Oracle® Communications Diameter Signaling Router

SS7/Sigtran User's Guide

E57512 Revision 01

March 2015

ORACLE®

Oracle® Communications SS7/Sigtran User's Guide

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter includes sections on the purpose, scope, audience, and organization of this guide; how to contact Oracle for assistance; and how to locate product documentation on the Oracle Customer Support site..

Purpose of this Manual

This content:

- Gives a conceptual overview of the application's purpose, architecture, and functionality
- Describes the pages and fields on the application GUI (Graphical User Interface)
- Provides procedures for using the application interface
- Explains the organization of, and how to use, the documentation

Scope and Audience

This guide is intended for trained and qualified system operators and administrators who are responsible for managing an SS7/Sigtran system.

Manual Organization

This manual is organized into the following chapters:

- *Introduction* contains general information about the *SS7/Sigtran User 's Guide*, the scope, audience, and organization of this manual, and how to contact Oracle for assistance.
- *User Interface Introduction* describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.
- *SS7 configuration* describes the GUI pages and procedures for viewing SS7 network status, and for performing configuration and maintenance tasks.
- *SS7 maintenance* describes the SS7 maintenance menu, which provides maintenance and troubleshooting capabilities on Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, Links, and Associations.
- *Command Line Interface* describes a method for bulk loading SS7 configuration data and for validating and executing command scripts.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
	**Danger**: (This icon and text indicate the possibility of *personal injury*.)
	**Warning**: (This icon and text indicate the possibility of *equipment damage*.)
	**Caution**: (This icon and text indicate the possibility of *service interruption*.)
	**Topple**: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the **Applications** tile.
   The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability

- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Chapter 2

User Interface Introduction

Topics:

This section describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction with an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

DSR GUI

In a DSR, the following Main Menu options are accessible from the System OAM (SOAM) server:

- Transport Manager
- Communication Agent
- SS7/Sigtran
- Diameter Common
- Diameter
- RBAR
- FABR
- Policy and Charging
- IPFE
- MAP-Diameter IWF
- CPA

The following Main Menu options are accessible from the Network OAM (NOAM) server:

- Communication Agent
- Diameter Common > Network Identifiers > MCCMNC, MCCMNC Mapping
- Diameter > Configuration for Topology Hiding,
- Network-wide Policy and Charging > Configuration components are configurable on the NOAM; some Configuration components are view-only on the SOAM. Policy and Charging > Maintenance components are accessible on the NOAM only.
- MAP-Diameter IWF

Bulk Import and Bulk Export functions appear on both OAMs, to be used for the data that can be configured on that OAM.

Most other Main Menu options are configurable from the Network OAM server and view-only from the System OAM server.

User Interface Elements

Table 2: User interface elements describes elements of the user interface.

Table 2: User interface elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.

Element	Location	Function
Session Banner	Next bar across the top of the web page	The left side of the banner just above the Main Menu provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner: • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates that a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • **Page Title Area**: Occupies the top of the work area. It displays the title of the current page being displayed, the date and time, and includes a link to context-sensitive help. • **Page Control Area**: Is located below the Page Title Area, and is used to show controls for the Page Area (this area is optional). When available for an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • **Page Area**: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is

Element	Location	Function
		provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Splash Page Welcome Message*.

Main Menu Options

Table 3: Main Menu Options describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options would not appear on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the NOAM and view-only on the SOAM; and some menu options are configurable only on the SOAM. See *DSR GUI*.

Note: Some features will not appear in the main menu until the features are activated.

Table 3: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Manage licenses and upgrades • Authenticate LDAP servers • Configure SNMP trapping services • Validate and transfer ISO files • Prepare, initiate, monitor, and complete upgrades • View the software versions report • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes

Menu Item	Function
	• Services • Servers • Server Groups • Resource Domains • Places • Place Associations On the SOAM, allows the user to configure the NOAM list plus Interface and Port DSCP.
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status & Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, and data file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager	Allows the user to configure adjacent nodes, configuration sets, or transports; and edit transports.
Communication Agent	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	Allows the user to configure various users, groups, remote signaling points, links and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data.
Diameter Common	Allows the user to configure: • Network Identifiers: on the NOAM - MCC Ranges • Network Identifiers on the SOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile assignments The DSR Bulk Import and Export functions are available on both OAMs for the data that is configured on that OAM.
Diameter	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAM, Diameter Topology Hiding configuration

Menu Item	Function
	• On the SOAM, Diameter Configuration, AVP Dictionary and Troubleshooting for IDIH configuration; Diameter Mediation configuration: and Maintenance functions
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only.

Policy and Charging
(optional)
	On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRF Pools
	  • PCRF Sub-Pool Selection Rules
	  • Network-Wide Options
	• Online Charging DRA
	  • OCS Session State
	  • Realms
	  • Network-Wide Options
	• Alarm Settings
	• Congestion Options
	On the NOAM, allows the user to perform maintenance tasks, edit options, and view elements for:
	• Maintenance
	  • SBR Status

Menu Item	Function

	• Policy Database Query
	
	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRFs
	  • Binding Key Priority
	  • PCRF Pools
	  • PCRF Pool to PRT Mapping
	  • PCRF Sub-Pool Selections
	  • Policy Clients
	  • Site Options
	• Online Charging DRA
	  • OCSs
	  • CTFs
	  • OCS Session State
	  • Realms
	• Error Codes
	• Alarm Settings
	• Congestion Options

Gateway Location Application (Optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP).
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only.
MAP-Diameter Interworking	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application: • MD-IWF Options • Diameter Realm

Menu Item	Function
	• Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping
CPA (Charging Proxy Application) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • System Options • Message Copy • Session Binding Repository • SBR Subresource Mapping This is accessible from the SOAM only.
Help	Launches the Help system for the user interface.
Logout	Allows the user to log out of the user interface.

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the **Group Administration** page. The default group, **admin**, is permitted access to all GUI options and functionality. Additionally, members of the **admin** group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options will not appear on your screen if you do not have administrative permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing a password upon login. The System Login page also features a current date and time stamp and a customizable login message.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request.

Customizing the Login Message

Prior to logging in, the **System Login** page appears. You can create a login message that will appear just below the **Log In** button on the **System Login** page.

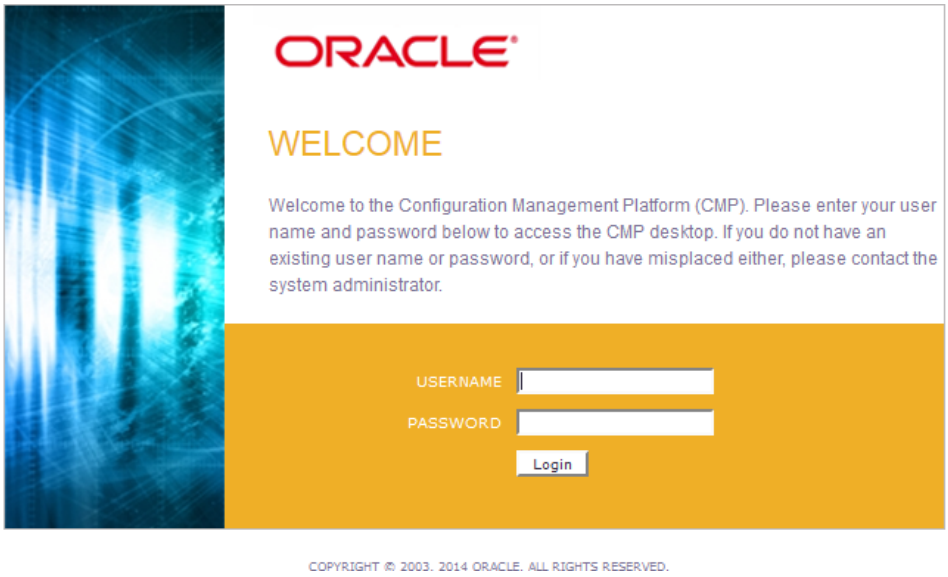


Figure 1: Oracle System Login

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.

   A status message appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the login message text is displayed.

Accessing the DSR Graphical User Interface

In a DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you will access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM** > **Administration** > **Access Control > Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example https://dsr-no.yourcompany.com.

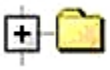
   When using Single Sign-On, you cannot use the IP address of the server.
2. When prompted by the browser, confirm that the server can be trusted.
   The System Login page appears.
3. Enter the Username and Password for your account.
   The DSR GUI for the NOAM appears.
4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.
   The DSR GUI for the SOAM appears.

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the **Main Menu**.

Table 4: Main Menu icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) will collapse the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.

Icon	Name	Description
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, you will see a variety of page formats. Tables, forms, tabbed pages, and reports are the most common formats in the user interface.

Note: Screenshots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination, with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see *Page Controls*.

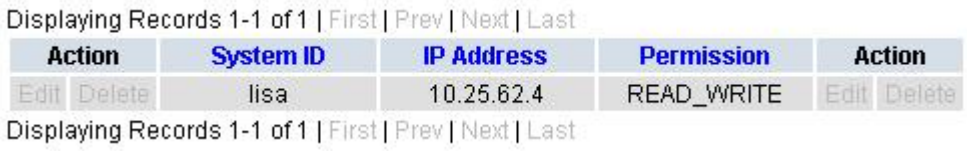
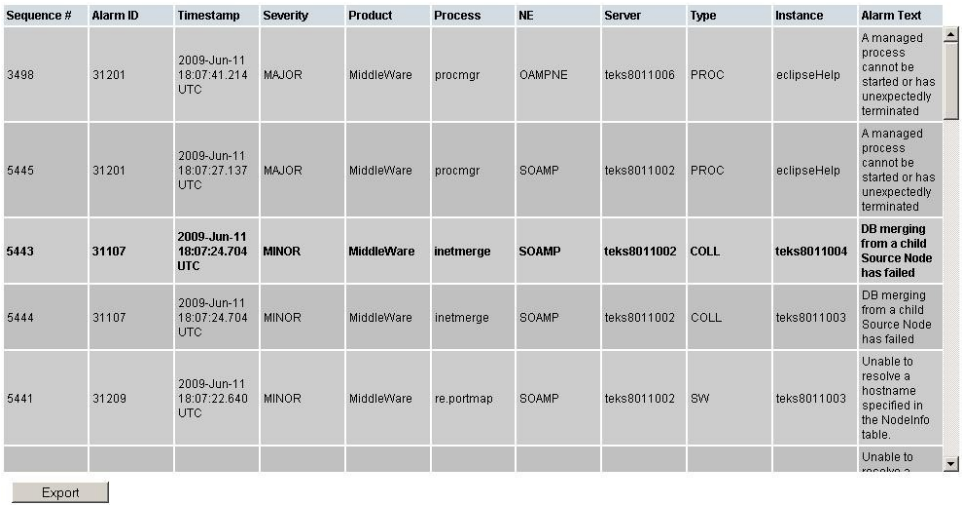


Figure 2: Paginated table

Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see *Page Controls*.



Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	MiddleWare	procmgr	SOAMP	teks8011002	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5443	**31107**	**2009-Jun-11 18:07:24.704 UTC**	**MINOR**	**MiddleWare**	**inetmerge**	**SOAMP**	**teks8011002**	**COLL**	**teks8011004**	**DB merging from a child Source Node has failed**
5444	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011003	DB merging from a child Source Node has failed
5441	31209	2009-Jun-11 18:07:22.640 UTC	MINOR	MiddleWare	re.portmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the NodeInfo table.
										Unable to

Export

Figure 3: Scrollable table

Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of pulldown lists, buttons and links.

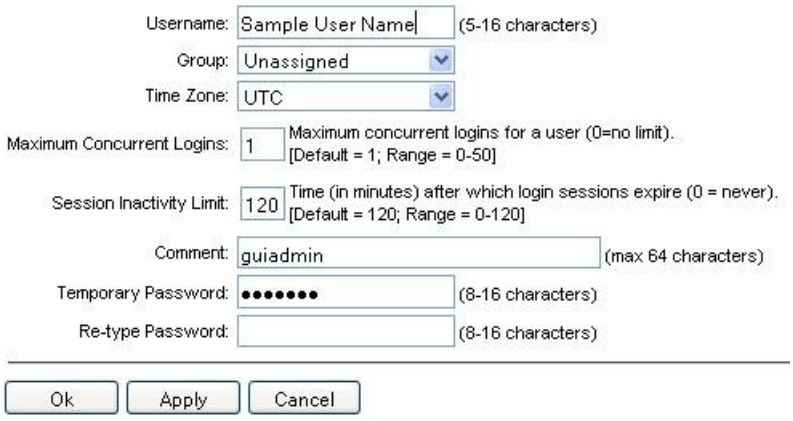


Figure 4: Form page

Tabbed pages

Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields will populate on the page. Retrieve is always the default for tabbed pages.

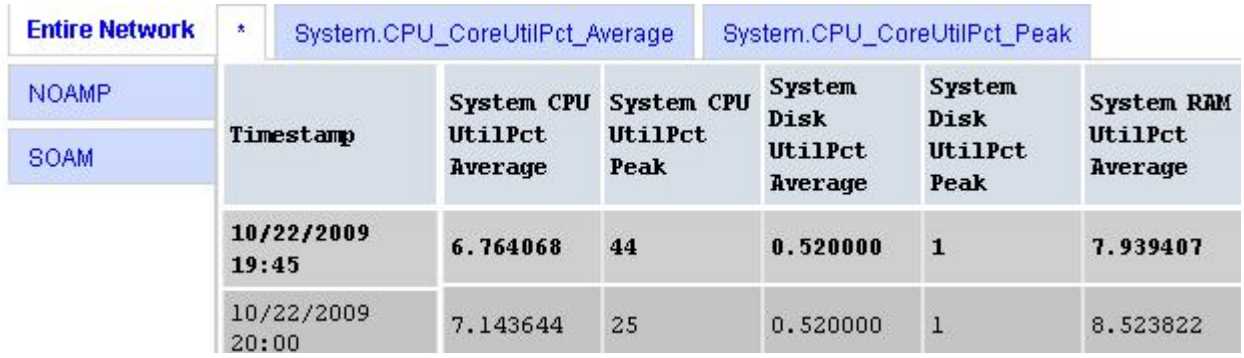


Figure 5: Tabbed pages

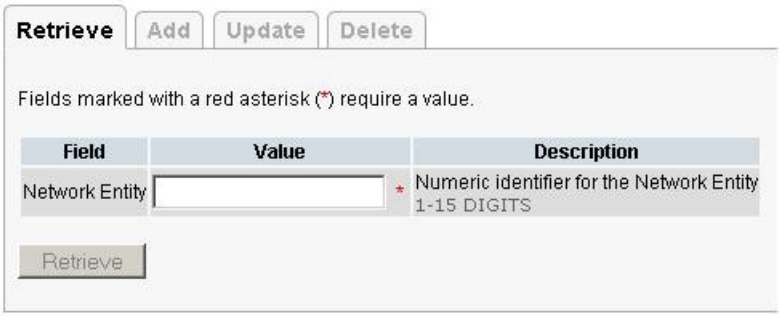


Figure 6: Tabbed pages

Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking the **Report** button. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

```
================================================================================

User Account Usage Report

================================================================================

Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiadmin

--------------------------------------------------------------------------------

Username          Date of Last Login    Days Since Last Login   Account Status
----------------  --------------------  ----------------------  ---------------
guiadmin          2009-06-19 19:00:17   0                       enabled

--------------------------------------------------------------------------------

End of User Account Usage Report

================================================================================
```

Figure 7: Report output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the **User Interface** splash page appears. You can display a customized welcome message on the **User Interface** splash page. Use this procedure to customize the message.

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Locate **WelcomeMessage** in the **Variable** column.
3. Enter the welcome message text in the **Value** column.
4. Click **Update OK** or **Apply** to submit the information.

   A status message appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the welcome message text is displayed.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See *Figure 8: Sorting a Table by Column Header*. Clicking the column header again reverses the direction of the sort.

Local Node Name ▾	Realm	FQDN	SCTP Listen Port	TCP Listen Port	Connection Configuration Set	CEX Configuration Set	IP Addresses

Figure 8: Sorting a Table by Column Header

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in **Group Administration**, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

Table 5: Example Action buttons contains examples of Action buttons.

Table 5: Example Action buttons

Action button	Function
Insert	Insert data into a table
Edit	Edit data within a table
Delete	Delete data from table
Change	Change the status of a managed object

Some Action buttons take you to another page.

Submit buttons, described in *Table 6: Submit buttons*, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 6: Submit buttons

Submit button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control is a widget that allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

Click the **X** next to a pulldown list to clear the field.

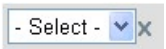


Figure 9: Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar appears in the Page Control Area of the GUI.

Figure 10: Optional Layout Element Toolbar

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear include:

- Filter - Allows you to filter data in a table.
- Errors - Displays errors associated with the work area.
- Info - Displays information messages associated with the work area.
- Status - Displays short status updates associated with the main work area.
- Warning - Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

Figure 11: Automatic Error Notification

Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.
   The selected element opens and overlays the work area.
2. Click **X** to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see *Optional Layout Element Toolbar*.

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element - When enabled, the Network Element filter limits the data viewed to a single Network Element.

  Note: Once enabled, the Network Element filter will affect all pages that list or display data relating to the Network Element.

- Collection Interval - When enabled, the collection interval filter limits the data to entries collected in a specified time range.
- Display Filter - The display filter limits the data viewed to data matching the specified criteria.

Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

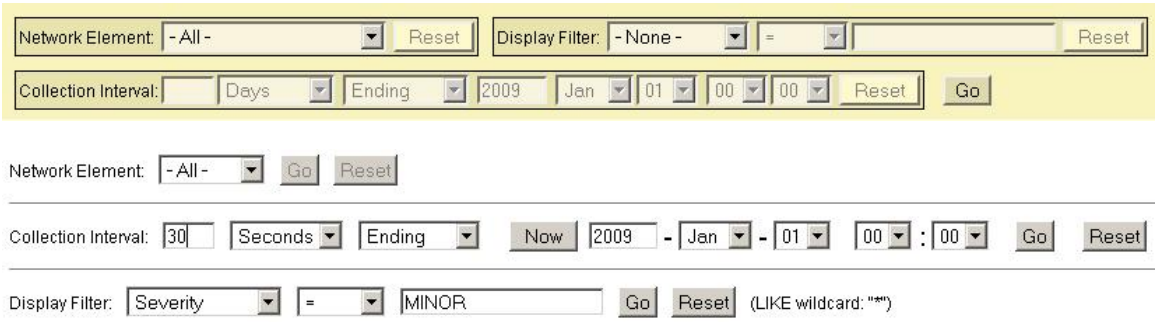


Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter control elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.

