks the message for compatibility with the specified (in this node) destination alphabet.

This node is used to determine if the message can be converted to the specified alphabet. If not then the control plan can be set to compare against another alphabet in another instance of this mode.

Node exits

This node has one entry and two exits. The number of exits cannot be changed.

Exit	Cause	Description
1	Pass	The message will be convertible to the destination alphabet with less than or equal to the allowed character conversion failures.
2	Fail	The message will not be converted to the destination alphabet without incurring more than the allowed character conversion failures.

Configuring the node

Follow these steps to edit the node configuration.

1. Select the destination alphabet for the message to be converted to from the **Alphabet** drop down list.
2. Enter the maximum number of characters that cannot be converted to the destination alphabet before failing the conversion test in the **Misses Allowed** field.
3. Click **Save**.