Operator	Description
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators will be available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Enter a duration for the **Collection Interval** filter.
   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.
   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes that you have a data table displayed on your screen. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Click **Filter** in the optional layout element toolbar.

The filter tool appears.

2. Select a field name from the **Display Filter** pulldown menu.

   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

   The selected field name displays in the **Display Filter** field.

3. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.

4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (**=**) operator and a value of MINOR, the table would show only records where Severity=MINOR.

5. For data tables that support compound filtering, click the **Add** button to add another filter condition. Then repeat steps 2 through 4.
   Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, select **Administration > General Options**.

   The **General Options Administration** page appears.

2. Change the value of the **MaxRecordsPerPage** variable.

   Note: MaxRecordsPerPage has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Chapter 3

SS7 configuration

Topics:

SS7/Sigtran provides the Signaling Network Interface for the MD-IWF SS7 Application. The interface supports standards-based M3UA, MTP3, and SCCP signaling.

This chapter describes GUI pages and procedures for viewing SS7 network status and performing configuration and maintenance tasks for he Signaling Network Interface for the MD-IWF SS7 Application.

SS7 network configuration overview

The **SS7/Sigtran > Configuration** GUI pages are used to configure the SS7 networking. Each Configuration menu item aligns with an SS7 network configuration task. The items appear on the menu in the order that SS7 configuration must be performed. This section explains the use of the Configuration items.

Any fields that require unique data for SS7/Sigtran configuration must be unique within the site but not across sites.

Table 8: High-level Overview of SS7 Configuration provides a high-level view of the SS7 network configuration and identifies the menu item that supports each task.

To bulk-load configuration data, see *Command Line Interface*.

If you are unfamiliar with any of the network components in the table, use the links provided or consult the Glossary.

Table 8: High-level Overview of SS7 Configuration

#	Task	Menu Option
1	Create signaling Network Element.	**Configuration > Network Elements**
2	Add MP and SOAM servers to the signaling Network Element.	**Configuration > Servers**
3	Create server groups for the MP servers.	**Configuration > Server Groups**
4	Configure Transport Manager • Adjacent Nodes, for use as Adjacent Server Members in SS7/Sigtran Adjacent Server Groups configuration • Transports (and Transport Configuration Sets if needed), for selection as Associations in SS7/Sigtran configuration.	**Transport Manager > Configuration >Adjacent Node** **Transport Manager > Configuration > Configuration Sets** **Transport Manager > Configuration > Transports**
5	Create Adjacent Server Groups for each IP Signaling point that the SS7 application will connect to. An example would be the EAGLE IP Signaling Gateway.	**SS7/Sigtran > Configuration > Adjacent Server Groups** (see *Adjacent Server Groups*)
6	Create Local Signaling Points for each point code that identifies an MP server for theSS7 application.	**SS7/Sigtran > Configuration > Local Signaling Points** (see *Local Signaling Points*)
7	Create a Local SCCP User for each SS7 application hosted by SS7-MP servers.	**SS7/Sigtran > Configuration > Local SCCP Users** (see *Local SCCP Users*).
8	Create remote signaling points for each adjacent signaling point that the SS7 application will connect to and each remote	**SS7/Sigtran > Configuration > Remote Signaling Points** (see *Remote Signaling Points*)

#	Task	Menu Option
	destination that the SS7 application will route messages to.	
9	Create Remote MTP3 Users for each Subsystem Number that the SS7 application will route messages to.	**SS7/Sigtran > Configuration > Remote MTP3 Users** (see *Remote MTP3 Users Maintenance*)
10	Create a Link Set for each LSP and for each Adjacent RSP.	**SS7/Sigtran > Configuration > Link Sets** (see *Link Sets*)
11	Create Links that reference each Association and Link Set.	**SS7/Sigtran > Configuration > Links** (see *Links*)
12	Create routes for each RSP and link set.	**SS7/Sigtran > Configuration > Routes** (see *Routes*)
13	Edit the SCCP, MTP3, and M3UA options as desired.	**SS7/Sigtran > Configuration > SCCP Options** (see *SCCP Options*) **SS7/Sigtran > Configuration > MTP3 Options** (see *MTP3 Options*) **SS7/Sigtran > Configuration > M3UA Options** (see *M3UA Options*)
14	Enable the LSUs.	**SS7/Sigtran > Maintenance > Local SCCP Users** (see *Local SCCP Users Maintenance*)
15	Enable the Links.	**SS7/Sigtran > Maintenance > Links** (see *Link Maintenance*)

Adjacent Server Groups

An Adjacent Server Group is a collection of Adjacent Servers that implements a distributed IP signaling function. The group represents a set of Adjacent Nodes that share a Point Code on the Signaling Gateway.

Note: "Adjacent Servers" are configured as "Adjacent Nodes" on the **Transport Manager > Configuration > Adjacent Node** pages.

An adjacent Remote Signaling Point (RSP) is associated with one Adjacent Server Group.

On the **Adjacent Server Groups** page, Adjacent Servers can be grouped that belong to the same Signaling Gateway. For example, an Adjacent Server Group can refer to an EAGLE STP with which this application is associated.

Adjacent Server Groups elements

Table 9: Adjacent Server Groups Elements describes the information on the **SS7/Sigtran > Configuration > Adjacent Server Groups** page. Data Input Notes apply only on the Insert and Edit pages.

Table 9: Adjacent Server Groups Elements

Element (* indicates a required files)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element to which the Adjacent Server Group is being added.	View-only
* Adjacent Server Group Identifier	Unique identifier used to label an Adjacent Server Group.	Format: Text box. Valid characters are alphanumeric and underscore. Must contain at least one letter and must not start with a digit. Range: Up to 32 characters.
* Adjacent Server Group Member(s)	The list of Adjacent Nodes that make up the Adjacent Server Group. An Adjacent Node can be a member of only one Adjacent Server Group.	Format: Drag and drop Range: 1 to 16 entries.

Viewing Adjacent Server Groups

Use this procedure to view the configured Adjacent Server Groups.

Select **SS7/Sigtran > Configuration > Adjacent Servers Groups.**

The **SS7/Sigtran > Configuration > Adjacent Server Groups** page appears with the configured Adjacent Server Groups listed.

For field definitions, see *Adjacent Server Groups elements*.

Inserting an Adjacent Server Group

Use this task to add an Adjacent Server Group.

Note: "Adjacent Servers" must be configured as "Adjacent Nodes: on the **Transport Manager > Configuration > Adjacent Node [Insert]** page, and are listed on the **Transport Manager > Configuration > Adjacent Node** page.

1. Select **SS7/Sigtran > Configuration > Adjacent Server Groups**.

   The **SS7/Sigtran > Configuration > Adjacent Server Groups** page appears. For field definitions, see *Adjacent Server Groups elements*.

2. Click **Insert**.

   The **SS7/Sigtran > Configuration > Adjacent Server Groups [Insert]** page appears.

3. Enter an **Adjacent Server Group identifier**.

4. To add an Adjacent Server, click the Adjacent Server name you want to add from the **Unassigned Adjacent Servers** list. You can select multiple individual items by holding down **ctrl** while clicking the item (**ctrl-click**). To move them to **Adjacent Servers in this Adjacent Server Group** click the double arrows (**>>**) or use the drag drop method (With the left mouse button held down, move the mouse to the **Adjacent Servers in this Adjacent Server Group** then release the left mouse button.) To select a range, select **shift-click**.

   Note: If you need to add an Adjacent Server and no Adjacent Servers are available, you must first define one. Once you have defined an Adjacent Server, the **Unassigned Adjacent Servers** field will be populated.

5. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - Any required field is empty (not entered)
   - Adding a new Adjacent Server Group Member would cause the maximum number of **Adjacent Server Group Members** (16) to be exceeded
   - The **Adjacent Server Group Identifier** field value already exists
   - An Adjacent Server Group Member in this Group no longer exists (has been deleted)
   - An Adjacent Server Group Member in this Group was already assigned to another Group (by another user)
   - Adding this **Adjacent Server Group** would cause the maximum number of **Adjacent Server Groups** per site (10) to be exceeded

Editing an Adjacent Server Group

Use this task to add or remove an Adjacent Server in an Adjacent Server Group.

Note: "Adjacent Servers" are configured as "Adjacent Nodes" on the **Transport Manager > Configuration > Adjacent Node** pages.

Note: An Adjacent Server cannot be removed from an Adjacent Server Group if the Adjacent Node is referenced by a Transport.

1. Select **SS7/Sigtran > Configuration > Adjacent Server Groups**

   The **SS7/Sigtran > Configuration > Adjacent Server Groups** page appears.

2. Click **Edit** next to the Adjacent Server Group that you want to modify.

   The **SS7/Sigtran > Configuration > Adjacent Server Groups [Edit]** page appears.

3. To add or remove an Adjacent Server, perform these steps:

   - To add an Adjacent Server, click the name in the **Unassigned Adjacent Servers** list and click the double arrows (**>>**).

     You can select multiple individual items by holding down **Ctrl** while clicking the item (**Ctrl-click**).To move them to **Adjacent Servers in this Adjacent Server Group** click the double arrows (**>>**) or use the drag drop method (With the left mouse button held down, move the

mouse to the **Adjacent Servers in this Adjacent Server Group** then release the left mouse button.) To select a range, select **Shift-click.**

Note: If you need to add an Adjacent Server and no Adjacent Nodes are available, you must first configure one. (Refer to "Inserting an Adjacent Node" in the *Transport Manager User's Guide* and Help). After an Adjacent Node is configured, the **Unassigned Adjacent Servers** field is populated.

- To remove an Adjacent Server from the Adjacent Server Group, click the name in the **Adjacent Servers in this Adjacent Server Group** list and click the double arrows (**<<**). You can select more than one Adjacent Server by holding down **Ctrl** while clicking each name. To select a range, select **Shift-click.**

4. Perform one of these actions
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to exit this page without saving any the data.

   If **OK** or **Apply** is clicked and the selected Adjacent Server Group no longer exists (was deleted by another user), an error message appears.

Deleting an Adjacent Server Group

Deleting an Adjacent Server Group removes the group from the network configuration.

Note: An Adjacent Server Group that is referenced by a Remote Signaling Point cannot be deleted. Use the *Deleting a Remote Signaling Point* procedure to remove the RSP.

1. Select **SS7/Sigtran > Configuration > Adjacent Server Groups**.

   The **SS7/Sigtran > Configuration > Adjacent Server Groups** page appears.

2. Click **Delete** in the row of the Adjacent Server Group that you want to remove.

   A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

Local Signaling Points

A Signaling Point is a set of signaling equipment represented by a unique point code within an SS7 domain (for example, ANSI, ITU-I, ITU-N). An LSP (Local Signaling Point) is a logical element representing an SS7 Signaling Point assigned to an MP Server Group.

A Point Code is a unique MTP3 (Message Transfer Part 3) address in a SS7 network. An LSP is uniquely identified by a point code and an SS7 domain.

The LSP assigns the SS7 identity to the MP server group. An LSP has an SS7 domain (ANSI, ITU-I, ITU-N) and a true point code. The LSP may optionally be assigned up to two CPCs (Capability Point Codes), which are point codes that can be shared with other LSPs. The LSP also has assigned a server group that hosts the point code.

The list of configured LSPs on the **SS7/Sigtran > Configuration > Local Signaling Points** page contains a row for every point code that represents an MP Server Group.

Local Signaling Points elements

Table 10: Local Signaling Points Elements describes the information on the **SS7/Sigtran > Configuration > Local Signaling Points** pages. Data Input Notes apply only to the Insert and Edit pages.

Table 10: Local Signaling Points Elements

Element (* indicates required field)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element to which the Local Signaling Point is being added.	View-only
* SS7 Domain	The SS7 domain in which the node resides.	Format: Pulldown list Range: ANSI, ITUN - ITU National, ITUI - ITU International, ITU National 24-bit Point Code **Note:** MD-IWF does not support ITUN24 - ITU National 24-bit point codes.
Local Signaling Point Name	Unique, case-sensitive name of the Local Signaling Point. The default name is auto-generated and populated. You can overwrite the default name. The default name is auto generated from the true point code in the following manner: • Domain: ANSI, true point code configured: 1-1-1 Default LSP Name - ANSI_001_001_001 • Domain: ITUI, true point code configured: 1-1-1 Default LSP Name - ITUI_1_001_1 • Domain: ITUN, true point code configured: 2057	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Element (* indicates required field)	Description	Data Input Notes
	Default LSP Name - ITUN_2057	
* MTP True Point Code	The MTP point code that identifies this LSP. Only one LSP can have this MTP True point code.	Format: Text field requires point code format (see *Point code formats*).
MTP Capability Point Code(s)	The MTP capability point code if this LSP shares a point code with one or more other LSPs.	Format: Checkbox and text field. The checkbox(es) must be checked to enable the field. The text field requires point code format (see *Point code formats*). The MTP Capability Point Code(s) cannot exist in the system as an MTP True Point Code. This field is optional unless the checkbox(es) are checked. If the checkbox(es) are checked, the text field(s) are required.
* Server Group(s)	Server Groups that serve this LSP.	Range: 1 entry

Point code formats

A point code is a unique (MTP3) address in an SS7 network. This application supports following point code formats based on the selected SS7 domain:

- **ANSI Point Code**

  Format: NNN-NNN-NNN

  Range: Point code must comply with ANSI T1.111.8.

- **ITU International Point Code**

  Format: J-NNN-J

  Range J can range from 0-7. NNN can range from 0-255.

- **ITU National Point Code**

  Format: NNNNN

  Range: NNNNN can range from 0-16383

- **ITU National 24-bit Point Code**

  Format: NNN-NNN-NNN

Range: Each NNN can range from 0 - 255

Note: MD-IWF does not support ITUN24 point codes.

Viewing Local Signaling Points

Use this procedure to view the configured LSPs.

Select **SS7/Sigtran > Configuration > Local Signaling Points**.

The **SS7/Sigtran > Configuration > Local Signaling Points** page appears with the configured LSPs listed.

For field definitions, see *Local Signaling Points elements*.

Inserting a Local Signaling Point

Use this procedure to insert an LSP.

1. Select **SS7/Sigtran > Configuration > Local Signaling Points**.

   The **SS7/Sigtran > Configuration > Local Signaling Points** page appears.

2. Click **Insert**.

   The **SS7/Sigtran > Configuration > Local Signaling Points [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Local Signaling Points elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **S7/Sigtran > Configuration > Local Signaling Points** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - Any required field is empty (not entered)
   - Adding a **Server Group** would cause the maximum number of **Server Groups** per LSP (1) to be exceeded
   - The **Local Signaling Point Name** field value already exists
   - A **Server Group** added to the list of Server Groups no longer exists (has been deleted)
   - A **Server Group** added to the list of Server Groups does not have at least one Server assigned to it
   - The **MTP True Point Code** was already assigned to another LSP (by another user)
   - The **MTP Capability Point Code** already exists as an MTP Capability Point Code for this LSP
   - The **MTP Capability Point Code** already exists as an MTP True Point Code
   - Any of the **MTP Capability Point Code** check boxes is checked, but the corresponding MTP Capability Point Code value was not entered
   - Adding this **Local Signaling Point** would cause the maximum number of Local Signaling Points per site (10) to be exceeded

Editing a Local Signaling Point

Use this procedure to edit an LSP.

The **Edit** operation lets you add or remove the MTP Capability Point Code and the assigned Server Group from an LSP configuration, if the LSP is not referenced by a Link Set.

1. Select **SS7/Sigtran > Configuration > Local Signaling Points**.

   The **SS7/Sigtran > Configuration > Local Signaling Points** page appears.

2. Click **Edit**.

   The **SS7/Sigtran > Configuration > Local Signaling Points [Edit]** page appears.

3. (Optional) To delete an **MTP Capability Point Code** from the LSP, uncheck the checkbox.

   A Capability Point Code cannot be removed from an LSP that is referenced by a Link Set. If necessary, perform *Deleting a Link Set* to remove the reference.

4. (Optional) To add an **MTP Capability Point Code**, check the checkbox and then enter the MTP Capability Point Code as described in *Local Signaling Points elements*.

5. (Optional) To add a **Server Group**, click the name in the **Unassigned Server Group** list and click the (**>>**) arrows to add the Server Groups to the **Server Groups included in this Local Signaling Point** field. You can select more than one by holding down **ctrl** while clicking a name then click the (**>>**) arrows to add the Server Groups to the **Server Groups included in this Local Signaling Point** field. Use **Shift-click** to select a range.

6. (Optional) To remove a **Server Group**, click the name in the **Server Groups included in this Local Signaling Point** list and the (**<<**) arrows. You can select more than one by holding down **Ctrl** while clicking a name then click the (**<<**) arrows.

   A Server Group cannot be removed from an LSP that is referenced by a Link Set. If appropriate, perform *Deleting a Link Set*.

7. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - Any required field is empty (not entered)
   - Adding a **Server Group** would cause the maximum number of **Server Groups** per LSP (1) to be exceeded
   - The **Local Signaling Point Name** field value already exists
   - A **Server Group** added to the list of Server Groups no longer exists (has been deleted)
   - A **Server Group** added to the list of Server Groups does not have at least one Server assigned to it
   - The **MTP True Point Code** was already assigned to another LSP (by another user)
   - The **MTP Capability Point Code** already exists as an MTP True Point Code
   - The **MTP Capability Point Code** already exists as an MTP Capability Point Code for this LSP
   - Any of the **MTP Capability Point Code** check boxes is checked, but the corresponding MTP Capability Point Code value was not entered
   - Adding this **Local Signaling Point** would cause the maximum number of Local Signaling Points per site (10) to be exceeded

Deleting a Local Signaling Point

Deleting an LSP removes the LSP from the SS7 network configuration.

An LSP cannot be deleted that is referenced by a Link Set. If appropriate, perform *Deleting a Link Set*.

An LSP cannot be deleted that is referenced by a Local SCCP User. If appropriate, perform *Deleting a Local SCCP User*

1. Select **SS7/Sigtran > Configuration > Local Signaling Points**
   The **SS7/Sigtran > Configuration > Local Signaling Points** page appears.
2. Click **Delete** in the row of the LSP you want to remove.
   A delete confirmation message appears.
3. Click **OK** to confirm the deletion.

Generating a report on Local Signaling Points

1. Select **SS7/Sigtran > Configuration > Local Signaling Points**

   The **SS7/Sigtran > Configuration > Local Signaling Points** page appears.
2. Perform one of these actions:
   - Click **Report** next to an entry in the list to generate a report on the entry.
   - Click the **Report** link at the bottom of the list to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Local SCCP Users

An LSU (Local SCCP User) is an application configured with a subsystem number to handle Rt-on-SSN traffic for a local signaling point code hosted on an MP server.

Adding, deleting, or changing the status of an LSU affects the routing to configured Local SCCP Users. SCCP is notified when an operator creates a local subsystem via the GUI and assigns a Local SCCP User to the local subsystem. This assignment entry is added to SCCP's internal database with a default status of **Disabled**. The assignment enables SCCP to track the status of locally configured LSUs for messages that are routed on the SSN.

The **SS7/Sigtran > Configuration > Local SCCP Users** GUI page contains a row for each SS7 application hosted by SS7-MP servers. The fields in each row indicate which SSN is associated with an application.

Local SCCP Users elements

Table 11: Local SCCP Users Elements describes the information on the**SS7/Sigtran > Configuration > Local SCCP Users** pages: Data Input Notes apply only on the Insert page.

Table 11: Local SCCP Users Elements

Element (* indicates required field)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element Name to which the Local SCCP User is being added.	View-only
* SSN	The specific subsystem number served by this Local SCCP User. This field is used to route incoming messages to the application hosting this SSN.	Format: Numeric Range: 2 - 254
* (Local Signaling Point) Point Code	The point code of the Local Signaling Point associated with this Local SCCP User. Local signaling points are defined at **SS7/Sigtran > Configuration > Local Signaling Points** (see *Local Signaling Points*).	Format: Pulldown list of all configured LSPs associated with the selected **Signaling Network Element Name**. Range: 1 entry
* (Local Signaling Point) SS7 Domain	The SS7 domain of the selected Local Signaling Point.	Format: Pulldown list. Range: ANSI, ITUN - ITU National, ITUI - ITU International **Note:** MD-IWF does not support ITUN24 - ITU National 24-bit point codes.
* Application Name	Application Name to configure as the Local SCCP User.	Format: Pulldown list of all configured applications. If there is only one application configured, that **Application Name** appears in this field as a view-only entry. Range: 1 entry

Viewing Local SCCP Users

Use this procedure to view the configured LSUs.

Select **SS7/Sigtran > Configuration > Local SCCP Users**.

The **S7/Sigtran > Configuration > Local SCCP Users** page appears with the configured LSUs listed.

For field definitions, see *Local SCCP Users elements*.

Inserting a Local SCCP User

Use this procedure to insert an LSU.

An LSU cannot be added if an identical LSU already exists with an SSN corresponding to the same LSP (point code and domain).

1. Select **SS7/Sigtran > Configuration > Local SCCP Users**

   The**SS7/Sigtran > Configuration > Local SCCP Users** page appears.

2. Click **Insert**.

   The **SS7/Sigtran > Configuration > Local SCCP Users [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Local SCCP Users elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Local SCCP Users** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - The **SSN** field contains a value that is a wrong data type or is out of the allowed range
   - Any required field is empty (not entered)
   - An Identical LSU already exists for same SSN corresponding to same LSP (Point code and domain)
   - The **LSP** no longer exists (has been deleted)
   - Adding this **Local SCCP User** would cause the maximum number of LSPs per LSU (250) to be exceeded

   The LSU is added to the configuration. By default, the LSU is in the **Disabled** state. To enable the LSU, see *Enabling a Local SCCP User*.

Deleting a Local SCCP User

Deleting an LSU removes the LSU from the SS7 network configuration.

Caution: Deletion of an LSU that is in the **Enabled** state may result in the loss of signaling data. To disable an LSU, see *Disabling a Local SCCP User*.

1. Select **SS7/Sigtran > Configuration > Local SCCP Users**.

   The **SS7/Sigtran > Configuration > Local SCCP Users** page appears.

2. Click **Delete** in the row of the LSU you want to remove.

   A delete confirmation message appears.

3. Perform one of the following actions

   - Click **OK** to confirm the deletion.

If the LSU is **Enabled**, an additional confirmation message appears.

Continue with *Step 4*.

- Click **Cancel** to return to the **SS7/Sigtran > Configuration > Local SCCP Users** page without deleting the LSU.

4. Perform one of the following actions if the LSU is in the **Enabled** state:
   - If the confirmation message says that the LSU state reported by the MP server is not **Disabled**, click **Cancel** to close the confirmation message and then disable the LSU.
   - If the confirmation message says that the MP server cannot determine the LSU state, click **Cancel** to close the confirmation message, and look on **Status & Manage > Servers** GUI page to investigate.
   - On either confirmation message, click **OK** to force the deletion of the LSU.

Caution: Deletion of an LSU that is **Enabled** may result in the loss of signaling data. See *Disabling a Local SCCP User* to disable the LSU.

Status of a Local SCCP User

Use this procedure to view Status of the configured LSU.

1. Select **SS7/Sigtran > Configuration > Local SCCP Users**.

   The **SS7/Sigtran > Configuration > Local SCCP Users** page appears.

2. Select the **Signaling Network Element Name** to check the status.
3. Click **Status**.

   The **SS7/Sigtran > Maintenance > Local SCCP Users** page appears. See *Enabling a Local SCCP User* and *Disabling a Local SCCP User* for the procedures.

Generating a report on Local SCCP Users

1. Select **SS7/Sigtran > Configuration > Local SCCP Users**.

   The **SS7/Sigtran > Configuration > Local SCCP Users** page appears.

2. Perform one of these actions:
   - Click **Report** next to an entry in the list to generate a report on the entry.
   - Click the **Report** link at the bottom of the list to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Remote Signaling Points

An RSP (Remote Signaling Point) represents an SS7 network node (point code) that signaling must be sent to, from an SS7-MP. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.

Note: MD-IWF does not support ITUN24 - ITU National 24-bit point codes.

An Adjacent Server Group is configured if the Remote Signaling Point is an *adjacent* Remote Signaling Point. An STP to which an SS7-MPis connected via an Association is an adjacent RSP.

The list on the **SS7/Sigtran > Configuration > Remote Signaling Points** page must contain a row for every point code that is directly connected to the SS7 application and any remote destination that the SS7 application originates messages toward.

The list on the **SS7/Sigtran > Configuration > Remote Signaling Points** page provides a link to the **SS7/Sigtran > Maintenance > Remote Signaling Points** page where you can view the status of each configured RSP, and manually reset the network status of an RSP.

Remote Signaling Point elements

Table 12: Remote Signaling Points Elements describes the information on the **SS7/Sigtran > Configuration > Remote Signaling Points** pages: Data Input Notes apply only to the **[Insert]** page,

Table 12: Remote Signaling Points Elements

Element (* indicates required field)	Description	Data Input Notes
* SS7 Domain	The SS7 domain in which the RSP resides.	Format: Pulldown list Range: ANSI, ITUN - ITU National, ITUI - ITU International, ITU National 24-bit Point Code **Note:** MD-IWF does not support ITUN24 - ITU National 24-bit point codes.
* MTP Point Code	The unique MTP point code that identifies this RSP. Only one RSP can have this MTP point code.	Text field requires point code format (see *Point code formats*).
Remote Signaling Point Name	An optional name that uniquely identifies the Remote Signaling Point. RSP names are case sensitive. If this field displays dashes, it indicates that a name has not been configured for this RSP.	Format: Text box; valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Element (* indicates required field)	Description	Data Input Notes
Adjacent Server Group	The Adjacent Server Group associated with this RSP. Populate this field if this RSP represents an Adjacent Server. An Adjacent Server Group can be referenced by more than one RSP. An RSP, however, can reference one and only one Adjacent Server Group.	Format: Pulldown list Range: All configured Adjacent Server Groups. Default: None (this RSP will not be used to signal to an Adjacent Server).

Viewing Remote Signaling Points

Use this procedure to view the configured RSPs.

Select **SS7/Sigtran > Configuration > Remote Signaling Points**.

The **SS7/Sigtran > Configuration > Remote Signaling Points** page appears, listing all of the configured RSPs.

For field definitions, see *Remote Signaling Point elements*.

Inserting a Remote Signaling Point

Use this task to add a Remote Signaling Point.

1. Select **SS7/Sigtran > Configuration > Remote Signaling Points**.

   The **SS7/Sigtran > Configuration > Remote Signaling Points** page appears.

2. Click **Insert**.

   The **SS7/Sigtran > Configuration > Remote Signaling Points [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Remote Signaling Point elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Remote Signaling Points** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - Any fields contain a value that is out of the allowed range
   - Any required field is empty (not entered)
   - The **Remote Signaling Point Name** field value already exists
   - Adding a **Server Group** would cause the maximum number of **Server Groups** per LSP (1) to be exceeded
   - A selected **Adjacent Server Group** no longer exists (has been deleted)

- The **MTP Point Code** was already assigned to another RSP (by another user)
- Adding this **Remote Signaling Point** would cause the maximum number of Remote Signaling Points per site (512) to be exceeded

Deleting a Remote Signaling Point

Deleting an RSP removes the RSP from the SS7 network configuration.

An RSP cannot be deleted that is referenced by a Remote MTP3 User, a Link Set, or a Route. If necessary, perform *Deleting a Remote MTP3 User*, *Deleting a Link Set*, or *Deleting a Route* prior to attempting this procedure.

1. Select **SS7/Sigtran > Configuration > Remote Signaling Points**.
   The **SS7/Sigtran > Configuration > Remote Signaling Points** page appears.
2. Click **Delete** in the row you want to remove.
   A delete confirmation message appears.
3. Click **OK** to confirm the deletion.

Status of a Remote Signaling Point

Use this procedure to view Status of the configured RSP.

1. Select **SS7/Sigtran > Configuration > Remote Signaling Points**.
   The **SS7/Sigtran > Configuration > Remote Signaling Points** page appears.
2. Select the **SS7 Domain** to check the status.
3. Click **Status**.
   The **SS7/Sigtran > Maintenance > Remote Signaling Points** page appears. See *Resetting the subsystem and point code status* and *Resetting the Network Status of the Routes* for the procedures.

Generating a report on Remote Signaling Points

Use this task to generate a report on one or all Remote Signaling Points.

1. Select **SS7/Sigtran > Configuration > Remote Signaling Points**.
   The **SS7/Sigtran > Configuration > Remote Signaling Points** page appears.
2. Perform one of these actions:
   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Remote MTP3 Users

An RMU (Remote MTP3 User) represents a remote SCCP subsystem to which the Signaling Network Interface forwards signaling. When a message is forwarded from an MSC to an SS7-MP node, an RMU must be configured for the subsystem on the SS7-MP node.

There are two configuration scenarios for remote subsystems to which only service messages will be sent. A service message is a failure indication such as UDTS and XUDTS.

- If an MP must route signaling for UDT, XUDT, UDTS, or XUDTS to an RMU (such as a remote SCCP peer), then an RMU must be configured for that remote SCCP subsystem.
- For a remote SCMG (SCCP Management) subsystem, it is not necessary or possible to create an RMU. SCCP Management uses subsystem 1 instead. Subsystem 1 is automatically created at the time the message is forwarded.

If an RMU exists, the subsystem status is tracked and used for routing SS7 messages (including service messages).

STPs generally do not have subsystems and therefore do not need RMUs. An exception would be an application such as LNP (Local Number Portability) that can be hosted on an STP.

The **SS7/Sigtran > Configuration > Remote MTP3 Users** GUI page displays an entry for each MTP3 user to which SS7 SCCP signaling is sent, or for which status tracking is desired. The fields are used to populate the Called Party Address parameters.

The **SS7/Sigtran > Configuration > Remote MTP3 Users** GUI page also provides a link to the **SS7/Sigtran > Maintenance > Remote MTP3 Users** page, where you can view the status of each configured RMU and reset the subsystem and point code status of an RMU.

Remote MTP3 Users elements

Table 13: Remote MTP3 Users Elements describes the information on the **SS7/Sigtran > Configuration > Remote MTP3 Users** pages. Data Input Notes apply only to the Insert page.

Table 13: Remote MTP3 Users Elements

Element (* indicates required field)	Description	Data Input Notes
* SS7 Domain	The SS7 domain in which the selected Remote Signaling Point resides.	Format: Pulldown list. Range: ANSI, ITUN - ITU National, ITUI - ITU International, ITU National 24-bit Point Code **Note:** MD-IWF does not support ITUN24 - ITU National 24-bit point codes.
* Remote Point Code	The Remote Point Code configured in the Remote	Format: Pulldown list

Element (* indicates required field)	Description	Data Input Notes
	Signaling Point associated with this Remote MTP3 User. Remote Signaling Points are defined at **SS7/Sigtran > Configuration > Remote Signaling Points**.	All configured Remote Signaling Points.
* Remote SSN	The specific subsystem number to track the status of the RMU. The combination of Point Code and SSN must be unique.	Format: Text box; numeric Range: 2-254
Remote MTP3 User Name	An optional name that uniquely identifies the RMU. An RMU must be created for each MTP3 user whose status should be tracked by SCCP. The RMU name is case-sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Viewing Remote MTP3 Users

Use this task to view configured Remote MTP3 Users.

Select **SS7/Sigtran > Configuration > Remote MTP3 Users**.

The **SS7/Sigtran > Configuration > Remote MTP3 Users** page appears with the configured RMUs listed.

For field definitions, see *Remote MTP3 Users elements*.

Inserting a Remote MTP3 User

Use this task to add a Remote MTP3 User.

1. Select **SS7/Sigtran > Configuration > Remote MTP3 Users**.

   The **SS7/Sigtran > Configuration > Remote MTP3 Users** page appears.

2. Click **Insert** .

   The**SS7/Sigtran > Configuration > Remote MTP3 Users [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Remote MTP3 Users elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Remote MTP3 Users** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

- Any fields contain a value that is wrong data type or out of the allowed range
- Any required field is empty (not entered)
- The **Remote MTP3 User Name** field value already exists
- An **Remote MTP3 User** already exists with the same RSP and Remote SSN values
- A selected **Remote Point Code** no longer exists (has been deleted)
- Adding this **Remote MTP3 User** would cause the maximum number of Remote MTP3 Users per site (512) to be exceeded

Deleting a Remote MTP3 User

Use this task to delete a Remote MTP3 User.

1. Select **SS7/Sigtran > Configuration > Remote MTP3 Users**.

   The **SS7/Sigtran > Configuration > Remote MTP3 Users** page appears.

2. Click **Delete** in the row you want to remove.

   A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

Status of a Remote MTP3 User

Use this procedure to view Status of the configured Remote MTP3 User.

1. Select **SS7/Sigtran > Configuration > Remote MTP3 Users**.

   The **SS7/Sigtran > Configuration > Remote MTP3 Users** page appears.

2. Select the **SS7 Domain** to check the status.
3. Click **Status**.

   The **SS7/Sigtran > Maintenance > Remote MTP3 Users** page appears. See *Resetting the subsystem and point code status* and *Resetting the Network Status of the Routes* for the procedures.

Link Sets

A Link Set represents a logical signaling connection from one local point code (LSP) to one adjacent remote point code (adjacent RSP).

Each DSR site can be configured with up to 96 Link Sets. A Link Set may be assigned up to 16 links.

A Link Set can span Associations. For example, an STP point code can be distributed across multiple servers such as EAGLE E5-ENET cards. A Link Set cannot span MP servers because each MP server has its own point code.

A Link Set is typically configured for each combination of LSPs and adjacent RSPs with these parameters specified:

- The point code (the True Point Code or Capability Point Code) from the LSP that this Link Set serves
- The adjacent RSP
- (Optional) the Routing Context

The **SS7/Sigtran > Configuration > Link Sets** page lists Link Sets for each combination of Local Signaling Point and adjacent Remote Signaling Point.

The **SS7/Sigtran > Configuration > Links Sets** page also provides a link to the **SS7/Sigtran > Maintenance > Link Sets** page where you can view the status of each configured Link Set.

Link Sets elements

Table 14: Link Sets Elements describes information on the **SS7/Sigtran > Configuration > Link Sets** pages. Data Input Notes apply only to the Insert page.

Table 14: Link Sets Elements

Element (* indicates required field)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element to which the Link Set is being added.	View-only
* Link Set Name	A name that uniquely identifies this Link Set. The Link Set name is case-sensitive.	Format: Text box; valid characters are alphanumeric and underscore (_). Must contain at least one alpha and must not start with a digit. Range: A 32-character string.
* Mode	Defines the desired relationship between the local and remote peer for this Link Set. The mode specifies whether the Message Processor implements client or server procedures for session management. One mode is supported: **AS (Application Server) to SG (Signaling Gateway)**. The local side is the client; the remote side is the server. The local side has LMU and LSP; the remote side has RSP and optionally RMU.	Format: Pulldown list Range: Select **AS->SG** if the local side of the connection is an Application Server and the remote side is a Signaling Gateway. Default: AS->AG
* Local Signaling Point	Specifies the LSP served by this Link Set. Each Local Signaling Point entry is a hyperlink to the Local	Format: Pulldown list Range: All configured LSPs.

Element (* indicates required field)	Description	Data Input Notes
	Signaling Point table filtered by this LSP.	
SS7 Domain	The SS7 domain of the selected Local Signaling Point.	Format: This is a display-only field populated when a Local Signaling Point is selected.
* LSP Point Code	The point code of the selected Local Signaling Point to be served by this Link Set. A selection of **All** means that the Link Set will accept signaling destined for the selected Local Signaling Point's True Point Code or Capability Point Code, if one is assigned.	Format: Pulldown list Range: All Default: All
* Adjacent Remote Point Code	The point code of the Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway to be served by this Link Set. Each entry is a hyperlink to the Remote Signaling Point table filtered by this Adjacent Remote Point Code.	Format: Pulldown list Range: The list is based on the domain of the selected **Local Signaling Point**.
Assign Routing Context (appears on Insert Link Set page only)	Indicates whether a Routing Context applies to this Link Set. A Routing Context must be specified if links from this Link Set will share an Association with links from at least one other Link Set.	Format: Pulldown list Range: Yes, No Select **Yes** if a Routing Context Applies. If you select **No**, the Routing Context field is cleared and disabled. Default: No
Routing Context	Message parameter used to uniquely identify the application context. This value is used only if Assign Routing Context is set to **Yes**. This Routing Context must be configured to match the Routing Context value configured for this Link Set at the Signaling Gateway.	Format: Text box; numeric Range: 32-bit unsigned Default: First unused integer value greater than zero.

Viewing Link Sets

Use this task to view configured Link Sets.

Select **SS7/Sigtran > Configuration > Link Sets**.

The **SS7/Sigtran > Configuration > Link Sets** page appears with the configured Link Sets listed..

For field definitions, see *Link Sets elements* .

Inserting a Link Set

Use this task to add a Link Set.

1. Select **SS7/Sigtran > Configuration > Link Sets**.

   The **SS7/Sigtran > Configuration > Link Sets** page appears.

2. Click **Insert**.

   The**SS7/Sigtran > Configuration > Link Sets [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Link Sets elements* .
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Link Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - Any enabled field has no value, or a pullown list box has a value of **-- Select --**.
   - Any enabled field contains a value that is a wrong data type or is out of the allowed range
   - The **Link Set Name** already exists.
   - The selected **Local Signaling Point** no longer exists (has been deleted).
   - The selected **Adjacent Remote Point Code** no longer exists (has been deleted).
   - a Link Set with the selected LSP and RSP already exists.
   - Adding this **Link Set** would cause the maximum number of Link Sets per site (96) to be exceeded.

Deleting a Link Set

Use this task to delete a Link Set.

Deleting a Link Set removes the Link Set from the configuration.

A Link Set cannot be deleted that is referenced by a Link or a Route. If necessary, perform *Deleting a Link* or *Deleting a Route* before proceeding.

1. Select **SS7/Sigtran > Configuration > Link Sets**.

   The **SS7/Sigtran > Configuration > Link Sets** page appears.

2. Click **Delete** in the row you want to remove.

A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

Status of a Link Set

Use this procedure to view Status of the configured Link Set.

1. Select **SS7/Sigtran > Configuration > Link Sets**.

   The **SS7/Sigtran > Configuration > Link Sets** page appears.

2. Select the **Signaling Network Element Name** to check the status.
3. Click **Status**.

   The **SS7/Sigtran > Maintenance > Linksets** page appears. This is a read only page.

Generating a report on Link Sets

Use this task to generate a report for one or all Link Sets.

1. Select **SS7/Sigtran > Configuration > Link Sets**.

   The **SS7/Sigtran > Configuration > Link Sets** page appears.

2. Perform one of these actions:

   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Links

A Link carries signaling within a Link Set using a specific Association. A Link can belong to only one Link Set and one Association.

If a Link fails, the Signaling Network Interface attempts to divert signaling traffic to another Link in the same Link Set.

The **SS7/Sigtran > Configuration > Links** page shows all configured M3UA links.

The **SS7/Sigtran > Configuration > Links** page also provides a link to the **SS7/Sigtran > Maintenance > Links** page where you can view the status of all configured Links, and manually enable and disable Links.

Note: Links cannot be edited. A link can be changed only by deleting it and adding the changed link.

Links elements

Links elements describes the information on the **SS7/Sigtran > Configuration > Links** pages. Data Input Notes apply only to the Insert page.

Table 15: Links Elements

Element (* indicates required field)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element to which the Link is being added.	View-only
* Link Name	A name that uniquely identifies the Link. The name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.
* Link Set	The Link Set to which the Link is being added. A Link Set supports up to 16 links. Each Link Set entry is a hyperlink to the Link Set table filtered by this Link Set.	Format: Pulldown list Range: All Link Sets associated with the selected Signaling Network Element.
*Association	The SCTP Association that will host the Link. If the Link shares an Association with Links from other Link Sets, each Link Set using the Association must be configured with a unique routing context. Only one Link can be created for a given Link Set and Association.	Format: Pulldown list Range: All Associations configured as Transports under **Transport Manager > Configuration > Transports**.

Viewing Links

Use this procedure to view the configured links.

Select **SS7/Sigtran > Configuration > Links**.

The **SS7/Sigtran > Configuration > Links** page appears with the configured links listed.

For field definitions, see *Links elements*.

Inserting a Link

Use this task to add a Link.

A Link cannot be inserted if any of the following is true:

- The Local MP Server that hosts the selected Association does not exist in the Server Group that hosts the Local Signaling Point associated with the selected Link Set.
- A Link already exists with the same combination of Link Set and Association.
- The selected Association already hosts at least one Link from another Link Set that has the same Routing Context as the Routing Context in the selected Link Set.
- The Adjacent Server that hosts the selected Association does not exist in the Adjacent Server Group that represents the Remote Signaling Point associated with the selected Link Set.
- The selected Association already hosts at least one Link from another Link Set but at least one of the Link Sets has no Routing Context configured.

1. Select **SS7/Sigtran > Configuration > Links.**
   The **SS7/Sigtran > Configuration > Links** page appears.
2. Click **Insert**.

   The **SS7/Sigtran > Configuration > Links [Insert]** page appears.
3. Populate the fields with data. For field definitions, see *Links elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Links** page without saving any changes.

   The Link is added and is placed in the **Disabled** Administrative State. See *Link Maintenance* to view the Administrative State of the link. To enable the link, see *Enabling a Link*

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - A pulldown list box has a value of **-- Select --** or a required field value is missing (not entered).
   - Any fields contain a value that is out of the allowed range.
   - The **Link Name** field value already exists.
   - Adding this **Link** would cause the maximum number of Links per site (1024) to be exceeded.
   - Adding this **Link** would cause the maximum number of Links per Link Set (16) to be exceeded.
   - Adding this **Link** would cause the maximum number of Links per Association (8) to be exceeded.
   - The selected **Link Set** no longer exists (has been deleted).
   - The selected **Association** no longer exists (has been deleted).
   - The Local MP Server referenced by the selected **Association** does not exist in the Server Group hosting the LSP associated with the selected Link Set.
   - The Adjacent Server referenced by the selected **Association** does not exist in the Adjacent Server Group referenced by the RSP associated with the selected Link Set.
   - The selected **Association** already hosts at least one Link from another Link Set that has the same Routing Context as the Routing Context in the selected Link Set.
   - The selected **Association** already hosts at least one Link from another Link Set and at least one of the Link Sets has no Routing Context configured.

Deleting a Link

Deleting a Link removes the Link from the database.

A Link cannot be deleted if it is in-service. To disable the Link, (see *Disabling a Link*).

1. Select **SS7/Sigtran > Configuration > Links.**

   The **SS7/Sigtran > Configuration > Links** page appears.

2. Click **Delete** in the row that you want to remove.

   A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

Status of a Link

Use this procedure to view Status of the configured Link.

1. Select **SS7/Sigtran > Configuration > Links.**

   The **SS7/Sigtran > Configuration > Links** page appears.

2. Select the **Signaling Network Element Name** to check the status.
3. Click **Status**.

   The **SS7/Sigtran > Maintenance > Links** page appears. See *Enabling a Link* and *Disabling a Link* for the procedures.

Generating a report on Links

Use this task to generate a report for one or all links.

1. Select **SS7/Sigtran > Configuration > Links**.

   The **SS7/Sigtran > Configuration > Links** page appears.

2. Perform one of these actions:

   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

Routes

A Route represents a signaling path from a local (LSP) point code to a remote signaling point (RSP) point code using a given Link Set. Routes are needed for adjacent RSPs to route network management signaling. A Route consists of an RSP, a Link Set, and a relative cost.

There can be up to two routes between a local point code and a remote point code.

Each Route has a cost. The Signaling Network Interface attempts to route signaling over the lower cost Route. If two Routes have the same cost, signaling is load-shared across both Routes.

The Signaling Network Interface supports 1024 routes per site.

The **SS7/Sigtran > Configuration > Routes** page shows all configured Routes. Each Remote Signaling Point can have a maximum of two Routes.

The **SS7/Sigtran > Configuration > Routes** page also provides a link to the **SS7/Sigtran > Maintenance > Remote Signaling Points** page where you can view the status of all configured Routes and destinations and manually reset the network status of a Route.

Routes elements

Table 16: Routes Elements describes the information on the **SS7/Sigtran > Configuration > Routes** pages. Data Input Notes apply only to the Insert and Edit pages.

Table 16: Routes Elements

Element (* indicates required field)	Description	Data Input Notes
* Signaling Network Element Name	Identifies the Signaling Network Element to which the route is being added.	View-only
* SS7 Domain	The SS7 domain of the selected Remote Signaling Point.	Format: Pulldown list Range: ANSI, ITUN - ITU National, ITUI - ITU International, ITU National 24-bit Point Code **Note:** MD-IWF does not support ITUN24 - ITU National 24-bit point codes.
* Remote Point Code	The point code configured in the remote signaling point that identifies the destination of this route	Format: Pulldown list Range: Configured Remote Signaling Points associated with the selected SS7 Domain.
* Link Set	The Link Set to be used by this route. The choice of Link Set implies the LSP of the Route.	Format: Pulldown list Range: Configured Link Sets from the selected Remote Point Code domain.
Adjacent Point Code	The point code configured in the Adjacent RSP being used by the selected Link Set.	This field is view-only. The field is populated automatically when a Link Set is selected.
* Relative Cost	The relative cost assigned to this route. Lower cost routes are preferred over higher cost routes.	Format: Text box; numeric Default: 20 Range: 0 - 99

Element (* indicates required field)	Description	Data Input Notes
Route Name	An optional name that uniquely identifies the route. The name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Viewing Routes

Use this procedure to view the configured Routes.

Select **SS7/Sigtran > Configuration > Routes**.

The **SS7/Sigtran > Configuration > Routes** page appears with the configured Routes listed. For field definitions, see *Routes elements*.

Inserting a Route

Use this task to add a Route.

A Route cannot be inserted if any of the following is true:

- A Route already exists with the selected Remote Signaling Point and Link Set.
- The SS7 domain of the selected Remote Signaling Point does not match the SS7 domain of the Local Signaling Point configured for the selected Link Set.

1. Select **SS7/Sigtran > Configuration > Routes**.

   The **SS7/Sigtran > Configuration > Routes** page appears.

2. Click **Insert**.

   The **SS7/Sigtran > Configuration > Routes [Insert]** page appears.

3. Populate the fields with data. For field definitions, see *Routes elements*.
4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Routes** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exists, an error message appears:

   - Any fields contain a value that is wrong data type or out of the allowed range
   - Any required field is empty (not entered)
   - The **Route Name** field value already exists
   - The selected **Remote Point Code** no longer exists (has been deleted)
   - The selected **Link Set** no longer exists (has been deleted)

- The selected Remote Signaling Point (Remote Point Code) and Link Set already exist for an existing Route
- Adding this **Route** would cause the maximum number of Routes per site (1024) to be exceeded
- The maximum number of Routes per RSP per MP server (2) have already been created for the selected RSP and MP server

Editing a Route

The **Edit** operation lets you change the Relative Cost associated with a Route. All other fields on the page are read-only.

1. Select **SS7/Sigtran > Configuration > Routes**.

   The **SS7/Sigtran > Configuration > Routes** page appears.

2. Click **Edit**.

   The **SS7/Sigtran > Configuration > Routes [Edit]** page appears. For field definitions, see *Routes elements*.

3. Change the value in the **Relative Cost** field.
4. Perform one of these actions:
   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.
   - Click **Cancel** to return to the **SS7/Sigtran > Configuration > Routes** page without saving any changes.

   The relative cost associated with the Route is updated. Changes to the RMU take effect in the next outgoing message after the **OK** button is clicked.

Deleting a Route

Deleting a Route removes the Route from the database.

1. Select **SS7/Sigtran > Configuration > Routes**.

   The **SS7/Sigtran > Configuration > Routes** page appears.

2. Click **Delete** in the row you want to remove.

   A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

Status of a Route

Use this procedure to view Status of the configured Route.

1. Select **SS7/Sigtran > Configuration > Routes**.

   The **SS7/Sigtran > Configuration > Routes** page appears.

2. Select the **Signaling Network Element Name** to check the status.

3. Click **Status**.

   The **SS7/Sigtran > Maintenance > Remote Signaling Points** page appears. See *Resetting the subsystem and point code status* and *Resetting the Network Status of the Routes* for the procedures.

Generating a report on Routes

Use this task to generate a report on one or all Routes.

1. Select **SS7/Sigtran > Configuration > Routes**.

   The **SS7/Sigtran > Configuration > Routes** page appears.

2. Perform one of these actions:

   - Click **Report** next to an entry in the table to generate a report on the entry.
   - Click the **Report** link at the bottom of the table to generate a report on all entries.

   The report opens in its own browser window. You can then use the browser to save the report or perform other operations.

SCCP Options

The **SCCP Options** page shows all of the configured SCCP options.

SCCP Options elements

Table 17: SCCP Options Elements describes the information on the **SS7/Sigtran > Configuration > SCCP Options** page.

Table 17: SCCP Options Elements

Variable	Description	Data Input Notes
Subsystem Test Interval	The number of seconds to delay after sending an SST (Subsystem Test) before sending the next SST.	Format: Numeric Range: 1 - 600 Default: 30
ANSI Default GTT Point Code	Default ANSI Global Title STP point code in format NNN-NNN-NNN. If the egress SCCP message request does not contain a destination point code and the CdPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Format: Pulldown list Range: Point Code must comply with ANSI T1.111.8
ITUI Default GTT Point Code	Default ITUI Global Title STP point code in format J-NNN-J. If the egress	Pulldown

Variable	Description	Data Input Notes
	SCCP message request does not contain a destination point code and the CdPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Range: 'J' can range from 0-7, 'NNN' can range from 0-255
ITUN Default GTT Point Code	Default ITUN Global Title STP point code in format NNNNN. If the egress SCCP message request does not contain a destination point code and the CdPA routing indicator indicates global title translation is required, then this point code will be used as the DPC of the egress message.	Format: Pulldown list Range: 'NNNNN' can range from 0 - 16383
ITUN24 Default GTT Point Code	**Note:** MD-IWF does not support ITUN24 - ITU National 24-bit point codes.	N/A
Reassembly Timeout(ITU)	Time period after receiving the first segment, while waiting to receive all the remaining segments related to same ITU XUDT segmented message.	Format: Text box Range: 10-20 seconds Default: 10
Reassembly Timeout(ANSI)	Time period after receiving the first segment, while waiting to receive all the remaining segments related to same ANSI XUDT segmented message.	Format: Text box Range: 5-20 seconds Default: 5
SCCP Address Length in Signaling Network	Maximum SCCP Address Length in operator's network, considering any intermediate translations and network conversations.	Format: Text box Range: 3-28 bytes Default: 19
Route on GT Action	Configuration option for enforcing the default translation handling in the SS7 application.	Format: Pulldown list Range: Error Procedure, Forward To Application Default: Error Procedure

Viewing SCCP Options

Use this procedure to view the SCCP Options.

Select **SS7/Sigtran > Configuration > SCCP Options**.

The **SS7/Sigtran > Configuration > SCCP Options** page appears with the SCCP Options listed.

For field definitions, see *SCCP Options elements*.

Editing an SCCP Option

Use this procedure to edit the values of the variables on the **SS7/Sigtran > Configuration > SCCP Options** page.

1. Select **SS7/Sigtran > Configuration > SCCP Options**.

   The **SS7/Sigtran > Configuration > SCCP Options** page appears.

2. In the **Value** field, make the desired changes. For field definitions, see *SCCP Options elements*.
3. Click **Apply** to save the data.

MTP3 Options

The **MTP3 Options** page shows the MTP3 timers and their current values. The page enables you to change the value association with a timer.

MTP3 Options elements

Table 18: MTP3 Options Elements describes the information on the **SS7/Sigtran > Configuration > MTP3 Options** page:

Table 18: MTP3 Options Elements

Element	Description	Data Input Notes
Timer T1	Changeover timer. This timer introduces a delay to help prevent message mis-sequencing on link changeover.	Format: Numeric Range: 10 - 2000 msecs Default: 60 msecs
Timer T3	Change-back timer. This timer introduces a delay to help prevent message mis-sequencing on link change-back.	Format: Numeric Range: 10 - 2000 msecs Default: 60 msecs
Timer T6	Controlled Rerouting timer. This timer introduces a delay to help prevent message mis-sequencing on controlled rerouting.	Format: Numeric Range: 10 - 2000 msecs Default: 60 msecs
Timer T10	Destination Audit interval. This timer controls the interval at which RST/DAUD messages are sent when destination audit is activated. Destination audit is activated on receipt of a TFP/DUNA. If a TFA/DAVA is	Format: Numeric Range: 1000 - 120000 msecs Default: 60000 msecs

Element	Description	Data Input Notes
	received, destination audit is deactivated.	
Timer T15	Destination Congestion Test Delay. This timer controls the length of the wait prior to starting the signaling route set congestion test.	Format: Numeric Range: 100 - 10000 msecs Default: 2000 msecs
Timer T16	Destination Congestion Test Timeout. This timer controls the length of the wait for the route set congestion status update.	Format: Numeric Range: 100 - 10000 msecs Default: 1000 msecs
SLS Rotation	This value specifies whether the SLS rotation procedure is enabled for egress messages. If SLS rotation is **Enabled**, the SLS value of messages will be rotated before routing the messages to network.	Format: Pulldown list Range: Disabled, Enabled Default: Enabled

Viewing MTP3 Options

Use this task to view MTP3 Options.

Select **SS7/Sigtran > Configuration > MTP3 Options**.

The **SS7/Sigtran > Configuration > MTP3 Options** page appears with the MTP3 options listed.

For field definitions, see *MTP3 Options elements*.

Editing MTP3 Options

Use this task to edit MTP3 Options.

1. Select **SS7/Sigtran > Configuration > MTP3 Options**.

   The **SS7/Sigtran > Configuration > MTP3 Options** page appears.

2. Make the desired changes. For field definitions, see *MTP3 Options elements*.
3. Click **Apply** to save the data.

   The changes are added to the configuration and will be used the next time a timer is started.

M3UA Options

The **M3UA Options** page shows the M3UA timers and their current values. The page enables you to change the value associated with a timer.

M3UA Options elements

Table 19: M3UA Options Elements describes the information on the **SS7/Sigtran > Configuration > M3UA Options** page:

Table 19: M3UA Options Elements

Element	Description	Data Input Notes
State Management ACK Timer	This timer controls how long M3UA waits for ASP state and traffic management message acknowledgements. If this timer expires, the message may be retransmitted. In the case of M3UA heartbeats, if no BEAT-ACK is received in two-times this value, the SCTP association will be restarted.	Format: Numeric Range: 200 - 1200 msecs Default: 800 msecs
M3UA Heartbeating	This value specifies whether M3UA heartbeating is enabled for all M3UA associations. If M3UA heartbeating is enabled, the **M3UA Heartbeat Interval** field specifies the rate at which M3UA heartbeats are sent.	Format: Pulldown list Range: Enabled, Disabled Default: Disabled.
M3UA Heartbeat Interval	This value is the interval at which M3UA BEAT messages will be sent on each association when M3UA heartbeating is enabled. This value has no meaning when M3UA heartbeating is disabled.	Format: Numeric Range: 100 - 10000 msecs Default: 5000 msecs

Viewing M3UA Options

Use this task to view M3UA Options.

Select **SS7/Sigtran > Configuration > M3UA Options**.

The **SS7/Sigtran > Configuration > M3UA Options** page appears with the M3UA Options listed..

For field definitions, see *M3UA Options elements*.

Editing M3UA Options

Use this task to edit M3UA Options..

1. Select **SS7/Sigtran > Configuration > M3UA Options**.

   The **SS7/Sigtran > Configuration > M3UA Options** page appears.

2. Make the desired changes. For field definitions, see *M3UA Options elements*.
3. Click **Apply** to save the data.

   The changes are added to the configuration. The new timer value will be used the next time the timer is started.

Local Congestion Options

The **SS7/Sigtran > Configuration > Local Congestion Options** page is a view-only list of the congestion management configuration parameters. There are two sets of parameters:

- The parameters that define the maximum capacities of the resources that are monitored by congestion management. The system automatically calculates the alarm onset and abatement thresholds from these maximum capacities. These parameters are the first nine parameters listed on the page (through **SCTP Aggregate Association Writer Queue Utilization**).
- The parameters that define the message treatment percentages for each MP congestion level. There are nine view-only configuration parameters; three for each MP congestion level (labeled CL1, CL2, and CL3).

Thresholds for minor, major, and critical alarms are based on a fixed percentage of the maximum configured value in the Local Congestion Options table:

Table 20: Alarm Severity for Onset and Abatement Thresholds

Severity	Onset %	Abate %
Minor	60	50
Major	80	70
Critical	95	90

Local Congestion Options elements

Table 21: Local Congestion Options Elements describes the information on the **SS7/Sigtran > Configuration > Local Congestion Options** page:

Table 21: Local Congestion Options Elements

Element	Description
Maximum SS7 Process CPU Utilization	The SS7 process is responsible for all SS7 processing on an MP. Thresholds for minor, major

Element	Description
	and critical alarms are based on a fixed percentage of this maximum value. Default: 90%
Maximum Ingress Message Rate	The ingress message rate measures the data messages (SI > 0) per second that the MP receives from the network. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 15,000 msgs/sec.
Maximum PDU Buffer Pool Size for ANSI	A Protocol Data Unit (PDU) buffer is allocated for each ANSI message that arrives at an MP and is de-allocated when message processing completes. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 11000 PDUs
Maximum PDU Buffer Pool Size for ITUI/ITUN/ITUN24	A Protocol Data Unit buffer is allocated for each ITUI message that arrives at an MP and is de-allocated when message processing completes. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 11000 PDUs
Maximum SCCP Stack Event Queue Size	The internal event queue to the SCCP Stack which is responsible for all SCCP sublayer processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 4,000 events
Maximum M3RL Stack Event Queue Size	The internal event queue to the M3RL stack, which is responsible for all M3RL non-management (SI > 0) processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 4,000 events
Maximum M3RL Network Management Event Queue Size	The internal event queue to M3RL Network Management which is responsible for all M3RL management (SI = 0) processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 1000 events

Element	Description
Maximum M3UA Stack Event Queue Size	The internal egress event queue to the M3UA Stack which is responsible for all M3UA Stack processing. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 2,000 events
Maximum SCTP Single Association Writer Queue Size	The internal egress event queue to an SCTP Association Handler which is responsible for all non-Linux SCTP sublayer processing for a individual SCTP association. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 1,000 events
Maximum SCTP Aggregate Association Writer Queue Size	The internal egress event queue used to limit the maximum number of egress messages queued on all SCTP Association Handler Threads. Thresholds for minor, major and critical alarms are based on a fixed percentage of this maximum value. Default: 10,000 events
CL1 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL1. Default: 80%
CL1 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and an SCCP UDTS/XUDTS response is sent (when requested by the originator) when the local MP congestion level is CL1. Default: 10%
CL1 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL1. Default: 10%
CL2 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL2. Default: 70%
CL2 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and an SCCP UDTS/XUDTS response is sent (when requested by the originator) when the local MP congestion level is CL2.

Element	Description
	Default: 10%
CL2 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL2. Default: 20%
CL3 Message Treatment - Normal	Percentage of ingress messages that will receive normal processing treatment when the local MP congestion level is CL3. Default: 60%
CL3 Message Treatment - Discard & Respond	Percentage of ingress messages that will be discarded and an SCCP UDTS/XUDTS response is sent (when requested by the originator) when the local MP congestion level is CL3. Default: 0%
CL3 Message Treatment - Discard Only	Percentage of ingress messages that will be discarded without any further processing when the local MP congestion level is CL3. Default: 40%

Viewing Local Congestion Options

Use this task to view Local Congestion Options.

Select **SS7/Sigtran > Configuration > Local Congestion Options**

The **SS7/Sigtran > Configuration > Local Congestion Options** page appears with the Local Congestion Options listed.

For field definitions, see *Local Congestion Options elements*.

Capacity Constraint Options

The **SS7/Sigtran > Configuration > Capacity Constraint Options** page shows the maximum and current capacity of each SS7 Constraint.

On the **SS7/Sigtran > Configuration > Capacity Constraint Options** page you can configure the following values:

- **Alarm At** - The value at which the alarm for a specific constraint needs to be raised
- **Alarm Severity** - The severity of the alarm to be raised
- **Alarm Enabled** - Enable or disable the alarm for a specific constraint

Click the **Apply** button at the bottom of the page to save your changes.

Capacity Constraint Options elements

Table 22: Capacity Constraint Options Elements describes the information on the **SS7/Sigtran > Configuration > Capacity Constraint Options** page:

Table 22: Capacity Constraint Options Elements

Element	Description
SS7 Constraint values	List of available constraint values: • Adjacent Server Groups Per Site • Adjacent Servers Per Adjacent Server Group • SCTP Association Per MP Server • LSPs Per Site • LSUs Per LSP • Links Per Association • Links Per Linkset • Links Per Site • Linksets Per Site • RMUs Per Site • RSPs Per Site • Routes Per RSP Per MP • Routes Per Site • Server Groups Per LSP • Server Groups Per Site • Servers Per MP Server Group • Adjacent Servers Per Site • SCTP Association Configuration Sets Per Site • SCTP Associations Per Site
Maximum Capacity	Maximum capacity supported by the system.
Current Capacity	Capacity used by the current system configuration.
Alarm At	Use this field to set the value at which the specified alarm will be raised.
Alarm Severity	Use this pulldown list to select the alarm severity value.
Alarm Enabled	Use this check box to enable the specified alarm.
Apply	Use this button to apply your selections.

Table 23: SS7 Constraint Values lists the SS7 constraint value details:

Table 23: SS7 Constraint Values

Value	Description
AdjSvrGrpsPerSite	Number of Adjacent Server Groups (STPs) supported per SOAM pair.
AdjSvrsPerAdjSvrGrp	Number of Adjacent Nodes (Servers) supported in an Adjacent Server group (STP).
AdjNodesPerSite (AdjSvrsPerSite)	Number of Adjacent Nodes (Adjacent Servers) supported per SOAM pair.
LinksetsPerSite	Number of SS7 linksets supported per SOAM pair.
LinksPerAssociation	Number of SS7 links supported per SCTP association.
LinksPerLinkset	Number of links supported per linkset.
LinksPerSite	Numbers of SS7 links supported per SOAM pair.
LSPsPerSite	Number of LSPs supported per SOAM pair.
RMUsPerSite	Numbers of RMUs supported per SOAM pair
RoutesPerRSPPerMP	Number of SS7 Routes supported per RSP on one MP.
RoutesPerSite	Number of SS7 Routes supported per SOAM pair.
RSPsPerSite	Number of RSPs supported per SOAM pair.
TransConfigsPerSystem (SCTPAssocConfigsPerSystem)	Number of Transport Configuration Sets supported per System.
AssocPerSvr (SCTPAssocPerMP)	Number of SCTP associations supported per MP server.
TransportsPerSite (SCTPAssocPerSite)	Number of Transports (SCTP associations) supported per SOAM pair.
ServerGroupsPerLSP	Number of Server Groups per LSP
ServerGroupsPerSite	Number of Server groups (MPs) supported per SOAM pair.
ServersPerMP	Number of servers per MP.

Viewing Capacity Constraint Options

Use this task to view Capacity Constraint Options.

Select **SS7/Sigtran > Configuration > Capacity Constraint Options**

The **SS7/Sigtran > Configuration > Capacity Constraint Options** page appears.

For field definitions, see *Viewing Capacity Constraint Options*.

Chapter 4

SS7 maintenance

Topics:

SS7 Maintenance provides maintenance and troubleshooting capabilities on Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, and Links.

The SS7 Maintenance menu

The **SS7/Sigtran > Maintenance** GUI pages provides maintenance and troubleshooting capabilities on Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, and Links.

The Maintenance information is helpful under alarm conditions as a starting point for gathering additional information. For example, the maintenance pages display the timestamp when a Link Set or Link goes down. The timestamp can then be used to narrow the search in the event history log and measurements reports.

Errors, warnings, and the possible need for maintenance activity are shown in the GUI pages as colored cells so that the conditions are readily identifiable.

After rudimentary information for troubleshooting has been obtained, the network operator can continue investigating under the **Alarms & Events** and **Measurements** options on the GUI.

The menu also enables you to perform maintenance-related tasks such as:

- Enabling and disabling Links.
- Resetting the network status of Routes.
- Resetting the MP's SCCP status of the subsystem and point code.
- Enabling and disabling LSUs.

Status information is obtained on the system through a collection processed by the SOAM server collects data from the MP servers.

A user group must have permissions to view or execute any of the procedures on the **SS7/Sigtran Maintenance** menu. If a group does not have permissions for the **Maintenance** menu options for **Local SCCP Users**, **Remote Signaling Points**, **Remote MTP3 Users**, **Link Sets**, or **Links**, these options will not appear in the GUI.

SS7 maintenance is available from the SOAM. All maintenance links are active when the user is connected to the SOAM.

Color codes on the Maintenance pages

The colors on the **SS7/Sigtran > Maintenance** pages alert the network operator to potential problems:

Table 24: Maintenance Page Color Codes

Color	Description
Red background	Indicates an error.
Orange background	Indicates maintenance activity.
Yellow background	Used for warnings such as congestion or some of the links in a link set are down.

Color	Description
Gray background	Indicates that conditions are normal.
Gray text	If status cannot be collected from an MP server, cells with gray text indicate the last known information reported from the server.

Local SCCP Users Maintenance

The **Local SCCP Users Maintenance** page shows the status of each configured LSU.

Colored cells may indicate the need for maintenance activity. If status cannot be collected from a server, cells with gray text indicate the last known information reported from the server.

Local SCCP Users Maintenance elements

Table 25: Local SCCP Users Maintenance Elements describes the information on the **SS7/Sigtran > Maintenance > Local SCCP Users** page.

Table 25: Local SCCP Users Maintenance Elements

Element	Description
Signaling Network Element Name	The Signaling Network Element Name to which the Local SCCP User is associated.
SSN	The subsystem number served by this Local SCCP User.
(Local Signaling Point) Point Code	The point code of the Local Signaling Point associated with this Local SCCP User.
(Local Signaling Point) SS7 Domain	The SS7 domain of the Local Signaling Point.
Application Name	Application Name associated with the Local SCCP User.
SSN Status	The SSN Status. Possible values are **Enabled** and **Disabled**. These values indicate whether the Local SCCP subsystem is enabled or disabled. The user can manually disable an LSU (see *Disabling a Local SCCP User*).The Local SCCP subsystem will also be automatically disabled under the following conditions: • When SCCP receives a notification from the OAM subsystem that a Local Subsystem and SCCP User have been added to the MP's database.

Element	Description
	• In some cases, when SCCP receives a notification from the OAM Subsystem that an enabled Local Subsystem and SCCP User have been deleted from the MP database. The user can manually enable an LSU (see *Enabling a Local SCCP User*). When SCCP receives a notification from the OAM subsystem that a local SCCP user has been enabled, SCCP sets the subsystem status to **Enabled**.
Up/Down Since	Indicates the time when the LSU status was changed.
Pause updates	Unchecked by default to refresh every 15 seconds. Checked will stop the updates.

Viewing Local SCCP Users status

Use this procedure to view status information for Local SCCP Userss.

1. Select **SS7/Sigtran > Maintenance > Local SCCP Users**.

   The **SS7/Sigtran > Maintenance > Local SCCP Users** page appears. For field definitions, see *Local SCCP Users Maintenance elements*.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.

Enabling a Local SCCP User

The **Enable** command causes SCCP to set the Local SCCP subsystem status to **Enabled**.

LSUs must be enabled one LSU at a time.

1. Select **SS7/Sigtran > Maintenance > Local SCCP Users**.

   The **SS7/Sigtran > Maintenance > Local SCCP Users** page appears.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.

3. Click **Enable** in the row of the appropriate LSU.
   A confirmation message appears.

   The MP server will disregard the command if the LSU is already in the **Enabled** state.

4. Click **OK** to confirm.
   The **SSN Status** field changes to **Enabled**.

   The LSU is enabled. The **Up/Down Since** column now indicates when the LSU transitioned into the **Enabled** state.

Disabling a Local SCCP User

The **Disable** command causes the status of the Local SCCP subsystem to change to **Disabled**.

LSUs must be disabled one LSU at a time.

1. Select **SS7/Sigtran > Maintenance > Local SCCP User**.

   The **SS7/Sigtran > Maintenance > Local SCCP Users** page appears.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.

3. Click **Disable** in the row of the appropriate LSU.

   The MP server will disregard the command if the LSU is already in the **Disabled** state.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **SSN Status** field changes to **Disabled**, and the cell turns red.

   The LSU is disabled. The **Up/Down Since** column now indicates when the LSU transitioned into the **Disabled** state.

Remote Signaling Points Maintenance

The **SS7/Sigtran > Maintenance > Remote Signaling Points** page shows the status of each configured RSP and the Routes to that RSP. The status information is shown from the perspective of each MP at the site.

Each RSP can have up to two Routes. The Route status is divided into link set status and network status. The network status is the status of the RSP as reported from the network via the STP.

The **Reset** action resets the MP's view of the network status of both routes to Available. This action allows the network operator to attempt signaling on the routes.

Colored cells may indicate the need for maintenance activity. If status cannot be collected from a server, cells with gray text indicate the last known information reported from the server.

Remote Signaling Points Maintenance elements

Table 12: Remote Signaling Points Elements describes the information on the **SS7/Sigtran > Maintenance > Remote Signaling Points** page.

Table 26: Remote Signaling Points Maintenance Elements

Element	Description
Remote Point Code	The point code for this RSP.
SS7 Domain	The SS7 domain of the RSP.

Element	Description
RSP Status	RSP Status is an aggregation of the statuses for Route 1 and Route 2. The intent is to display the MP server's ability to signal to the RSP. Possible values are: • **Available**-at least one route is available. • **Unavailable**-both routes are down/unavailable. • **Congested**-a report has been received from the network that the RSP is congested, but not unavailable. • **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state. • **Non-Preferred**-the lower cost route is down/unavailable, causing signaling to use the non-preferred route. • **Application Disabled**-the application has been manually disabled via the **Server Status** page.
Route X Status, where Route X is Route 1 or Route 2	Route Status is an aggregation of **Link Set Status** and **Network Status**. If either the **Link Set Status** is **Down** or the **Network Status** is **Unavailable**, the route is **Unavailable**.
Link Set Status	Corresponds to the status of the Link Set that the Route is configured to use, as shown on the **Link Set Maintenance** page. Possible values are **Up** or **Down**. If **Down**, more information can be found on the **Link Set Maintenance** page. For information on Link Set Maintenance, see *Link Set Maintenance*.
Network Status	Indicates the Route status reported from the network. Possible values are **Available** or **Unavailable**. **Unavailable** means that a DUNA/TFP was received from a signaling gateway indicating that the RSP is not accessible from that signaling gateway. A restricted route is displayed as available.
Time of Last Status Change	Indicates the last time when any status change occurred on this row, including changes for the RSP status and the link set and network status for Route 1 and Route 2.
MP Server Hostname	The hostname of the MP server reporting the status.

Element	Description
Route X Details, where Route X is Route 1 or Route 2	Route Details provides detailed information about Route 1 and Route 2.
Route Cost	The cost associated with the Route.
Link Set Name	The Link Set associated with the Route.
Adjacent Point Code	The Adjacent Point Code associated with the Route.
Pause updates	Unchecked by default to refresh every 15 seconds. Checked will stop the updates.

Viewing Remote Signaling Points status

Use this task to view status information for Remote Signaling Points.

1. Select **SS7/Sigtran > Maintenance > Remote Signaling Points**.

   The **SS7/Sigtran > Maintenance > Remote Signaling Points** page appears. For field definitions, see *Remote Signaling Points Maintenance elements*.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.

About resetting the Network Status of the routes

The **Reset** action allows the network operator to reset the MP server's view of the **Network Status** for both Routes to **Available**. If the **Link Set Status** values for the two Routes do not prevent signaling, then both Routes (and the RSP) will become available for signaling. The **Link Set Status** is not affected by the **Reset** action. Resetting the **Network Status** for the Routes may cause the **RSP Status** to change.

Reset should be used only in cases in which the network operator suspects that a DAVA/TFA management message may have been lost so that the MP has a stale view of the true network status. If **Reset** is used and the **Network Status** was correct (was Unavailable), then response method signaling will set the **Network Status** back to the correct value. Clicking **Reset** when the route **Network Status** is already Available has no effect.

Reset can also be used to reset the MP's view of the RSP's congestion status. In other words, **Reset** will make the MP server think that the RSP is no longer congested. Again, if the RSP really is congested, response method signaling may set it back to Congested.

Reset has no effect on an RSP for which both Routes are Up/Available and the RSP is not congested.

Resetting the Network Status of the Routes

Use this task to reset the Network Status of the Routes.

1. Select **SS7/Sigtran > Maintenance > Remote Signaling Points**.

   The **SS7/Sigtran > Maintenance > Remote Signaling Points** page appears.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.
3. Click **Reset** in the row of the appropriate Route.

   A confirmation message appears.
4. Click **OK** to confirm.

   The **Network Status** field shows **Available**.

Remote MTP3 Users Maintenance

The **SS7/Sigtran > Maintenance > Remote MTP3 Users** page shows the Operational Status of each configured RMU. The subsystem statuses are shown from the perspective of each MP server.

The **Reset** action causes the MP's view of the remote subsystem to be reset, allowing signaling attempts to occur.

Colored cells may indicate the need for maintenance activity. If status cannot be collected from a server, cells with gray text indicate the last known information reported from the server.

Remote MTP3 Users Maintenance elements

Table 27: Remote MTP3 Users Maintenance Elements describes the information on the **SS7/Sigtran > Maintenance > Remote MTP3 Users** page.

Table 27: Remote MTP3 Users Maintenance Elements

Element	Description
Remote Point Code	The Remote Point Code associated with the RMU.
SS7 Domain	The SS7 domain of the RMU.
Remote SSN	The Remote Subsystem Number whose status is being tracked.
MP Server Hostname	The hostname of the MP server reporting the status.
Operational Status	RMU status is an aggregation of the Remote PC and Remote SSN status that indicates the MP's ability to signal to the specified RMU. Possible values are: • **Available**-the RMU is *available* (none of the conditions for **Unavailable** is true). A congested point code can have a status of **Available**. • **Unavailable**-the SSN is prohibited or the point code is unavailable.

Element	Description
Operational SSN Reason	Shows one of these values: • **Normal**-the MP server thinks the RMU's subsystem is fully accessible for SCCP signaling. • **Prohibited**-an SSP was received for the point code and subsystem. • **Unknown**- DUPU/UPU was received for the point code indicating that SCCP is unavailable on that RSP. • **Application Disabled** -the application has been manually disabled via the **Server Status** page. • **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state. A value of ITU subsystem congestion (SSC) is not yet supported.
Operational Point Code Reason	Shows one of these values: • **Normal**-the point code is *normal* (none of the other conditions listed in this section is true). • **User Part Unavailable**-an MTP-Status indicating user part unavailable or unknown is received from the signaling gateway. • **Point Code Paused**-SCCP received an MTP-Pause indicating that the point code is inaccessible for signaling. • **Congested**-an MTP-Status message is received indicating that the point code is congested. • **Application Disabled** -the application has been manually disabled via the **Server Status** page. • **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.
Available/Unavailable Since	Indicates the last time when the operational status changed.
Pause updates	Unchecked by default to refresh every 15 seconds. Checked will stop the updates.

Viewing Remote MTP3 Users status

Use this procedure to view status information for Remote MTP3 Users.

1. Select **SS7/Sigtran > Maintenance > Remote MTP3 Users**.

   The **SS7/Sigtran > Maintenance > Remote MTP3 Users** page appears. For field definitions, see *Remote MTP3 Users Maintenance elements*.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.

About resetting the subsystem and point code status

The **Reset** action enables the network operator to reset the MP's SCCP view of the SSN status to allowed and the point code status to available.

Reset should be used only if the network operator suspects that an SSA or MTP-Resume management message may have been lost, resulting in the MP server having a stale view of the true network status. If **Reset** is used and the network status was correct (was really Unavailable), then response method signaling will set the network status back to the correct value.

Reset can also be used to reset the MP's view of the point code's congestion status. In other words, **Reset** will make the MP server SCCP think that the point code is no longer congested. Again, if the point code really is congested, response method signaling may set it back to Congested. **Reset** has no effect on an RMU for which both **SSN Reason** and **PC Reason** are Normal.

Resetting the subsystem and point code status

Use this task to reset the subsystem and point code status.

1. Select **SS7/Sigtran > Maintenance > Remote MTP3 Users**.

   The **SS7/Sigtran > Maintenance > Remote MTP3 Users** page appears.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner). It is unchecked by default.
3. Click **Reset** in the row of the appropriate route.

   A confirmation message appears.

4. Click **OK** to confirm.
   The SSN status is reset to Allowed. The point code status is reset to Available.

Link Set Maintenance

The **SS7/Sigtran > Maintenance > Link Sets** page shows status information for each Link Set as viewed by each MP server. Each MP server reports status only for Link Sets hosted by that MP server (Link Sets that include Links that use Associations hosted by the MP server).

Each Link Set's Operational Status and the reason for the Operational Status are shown.

The **SS7/Sigtran > Maintenance > Link Sets** page does not distinguish between links down for maintenance and links down due to errors. Colored cells may indicate the need for maintenance activity. When the server's collection status is Unknown, cells with gray text indicate the last known information about the Link Set.

For additional details on Link status, see *Link Maintenance*.

Link Set Maintenance elements

Table 28: Link Sets Maintenance Elements describes information on the **SS7/Sigtran > Maintenance > Link Sets** page:

Table 28: Link Sets Maintenance Elements

Element	Description
Signaling Network Element Name	The name of the Signaling Network Element associated with the Link Set.
Link Set Name	The name that identifies this Link Set.
MP Server Hostname	The hostname for the MP server.
Local Signaling Point	The LSP associated with the Link Set.
SS7 Domain	The SS7 domain of the LSP.
Adjacent Remote Point Code	The point code of the Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway to be served by this Link Set.
Operational Status	The operational status of the Link Set: **Down** or **Up**. Link Set status is reported per MP server, meaning each MP reports its view of the Link Set. There is no aggregated view.
Operational Reason	The reason a given operational status is shown. For information on a value listed in this field, see *Link Set Operational Status and Reason*.
MP Server HA Status	The high availability status of the MP server: **Active** or **Standby**.
Up/Down Since	The date and time that the Link Set came up or went down. After a database restart, reboot, or initial startup before the Associations and Links are initialized, the value is the time when the application initialization runs.
Pause updates	Unchecked by default to refresh every 15 seconds. Checked will stop the updates.

Link Set Operational Status and Reason

This list shows the possible values that may appear in the **Operational Status** and **Operational Reason** fields of the **SS7/Sigtran > Maintenance > Link Sets** page. The **Operational Status** is either **Up** or **Down**. **Up** indicates that the Link Set can be used for signaling. **Down** indicates that the Link Set cannot be used for signaling. If the **Status** is **Down**, the **Operational Reason** provides information about why it is down.

Possible values of the **Operational Reason** field where **Status=Down** are:

- **Application Disabled**-the MP server's application Administrative State has been manually **Disabled** via the **Server Status** page.
- **All Links Normal**-this status occurs when all of the configured Links that reference this Link Set are reporting an Operational Reason of **Normal**.
- **Forced Standby**-the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.
- **No Link Defined**-a link is not defined for the link set.
- **0 of N Links Normal**-all Links configured on this MP for this Link Set are reporting an Operational Reason other than **Normal**.

Possible values of the **Operational Reason** field where **Status=Up** are:

- **All Links Normal**-this is the desired status of the server. This status occurs when all of the configured Links that reference this Link Set are reporting an Operational Reason of **Normal**.
- **M of N Links Normal**-some of the configured Links on an MP server that reference this Link Set are reporting an Operational Reason of **Normal**. **N** represents the sum of Links on the MP server that belong to the Link Set. **M** represents the subset of **N** that are reporting an Operational Reason of **Normal**.

Viewing Link Set status

Use this procedure to view information on the Operational Status of a Link Set.

Select **SS7/Sigtran > Maintenance > Link Sets**

The **SS7/Sigtran > Maintenance > Link Sets** page appears. For field definitions, see *Link Set Maintenance elements*

Link Maintenance

The**SS7/Sigtran > Maintenance > Links** page shows the Administrative State and Operational Status of each SS7 Link. The Administrative State is either **Enabled** or **Disabled**. The Operational Status is either **Up** or **Down**.

Each MP server reports status only for Links hosted by that MP server.

Colored cells may indicate the need for maintenance activity. Red cells indicate failures. Orange cells indicate maintenance conditions. When the active server's collection status is Unknown, cells with gray text indicate the last known information about the Link.

You can obtain additional information about the Link status by viewing the status of the Transport that hosts the link (refer to the *Transport Manager User's Guide* and Help).

Links Maintenance elements

Table 29: Links Maintenance Elements describes the information on the **SS7/Sigtran > Maintenance > Links** page:

Table 29: Links Maintenance Elements

Element	Description
Signaling Network Element Name	The Signaling Network Element associated with the Link.
Link Name	The name that identifies this Link.
Link Set	The name that identifies this Link Set.
MP Server Hostname	The hostname for the MP server associated with this Link.
Admin State	Shows the Link's administrative state: **Enabled** or **Disabled**. In the **Enabled** administrative state, the Link is in the ASP-Active state on an active MP server or the ASP-INACTIVE state on a standby MP server. In the **Disabled** administrative state, the Link is in the ASP-INACTIVE state on the MP server and is unavailable for Sigtran signaling. When a new Link is configured, the Link is in the **Disabled** administrative state. The Link must be placed in the **Enabled** administrative state to bring the Link up. Orange color highlights the administrative state when it is **Disabled**.
Operational Status	The operational status of the Link: **Up** or **Down**.
Operational Reason	The reason a given operational status is shown. For information on a value listed in this field, see *Link Operational Status and Reason*.
MP Server HA Status	The high availability status of the MP server: **Active** or **Standby**.
Up/Down Since	The date and time that the Link came up or went down. For a newly added Link, the time is when the Link was configured. After a database restart, reboot, or initial startup before the Associations and Links are initialized, the value is the time when the application initialization runs.
Pause updates	Unchecked by default to refresh every 15 seconds. Checked will stop the updates.

Link Operational Status and Reason

This list shows the possible values that may appear in the **Operational Status** and **Reason** fields of the **SS7/Sigtran > Maintenance > Links** page. The **Operational Status** of a Link is either **Up** or **Down**. **Up** indicates that the Link is available for signaling. **Down** indicates the Link is not available for signaling. If the status is **Down**, the **Operational Reason** provides information about why it is down.

Possible values of the **Operational Reason** field where **Status=Down** are:

- **Disabled**-the Link's administrative state is **Disabled**. This is the initial operational status and reason for a newly configured Link. This reason is also shown when a link is manually disabled.
- **Application Disabled**-the Link's administrative state is **Enabled** and the server's application administrative state has been manually **Disabled** via the **Server Status** page.
- **Association Down**-the Link's administrative state is **Enabled**, but the Link's Association is in any of these **Down** states: Down/Disabled, Down/Connecting, Down/Blocked, or Down/Up Pending.
- **Forced Standby**-the Link's administrative state is **Enabled** and the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.
- **Up Pending**-the Link's administrative state is **Enabled**, but the ASP-ACTIVE-ACK has not yet been received.

Possible values of the **Operational Reason** field where **Status=Up** are:

- **Normal**-this status occurs when the administrative state is **Enabled** and the ASP-ACTIVE-ACK has been received.

Viewing Link status

Use this procedure to view information on the Administrative State and Operational Status of a Link.

1. Select **SS7/Sigtran > Maintenance > Links**.

   The **SS7/Sigtran > Maintenance > Links** page appears. For field definitions, see *Links Maintenance elements*.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner).

   It is unchecked by default.

Enabling a Link

Use this task to enable a link.

When a Link is put in the **Enabled** administrative state, the MP server begins attempts to bring the Link to the ASP-ACTIVE state on an active MP server or the ASP-INACTIVE state on a standby MP server.

Links must be enabled one Link at a time.

1. Select **SS7/Sigtran > Maintenance > Links**.

   The **SS7/Sigtran > Maintenance > Links** page appears.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner).

It is unchecked by default.

3. Click **Enable** in the row of the appropriate Link.

   The MP server will disregard the command if the Link is already in the selected administrative state.

   If the link you wish to enable is missing or displayed in gray text, it indicates a management network problem between the MP server and the SOAM server from which your GUI session is hosted.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Link transitioned into the **Up** status. The **Enable** action is now grayed out.

Disabling a Link

Use this task to disable a link.

Caution: Disabling a Link causes a Link alarm, and possibly, alarms for Link Sets, Routes, or node isolation.

When a Link is put in the **Disabled** administrative state, the MP server begins attempts to place the Link in the ASP-INACTIVE state. Placing a Link in the **Disabled** administrative state makes the Link unavailable for SS7/Sigtran signaling.

Links must be disabled one Link at a time.

1. Select **SS7/Sigtran>Maintenance > Links**.

   The **SS7/Sigtran>Maintenance > Links** page appears.

2. Check the **Pause updates** box to stop the 15 second auto refresh for the page (lower right corner).

   It is unchecked by default.

3. Click **Disable** in the row of the appropriate Link.

   If the **Disable** link is grayed out, the Link's administrative state is already **Disabled**. Also if collection on the server is not working, both the **Enable** and **Disable** links are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Link is already in the selected administrative state.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Link transitioned into the **Up** status. The **Enable** action is now grayed out.

Chapter 5

Command Line Interface

Topics:

The **SS7/Sigtran > Command Line Interface > Command Import** page provides a method for bulk loading SS7 configuration data. The **SS7/Sigtran > Command Line Interface > Command Import** page allows you to validate and execute command scripts. Validation and execution results are written to log files in the file management area.

The following types of data can be configured on the **SS7/Sigtran > Command Line Interface > Command Import** page:

- Adjacent Server Groups
- Local Signaling Points
- Remote Signaling Points
- Remote MTP3 Users
- Links
- Link Sets
- Routes
- Local SCCP Users

Command Import elements

Table 30: Command Import Elements describes the information on the **SS7/Sigtran > Command Line Interface > Command Import** page:

Table 30: Command Import Elements

Element	Description	Data Input Notes
Command Script Location	A file selection field used to locate commands.	Format: Text box
Validate	Validates the command script when the user selects **Submit**.	Format: Radio button **Note:** Validate is the default value.
Execute	Executes the command script when the user selects **Submit**.	Format: Radio button
Submit	Initiates either the validation or execution of the selected command script.	Format: Button

Validating commands

Use this procedure to validate commands.

Only the syntax of input commands is validated. For example, the validation function validates command format, verifies that the operation is supported for the managed object, and confirms that all required attributes are present. It does not validate field values.

1. Select **SS7/Sigtran > Command Line Interface > Command Import.**
   The **SS7/Sigtran > Command Line Interface > Command Import** page appears.
2. Click **Browse** to select a file.

   The file browse dialog appears.
3. Select the file that you want to validate.
4. Click **Open**.
   The file appears in the **Command Script Location** field.
5. Select the **Validate** radio button, and click **Submit**.
   The file is validated and results are exported to a Command Validation Results TXT file, which is stored in the File Management Area. The results can also be accessed through the link in the work area of the **SS7/Sigtran > Command Line Interface > Command Import** page.
6. Click the link that appears in the work area of the **SS7/Sigtran > Command Line Interface > Command Import** page to view the Command Validation Results file.

If the link is clicked immediately after submit, the validation may not be complete, and a partial file may be displayed.

Note: If you navigate away from the **SS7/Sigtran > Command Line Interface > Command Import** page, the link will no longer be available.

The Command Validation Results file opens.

An example Command Validation Results file is shown in *Command Execution Results*.

The elements in the Command Validation Results file are described in *Command Execution Results elements*.

Command Validation Results

Results from command script validation are written to a TXT file. The naming convention of the file is <*filename*>.<*timestamp*>.txt, where <*filename*> is the name portion of the selected command script file and <*timestamp*> is the time in UTC that the results file was created.

```
================================================================================
Command Validation Results
================================================================================
Report Generated: Fri Aug 06 17:20:18 2010 UTC
From: Active NETWORK_OAMP on host XGNO
Report Version: 3.0.0-3.0.0_30.5.0
User: guiadmin

------------------------------------------------
Command Validation Details

08/06/2010 17:20:18:883 1 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=
08/06/2010 17:20:18:883 1 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:883 2 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=10.250.52.54
08/06/2010 17:20:18:884 2 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: adjserver

08/06/2010 17:20:18:884 4 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
 ADJSERVERS=
08/06/2010 17:20:18:884 4 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:885 5 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
 ADJSERVERS=AS_01
08/06/2010 17:20:18:885 5 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: asgroup

08/06/2010 17:20:18:886 7 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=
08/06/2010 17:20:18:886 7 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:18:887 8 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=SG_MP
08/06/2010 17:20:18:887 8 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: lsp

08/06/2010 17:20:18:888 10 FAILED: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
```

```
 DOMAIN=ITUI: SSN=5: APPLICATION=
08/06/2010 17:20:18:888 10 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:889 11 SUCCESS: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=TCAP
08/06/2010 17:20:18:890 13 FAILED: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=
08/06/2010 17:20:18:890 13 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:891 14 SUCCESS: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=itui: asgroup=AdjServGrp1
08/06/2010 17:20:18:892 16 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-006-6:DOMAIN=ITUI: SSN=
08/06/2010 17:20:18:892 16 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:893 17 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN= : SSN=5
08/06/2010 17:20:18:893 17 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:894 18 SUCCESS: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN=ITUI: SSN=5
08/06/2010 17:20:18:895 20 FAILED: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
 LSP=ITUI_1_001_1: POINTCODE
08/06/2010 17:20:18:895 20 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:896 21 SUCCESS: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
 LSP=ITUI_1_001_1: POINTCODE=6-006-6: DOMAIN=ITUI: ASSIGNRC=no
08/06/2010 17:20:18:897 23 FAILED: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=
08/06/2010 17:20:18:897 23 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:898 24 SUCCESS: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=192.168.67.151
08/06/2010 17:20:18:899 26 FAILED: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=
08/06/2010 17:20:18:899 26 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:900 27 SUCCESS: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=LS_01: ASSOCIATION=AssocTest1
08/06/2010 17:20:18:901 29 FAILED: INSERT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-006-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:18:901 29 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:902 30 SUCCESS: INSERT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-6-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=5
08/06/2010 17:20:18:903 32 FAILED: EDIT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-006-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:18:903 32 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:904 33 SUCCESS: EDIT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-006-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=10
08/06/2010 17:20:18:905 35 FAILED: DELETE: ROUTE: POINTCODE=
08/06/2010 17:20:18:905 35 ***ERROR*** [Error Code 10095] - Invalid command
syntax.
```

```
08/06/2010 17:20:18:906 36 SUCCESS: DELETE: ROUTE: POINTCODE=6-006-6: DOMAIN=ITUI:
 LINKSET=LS_01
08/06/2010 17:20:18:907 38 FAILED: DELETE: LINK: NAME=
08/06/2010 17:20:18:907 38 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:908 39 SUCCESS: DELETE: LINK: NAME=Link1: FORCE=1
08/06/2010 17:20:18:909 41 FAILED: DELETE: ASSOCIATION: NAME=
08/06/2010 17:20:18:909 41 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:910 42 SUCCESS: DELETE: ASSOCIATION: NAME=AssocTest1: FORCE=1
08/06/2010 17:20:18:911 44 FAILED: DELETE: LINKSET: NAME=
08/06/2010 17:20:18:911 44 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:912 45 SUCCESS: DELETE: LINKSET: NAME=LS_01
08/06/2010 17:20:18:913 47 FAILED: DELETE: RMU: POINTCODE=6-006-6: DOMAIN=ITUI:
08/06/2010 17:20:18:914 47 ***ERROR*** [Error Code 001] - Missing Field Value:
ssn

08/06/2010 17:20:18:914 48 SUCCESS: DELETE: RMU: POINTCODE=6-6-6: DOMAIN=ITUI:
SSN=5
08/06/2010 17:20:18:915 50 FAILED: DELETE: RSP: pointcode=6-6-6
08/06/2010 17:20:18:916 50 ***ERROR*** [Error Code 001] - Missing Field Value:
domain

08/06/2010 17:20:18:916 51 SUCCESS: DELETE: RSP: pointcode=6-006-6: domain=itui
08/06/2010 17:20:18:917 53 FAILED: Delete: Lsu: Pointcode=1-001-1: Domain=ITUI:
 Ssn=
08/06/2010 17:20:18:917 53 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:918 54 SUCCESS: Delete: Lsu: Pointcode=1-1-1: Domain=ITUI:
Ssn=5: Force=1
08/06/2010 17:20:18:919 56 FAILED: DELETE: LSP: NAME=
08/06/2010 17:20:18:919 56 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:920 57 FAILED: DELETE: LSP: NAME=LSP_01
08/06/2010 17:20:18:920 57 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: lsp

08/06/2010 17:20:18:921 59 FAILED: DELETE: ASGROUP: NAME=
08/06/2010 17:20:18:921 59 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:922 60 FAILED: DELETE: ASGROUP: NAME=ASG_01
08/06/2010 17:20:18:922 60 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: asgroup

08/06/2010 17:20:18:923 62 FAILED: DELETE: ADJSERVER: NAME=
08/06/2010 17:20:18:923 62 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:18:924 63 FAILED: DELETE: ADJSERVER: NAME=AS_01
08/06/2010 17:20:18:924 63 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: adjserver


------------------------------------------------
Command Validation Summary

Input File: cli_commands.txt
```

```
Number of Commands Executed:    43
Number of Commands Succeeded:   15
Number of Commands Failed:      28

--------------------------------------------------------------------------------
End of Command Validation Results
================================================================================
```

Figure 13: Example Command Validation Results file

Command Validation Results elements

Results from command script validation are written to a TXT file. *Table 31: Command Validation Results* describes the elements of the Command Validation Results file.

Table 31: Command Validation Results

Element	Description
Command Validation Results	Displays the following information: • Time the report was generated • Server name • Report version number • User name
Command Validation Details	Output in the details section of the results file displays: • UTC timestamp in millisecond format: MM/DD/YYYY hh:mm:ss:uuu • Corresponding line number from the input file • Command statements from the input file • Successfully validated commands are preceded by: SUCCESS • Failed commands are preceded by: FAILED • Failed commands are followed by a line that begins: ***ERROR*** [Error Code <number>] - <error code text> • Comments from the input file, if applicable • Comments are preceded by: Comment
Command Validation Summary	Output in the summary section of the file displays: • Name of the input file • Number of commands validated • Number of commands succeeded • Number of commands failed

Element	Description
	• If a fatal error occurs, the script is terminated, and the summary will contain this message: ***SCRIPT ABORTED DUE TO ERROR***

Executing commands

Use this procedure to execute commands.

1. Select **SS7/Sigtran > Command Line Inteface > Command Import.**
   The **SS7/Sigtran > Command Line Inteface > Command Import** page appears.
2. Click **Browse** to select a file.

   The file browse dialog appears.
3. Select the file you want to execute.
4. Click **Open**.
   The file appears in the **Command Script Location** field.
5. Select the **Execute** radio button and click **Submit**.
   The commands in the file are executed and results are exported to a Command Execution Results TXT file, which is stored in the file management area. The results can also be accessed through the link in the work area of the **SS7/Sigtran > Command Line Inteface > Command Import** page.
6. Click the link that appears in the work area of the **SS7/Sigtran > Command Line Inteface > Command Import** page to view the Command Execution Results file.

   If the link is clicked immediately after submit, the validation may not be complete, and a partial file may be displayed.

   Note: If you navigate away from the **SS7/Sigtran > Command Line Inteface > Command Import** page, the link will no longer be available.

   The Command Execution Results file opens.

   An example Command Execution Results file is shown in *Command Execution Results*.

   The elements in the Command Execution Results file are described in *Command Execution Results elements*.

Command Execution Results

Results from command script execution are written to a TXT file. The naming convention of the file is <*filename*>.<*timestamp*>.txt, where <*filename*> is the name portion of the selected command script file and <*timestamp*> is the time in UTC that the results file was created.

```
================================================================================
Command Execution Results
================================================================================
Report Generated: Fri Aug 06 17:20:56 2010 UTC
```

```
From: Active NETWORK_OAMP on host XGNO
Report Version: 3.0.0-3.0.0_30.5.0
User: guiadmin

-----------------------------------------------
Command Execution Details

08/06/2010 17:20:57:544 1 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=
08/06/2010 17:20:57:544 1 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:546 2 FAILED: INSERT: ADJSERVER: NENAME=Sig_OAM: NAME=AS_01:
 IPADDRESS=10.250.52.54
08/06/2010 17:20:57:546 2 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: adjserver

08/06/2010 17:20:57:549 4 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
 ADJSERVERS=
08/06/2010 17:20:57:549 4 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:551 5 FAILED: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01:
 ADJSERVERS=AS_01
08/06/2010 17:20:57:551 5 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: asgroup

08/06/2010 17:20:57:553 7 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=
08/06/2010 17:20:57:553 7 ***ERROR*** [Error Code 10095] - Invalid command syntax.

08/06/2010 17:20:57:555 8 FAILED: INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01:
DOMAIN=ITUI: POINTCODE=1-1-1: SVRGROUPS=SG_MP
08/06/2010 17:20:57:555 8 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: lsp

08/06/2010 17:20:57:557 10 FAILED: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=
08/06/2010 17:20:57:557 10 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:576 11 SUCCESS: INSERT: LSU: NENAME=Sig_OAM: POINTCODE=1-1-1:
 DOMAIN=ITUI: SSN=5: APPLICATION=TCAP
08/06/2010 17:20:57:579 13 FAILED: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=
08/06/2010 17:20:57:579 13 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:593 14 SUCCESS: INSERT: RSP: name=STP_01: pointcode=6-6-6:
domain=itui: asgroup=AdjServGrp1
08/06/2010 17:20:57:596 16 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-006-6:DOMAIN=ITUI: SSN=
08/06/2010 17:20:57:596 16 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:600 17 FAILED: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN= : SSN=5
08/06/2010 17:20:57:600 17 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:615 18 SUCCESS: INSERT: RMU: NAME=RMU_01:
POINTCODE=6-6-6:DOMAIN=ITUI: SSN=5
08/06/2010 17:20:57:617 20 FAILED: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
 LSP=ITUI_1_001_1: POINTCODE
08/06/2010 17:20:57:617 20 ***ERROR*** [Error Code 10095] - Invalid command
syntax.
```

```
08/06/2010 17:20:57:637 21 SUCCESS: INSERT: LINKSET: NENAME=Sig_OAM: NAME=LS_01:
 LSP=ITUI_1_001_1: POINTCODE=6-006-6: DOMAIN=ITUI: ASSIGNRC=no
08/06/2010 17:20:57:639 23 FAILED: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=
08/06/2010 17:20:57:639 23 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:659 24 SUCCESS: INSERT: ASSOCIATION: NENAME=Sig_OAM:
NAME=AssocTest1: HOSTNAME=XGMP: ADJSERVERS=AdjServ1: IPADDRESS=192.168.67.151
08/06/2010 17:20:57:662 26 FAILED: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=
08/06/2010 17:20:57:662 26 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:683 27 SUCCESS: INSERT: LINK: NENAME=Sig_OAM: NAME=Link1:
LINKSET=LS_01: ASSOCIATION=AssocTest1
08/06/2010 17:20:57:686 29 FAILED: INSERT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-006-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:57:686 29 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:705 30 SUCCESS: INSERT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-6-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=5
08/06/2010 17:20:57:707 32 FAILED: EDIT: ROUTE: NENAME=Sig_OAM: POINTCODE=6-006-6:
 DOMAIN=ITUI: LINKSET=LS_01: RELCOST=
08/06/2010 17:20:57:707 32 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:720 33 SUCCESS: EDIT: ROUTE: NENAME=Sig_OAM:
POINTCODE=6-006-6: DOMAIN=ITUI: LINKSET=LS_01: RELCOST=10
08/06/2010 17:20:57:722 35 FAILED: DELETE: ROUTE: POINTCODE=
08/06/2010 17:20:57:722 35 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:735 36 SUCCESS: DELETE: ROUTE: POINTCODE=6-006-6: DOMAIN=ITUI:
 LINKSET=LS_01
08/06/2010 17:20:57:737 38 FAILED: DELETE: LINK: NAME=
08/06/2010 17:20:57:737 38 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:750 39 SUCCESS: DELETE: LINK: NAME=Link1: FORCE=1
08/06/2010 17:20:57:752 41 FAILED: DELETE: ASSOCIATION: NAME=
08/06/2010 17:20:57:752 41 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:765 42 SUCCESS: DELETE: ASSOCIATION: NAME=AssocTest1: FORCE=1
08/06/2010 17:20:57:767 44 FAILED: DELETE: LINKSET: NAME=
08/06/2010 17:20:57:767 44 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:780 45 SUCCESS: DELETE: LINKSET: NAME=LS_01
08/06/2010 17:20:57:783 47 FAILED: DELETE: RMU: POINTCODE=6-006-6: DOMAIN=ITUI:
08/06/2010 17:20:57:783 47 ***ERROR*** [Error Code 001] - Missing Field Value:
ssn

08/06/2010 17:20:57:797 48 SUCCESS: DELETE: RMU: POINTCODE=6-6-6: DOMAIN=ITUI:
SSN=5
08/06/2010 17:20:57:799 50 FAILED: DELETE: RSP: pointcode=6-6-6
08/06/2010 17:20:57:799 50 ***ERROR*** [Error Code 001] - Missing Field Value:
domain

08/06/2010 17:20:57:813 51 SUCCESS: DELETE: RSP: pointcode=6-006-6: domain=itui
08/06/2010 17:20:57:815 53 FAILED: Delete: Lsu: Pointcode=1-001-1: Domain=ITUI:
```

```
 Ssn=
08/06/2010 17:20:57:815 53 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:828 54 SUCCESS: Delete: Lsu: Pointcode=1-1-1: Domain=ITUI:
Ssn=5: Force=1
08/06/2010 17:20:57:831 56 FAILED: DELETE: LSP: NAME=
08/06/2010 17:20:57:831 56 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:833 57 FAILED: DELETE: LSP: NAME=LSP_01
08/06/2010 17:20:57:833 57 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: lsp

08/06/2010 17:20:57:835 59 FAILED: DELETE: ASGROUP: NAME=
08/06/2010 17:20:57:835 59 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:837 60 FAILED: DELETE: ASGROUP: NAME=ASG_01
08/06/2010 17:20:57:837 60 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: asgroup

08/06/2010 17:20:57:839 62 FAILED: DELETE: ADJSERVER: NAME=
08/06/2010 17:20:57:839 62 ***ERROR*** [Error Code 10095] - Invalid command
syntax.

08/06/2010 17:20:57:841 63 FAILED: DELETE: ADJSERVER: NAME=AS_01
08/06/2010 17:20:57:841 63 ***ERROR*** [Error Code 10096] - Managed object not
yet supported: adjserver


------------------------------------------------
Command Execution Summary

Input File: cli_commands.txt
Number of Commands Executed:    43
Number of Commands Succeeded:   15
Number of Commands Failed:      28

--------------------------------------------------------------------------------
End of Command Execution Results
================================================================================
```

Figure 14: Example of Command Execution Results file

Command Execution Results elements

Results from command script execution are written to a TXT file. *Table 32: Command Execution Results* describes the elements of the Command Execution Results file.

Table 32: Command Execution Results

Element	Description
Command Execution Results	Displays the following information: • Time the report was generated • Server name

Element	Description
	• Report version number • User name
Command Execution Details	Output in the details section of the results file displays: • UTC timestamp in millisecond format: MM/DD/YYYY hh:mm:ss:uuu • Corresponding line number from the input file • Command statements from the input file • Successfully executed commands are preceded by: SUCCESS • Failed commands are preceded by: FAILED • Failed commands are followed by a line that begins with: ***ERROR*** [Error Code <number>] - <error code text> • Comments from the input file, if applicable • Comments are preceded by: Comment
Command Execution Summary	Output in the summary section of the file displays: • Name of the input file • Number of commands executed • Number of commands succeeded • Number of commands failed • If a fatal error occurs, the script is terminated, and the summary will contain this message: ***SCRIPT ABORTED DUE TO ERROR***

Command line interface import file

The CLI (Command Line Interface) import file enables you to create command scripts to insert, delete, and edit SS7 data. Using an import file facilitates the provisioning of large amounts of data. It also provides a convenient method for configuring data that is common to multiple sites.

CLI command structure

CLI commands are formatted as follows:

```
<operation>: <managed object>: <attribute>=<value>
```

Commands can contain multiple attribute value pairs. The format for commands that contain multiple attribute value pairs is:

```
<operation>: <managed object>: <attribute>=<value>: <attribute>=<value>
```

Table 33: CLI Command Values

Element	Valid Values	Data Input Notes
Operation	• insert • edit • delete	Operation names are not case-sensitive.
Managed object	• rsp • rmu • association • linkset • link • route • lsu	Managed object names are not case-sensitive.
Attributes	Attributes are specific to the commands. Some attributes are required; others are optional. For more information, see: • *Remote Signaling Points* • *Remote MTP3 Users* • *Link Sets* • *Links* • *Routes* • *Local SCCP Users*	Attribute names are not case-sensitive.
Value	For more information about attribute values, see: • *Remote Signaling Point elements* • *Remote MTP3 Users elements* • *Link Sets elements* • *Links elements* • *Routes elements* • *Local SCCP Users elements*	Attribute values are case-sensitive.

CLI File format

The following rules apply to the format of command script files:

- One command is allowed per line.
- Command lines that begin with the pound sign (#) are treated as comments. Comments are included in the results file, and they are counted, but are not validated or executed.
- Blank lines are skipped.

Sample command scripts

```
insert: rmu: pointcode=003-003-003: domain=ansi: ssn=5
insert: rmu: pointcode=004-004-004: domain=ansi: ssn=6
# This is a sample script that demonstrates how to use insert
```

Figure 15: Insert commands

```
delete: rsp: pointcode=100-1-1: domain=ansi
delete: rsp: pointcode=100-1-2: domain=ansi
# This is a sample script that demonstrates how to use delete
```

Figure 16: Delete commands

```
edit: Route: Pointcode=001-001-001: Domain=Ansi: Linkset=LS1: Relcost=10
edit: Route: Pointcode=001-001-002: Domain=Ansi: Linkset=LS1: Relcost=5
edit: Route: Pointcode=001-001-003: Domain=Ansi: Linkset=LS1: Relcost=3
# This is a sample script that demonstrates how to use edit
```

Figure 17: Edit commands

Managed objects

Command Import supports the following managed objects:

- `asg`
- `lsp`
- `rsp`
- `rmu`
- `linkset`
- `link`
- `route`
- `lsu`

Adjacent Server Groups

Managed object

`asg`

GUI Page updated

SS7/Sigtran > Configuration > Adjacent Server Groups page

Allowed operations

Table 34: CLI ASG Allowed Operations shows the operations allowed on the **SS7/Sigtran > Configuration > Adjacent Server Groups** page. The operation is not case-sensitive, for example, `INSERT`, `insert` and `Insert` are valid.

Table 34: CLI ASG Allowed Operations

Operation	Description
Insert	Adds an ASG to the configuration.
Delete	Deletes an ASG from the configuration.
Edit	Allows modification of an existing ASG.

Required attributes

Table 35: CLI ASG Required Attributes lists the required attributes for the `asg` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Adjacent Server Groups** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Adjacent Server Groups elements*).

Table 35: CLI ASG Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
name	Adjacent Server Group Identifier	• Insert	Unique identifier used to label an Adjacent Server Group
adjservers	Adjacent Server Group Member(s)	• Insert	The list of Adjacent Servers that make up the Adjacent Server Group. This field contains a comma-separated list of Adjacent Servers.

Optional attribute

Table 36: CLI ASG Optional Attribute lists an optional attribute for the `asg` managed object. The table maps the command attribute to its corresponding field name on the **SS7/Sigtran > Configuration > Adjacent Server Groups** page in the GUI.

The attribute name is not case sensitive; however, the attribute value is.

Note: All attribute values must be valid values that are allowed by the GUI (see *Adjacent Server Groups elements*).

Table 36: CLI ASG Optional Attribute

Attribute Name	GUI Field Name	For Operation
nename	Signaling Network Element Name	• Insert

Samples

To insert Adjacent Server Group ASG_01 on Signaling NE Sig_OAM with Adjacent Servers AS_0, use any of the following commands.

```
insert: asgroup: nename=Sig_OAM: name=ASG_01: adjservers=AS_0, as1
Insert:  Insert: AsGroup: NeName=Sig_OAM: Name=ASG_01: AdjServers=AS_0, as1
INSERT: INSERT: ASGROUP: NENAME=Sig_OAM: NAME=ASG_01: ADJSERVERS=AS_0, as1
```

To delete Adjacent Server Group ASG_01, use any of the following commands:

```
delete: asgroup: name=ASG_01
Delete: Asgroup: Name=ASG_01
DELETE: ASGROUP: NAME=ASG_01
```

Note: All Values for field name are case-sensitive. For example, the following commands will add two different Adjacent Server Groups:

```
 insert: asgroup: nename=Sig_OAM: name=ASG_01:adjservers=AS_0, as1
insert: asgroup: nename=Sig_OAM: name=Asg_01: adjservers=AS_1
```

Local Signaling Points

Managed object

`lsp`

GUI Page updated

SS7/Sigtran > Configuration > Local Signaling Points page

Allowed operations

Table 37: CLI LSP Allowed Operations shows the operations allowed on the **SS7/Sigtran > Configuration > Local Signaling Points** page. The operation is not case-sensitive, for example, `INSERT`, `insert` and `Insert` are valid.

Table 37: CLI LSP Allowed Operations

Operation	Description
Insert	Adds an LSP to the configuration.

Operation	Description
Delete	Deletes an LSP from the configuration.
Edit	Allows modification of an existing LSP.

Required attributes

Table 38: CLI LSP Required Attributes lists the required attributes for the `lsp` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Local Signaling Points** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Local Signaling Points elements*).

Table 38: CLI LSP Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
pointcode	MTP Code	• Insert	The MTP point code that identifies this Local Signaling Point. Only one LSP can have this MTP True Point Code.
domain	SS7 Domain	• Insert	The SS7 domain in which the Node resides.
svrgroups	Server Group(s)	• Insert	Server Group(s) that serve this Local Signaling Point. For multiple server groups, this field contains a comma-separated list of server groups. Each server group can host an lsp of each of the three domains - ANSI, ITUI and ITUN.

Optional attribute

Table 39: CLI LSP Optional Attribute lists an optional attribute for the `lsp` managed object. The table maps the command attribute to its corresponding field name on the **SS7/Sigtran > Configuration > Local Signaling Points** page in the GUI.

The attribute name is not case sensitive; however, the attribute value is.

Note: All attribute values must be valid values that are allowed by the GUI (see *Local Signaling Points elements*).

Table 39: CLI LSP Optional Attribute

Attribute Name	GUI Field Name	For Operation
netname	Signaling Network Element Name	• Insert
cpc	MTP Capability Point Code(s)	• Insert

Attribute Name	GUI Field Name	For Operation
cpc2	MTP Capability Point Code(s)	• Insert
name	Local Signaling Point Name	• Insert

Samples

To insert Local Signaling Point with pointcode as 001-001-001 in ANSI domain and auto generated LSP Name for Signaling NE Sig_OAM, use any of the following commands. The LSP Name added would be: ANSI_001_001_001

```
insert: lsp: nename=Sig_OAM: domain=ANSI: pointcode=001-001-001: svrgroups=SG_MP

Insert: Lsp: NeName=Sig_OAM: Domain=ANSI: Pointcode=001-001-001: Svrgroups=SG_MP

INSERT: LSP: NENAME=Sig_OAM: DOMAIN=ANSI: POINTCODE=001-001-001: SVRGROUPS=SG_MP
```

To insert Local Signaling Point LSP_01 with pointcode as 001-001-001 in ANSI domain for Signaling NE Sig_OAM, use any of the following commands:

```
insert: lsp: nename=Sig_OAM: name=LSP_01: domain=ANSI: pointcode=001-001-001:
svrgroups=SG_MP

Insert: Lsp: NeName=Sig_OAM: Name=LSP_01: Domain=ANSI: Pointcode=001-001-001:
Svrgroups=SG_MP

INSERT: LSP: NENAME=Sig_OAM: NAME=LSP_01: DOMAIN=ANSI: POINTCODE=001-001-001:
SVRGROUPS=SG_MP
```

To delete Local Signaling Point LSP_01, use any of the following commands:

```
delete: lsp: name=LSP_01

Delete: Lsp: Name=LSP_01

DELETE: LSP: NAME=LSP_01
```

Note: All Values for field name are case-sensitive. For example, the following commands will add two different Local Signaling Points:

```
 insert: lsp: nename=Sig_OAM: name=LSP_01: domain=ANSI: pointcode=001-001-001:
servergroups=SG_MP

 insert: lsp: nename=Sig_OAM: name=lsp_01: domain=ANSI: pointcode=002-002-002:
servergroups=SG_MP1
```

Remote Signaling Points

Managed object

`rsp`

GUI Page updated

SS7/Sigtran > Configuration > Remote Signaling Points page

Allowed operations

Table 40: CLI RSP Allowed Configuration Operations shows the operations allowed on the **SS7/Sigtran > Configuration > Remote Signaling Points** page. The operation is not case-sensitive, for example, `INSERT`, `insert` and `Insert` are valid.

Table 40: CLI RSP Allowed Configuration Operations

Operation	Description
Insert	Adds an RSP to the configuration.
Delete	Deletes an RSP from the configuration.
Edit	Allows modification of an existing RSP.

Table 41: CLI RSP Allowed Maintenance Operation shows the operation allowed on the **SS7/Sigtran > Maintenance > Remote Signaling Points** page. The operation is not case-sensitive; for example, `RESET`, `Reset` and `reset` are valid.

Table 41: CLI RSP Allowed Maintenance Operation

Operation	Description
Reset	Resets the MP's view of the network status of both routes to Available.

Required attributes

Table 42: CLI RSP Required Attributes lists the required attributes for the `rsp` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Remote Signaling Points** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote Signaling Point elements*).

Table 42: CLI RSP Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
pointcode	MTP Point Code	• Insert • Delete	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 Domain	• Insert	Not applicable

Attribute Name	GUI Field Name	For Operation	Notes
		• Delete	

Optional attribute

Table 43: CLI RSP Optional Attribute lists an optional attribute for the `rsp` managed object. The table maps the command attribute to its corresponding field name on the **SS7/Sigtran > Configuration > Remote Signaling Points** page in the GUI.

The attribute name is not case sensitive; however, the attribute value is.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote Signaling Point elements*).

Table 43: CLI RSP Optional Attribute

Attribute Name	GUI Field Name	For Operation
name	Remote Signaling Point Name	• Insert
asgroup	Adjacent Server Group	• Insert

Samples

To insert RSP STP_01 with pointcode 100-1-1 for the ANSI Domain with the Adjacent Server Group as asg1, use any of the following commands:

```
insert: rsp: pointcode=100-1-1: domain=ansi: asgroup=asg1
Insert: RSP: pointcode=100-1-1: domain=ansi: asgroup=asg1
INSERT: RSP: name=STP_01: pointcode=100-1-1: domain=ansi: asgroup=asg1
```

To delete RSP STP_01, use any of the following commands:

```
delete: rsp: pointcode=100-1-1: domain=ansi
Delete: RSP: pointcode=100-1-1: domain=ansi
DELETE: RSP: pointcode=100-1-1: domain=ansi
```

Remote MTP3 Users

Managed object

`rmu`

GUI Page updated

SS7/Sigtran > Configuration > Remote MTP3 Users page

Allowed operations

Table 44: CLI RMU Allowed Configuration operations shows the operations allowed on the **SS7/Sigtran > Configuration > Remote MTP3 Users** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 44: CLI RMU Allowed Configuration operations

Operation	Description
Insert	Adds an RMU to the configuration.
Delete	Deletes an RMU from the configuration.

Table 45: CLI RMU Allowed Maintenance Operation shows the operation allowed on the **SS7/Sigtran > Maintenance > Remote MTP3 Users** page. The operation is not case-sensitive; for example, `RESET`, `Reset`, and `reset` are valid.

Table 45: CLI RMU Allowed Maintenance Operation

Operation	Description
Reset	Resets the MP's view of the remote subsystem.

Required attributes

Table 46: CLI RMU Required attributes lists the required attributes for the `rmu` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Remote MTP3 Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote MTP3 Users elements*).

Table 46: CLI RMU Required attributes

Attribute Name	GUI Field Name	For Operation	Notes
domain	SS7 Domain	• Insert • Delete	Not applicable
pointcode	Remote Point Code	• Insert • Delete	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
ssn	Remote SSN	• Insert • Delete	CLI ignores leading zeros, for example: 001 = 01 = 1

Optional attributes

Table 47: CLI RMU Optional Attribute lists the optional attributes for the `rmu` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Remote MTP3 Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Remote MTP3 Users elements*).

Table 47: CLI RMU Optional Attribute

Attribute Name	GUI Field Name	Operation
name	Remote MTP3 User Name	• Insert

Samples

To insert an RMU named RMU_01 with a point code of 3-3-3, the domain as ANSI, and an SSN of 5, use any of use any of these commands:

```
insert: rmu: pointcode=003-003-003: domain=ansi: ssn=5

Insert: RMU: Pointcode=3-3-3: Domain=ansi: Ssn=5

INSERT: RMU: NAME=RMU_01: POINTCODE=003-003-003: DOMAIN=ANSI: SSN=5
```

To delete the RMU RMU_01, use any of the following commands:

```
delete: rmu: pointcode=003-003-003: domain=ansi: ssn=5

Delete: RMU: Pointcode=3-3-3: Domain=ansi: Ssn=5

DELETE: RMU: POINTCODE=003-003-003: DOMAIN=ANSI: SSN=5
```

Link Sets

Managed object

`linkset`

GUI page updated

SS7/Sigtran > Configuration > Link Sets page

Allowed operations

Table 48: CLI Link Sets Allowed operations shows the operations allowed on the **SS7/Sigtran > Configuration > Link Sets** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 48: CLI Link Sets Allowed operations

Operation	Description
Insert	Adds a Link Set to the configuration.
Delete	Deletes a Link Set from the configuration.

Required attributes

Table 49: CLI Link Sets Required Attributes lists the required attributes for the `linkset` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Link Sets** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Link Sets elements*).

Table 49: CLI Link Sets Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
name	Link Set Name	• Insert • Delete	Not applicable
lsp	Local Signaling Point	• Insert	Not applicable
pointcode	Adjacent Remote Point Code	• Insert	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 domain	• Insert	Not application
assignrc	Assign Routing Context	• Insert	If **assignrc = yes**, and the optional **routingcontext** attribute is not specified, then the default value of **routingcontext** prevails (the first unused integer value greater than zero).

Optional attributes

Table 50: CLI Link Sets Optional Attributes lists the optional attributes for the `linkset` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Link Sets** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Link Sets elements*).

Table 50: CLI Link Sets Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	On SS7 applications where configuration is performed from the SOAM, this parameter is optional.

routingcontext	Routing Context	• Insert	The following rules are applicable for routing context. The attribute value is not case-sensitive:
			• If you do not want a routing context to be assigned, specify **No** for the **assignrc** field. If the **routingcontext** attribute is specified and **assignrc=no**, then the routing context is ignored:
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=003-003-003: domain=ansi: assignrc=NO`
			or
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=3-3-3: domain=ansi: assignrc=no: routingcontext=55`
			• To specify the default routing context as the first unused integer value greater than zero, specify **assignrc=yes**, but do not specify **routingcontext**:
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=3-3-3: domain=ansi: assignrc=YES`
			• To define the routing context, specify **assignrc=yes** and specify a value for **routingcontext**:
			`insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=003-003-003: domain=ansi:assignrc=YES: routingcontext=1000`

Samples

To insert Linkset LS_01 with the LSP as LSP_01 and the adjacent point code as 003-003-003 with no routing context, use any of the following commands:

```
insert: linkset: nename=sig_oam: name=LS_01: lsp=LSP_01: pointcode=3-3-3:
domain=ansi: assignrc=no
```

```
Insert: Linkset: NeName=sig_oam: Name=LS_01: Lsp=LSP_01: Pointcode=003-003-003:
 Domain=ansi: Assignrc=no

INSERT: LINKSET: NENAME=sig_oam: NAME=LS_01: LSP=LSP_01: POINTCODE=003-003-003:
 DOMAIN=ANSI: ASSIGNRC=no
```

To delete Link Set LS_01, use any of the following commands:

```
delete: linkset: name=LS_01

Delete: Linkset: Name=LS_01

DELETE: LINKSET: NAME=LS_01
```

All attribute values are case sensitive. The following commands add two different Link Sets:

```
insert: linkset: name=LS_01: lsp=LSP_01: pointcode=003-003-003: domain=ansi:
assignrc=no

insert: linkset: name=ls_01: lsp=LSP_01: pointcode=003-003-002: domain=ansi:
assignrc=no
```

Links

Managed object

`link`

GUI page updated

SS7/Sigtran > Configuration > Links page

Allowed operations

Table 51: CLI Links Allowed Configuration operations shows the operations allowed on the **Links** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 51: CLI Links Allowed Configuration operations

Operation	Description
Insert	Adds a Link to the configuration.
Delete	Deletes a Link from the configuration.

Table 52: CLI Links Allowed Maintenance Operations shows the operations allowed on the **SS7/Sigtran > Maintenance > Links** page. The operation is not case-sensitive; for example, `ENABLE`, `Enable` and `enable` are valid.

Table 52: CLI Links Allowed Maintenance Operations

Operation	Description
Enable	Enables a Link io the system.
Disable	Disables a Link in the system.

Required attributes

Table 53: CLI Links Required Attributes lists the required attributes for the `link` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Links** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Links elements*).

Table 53: CLI Links Required Attributes

Attributes Name	GUI Field Name	For Operation
name	Link Name	• Insert • Delete
linkset	Link Set	• Insert
association	Association	• Insert

Optional attributes

Table 54: CLI Links Optional Attributes lists the optional attributes for the `link` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Links** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Links elements*).

Table 54: CLI Links Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	On SS7 applications where configuration is performed from the SOAM, this parameter is optional.
force	Not applicable	• Delete	The only valid value is **force=1**. The attribute is used to force the delete operation for an association, irrespective of its Admin State.

Samples

To insert a Link named Linkl with a Link Set of LS1 and an association of Assoc1 on Signaling Network Element NE_01, use any of the following commands: :

```
insert: link: nename=NE_01: name=Link1: linkset=LS1: association=Assoc1
Insert: Link: NeName=NE_01: Name=Link1: Linkset=LS1: Association=Assoc1
INSERT: LINK: NENAME=NE_01: NAME=Link1: LINKSET=LS1: ASSOCIATION=Assoc1
```

To delete the Link, Link1, use any of the following commands:

```
delete: link: name=Link1
Delete: Link: Name=Link1
DELETE: LINK: NAME=Link1
DELETE: LINK: NAME=Link1: FORCE=1
```

All attribute values are case sensitive. The following commands add two different Links:

```
insert: link: nename=NE_01: name=Link1: linkset=LS1: association=Assoc1
insert: link: nename=NE_01: name=LINK1: linkset=LS2: association=Assoc1
```

Routes

Managed object

`route`

GUI Page updated

SS7/Sigtran > Contiguration > Routes page

Allowed operations

Table 55: CLI Routes Allowed Operations shows the operations allowed on the **SS7/Sigtran > Configuration > Routes** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 55: CLI Routes Allowed Operations

Operation	Description
Insert	Adds a Route to the configuration.
Delete	Deletes a Route from the configuration.
Edit	Allows modification of the Route Cost for an existing Route.

Required attributes

Table 56: CLI Routes Required Attributes lists the required attributes for the `route` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Routes** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Routes elements*).

Table 56: CLI Routes Required Attributes

Attribute Name	GUI Field Name	For Operation	Notes
pointcode	Remote Point Code	• Insert • Delete • Edit	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 Domain	• Insert • Delete • Edit	Not applicable
linkset	Link Set	• Insert • Delete • Edit	Not applicable
relcost	Relative Cost	• Insert • Edit	CLI ignores leading zeros, for example: 001 = 01 = 1

Optional attributes

Table 57: CLI Routes Optional Attributes lists the optional attributes for the `route` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Routes** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Routes elements*).

Table 57: CLI Routes Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	In the MD-IWF SS7 Application, where configuration is performed from the SOAM, this parameter is optional.
name	Route Name	• Insert	Not applicable.

Samples

To insert a Route with a point code of 1-1-1, the domain as ANSI, and a relative cost of 5, use any of the following commands:

```
insert: route: nename=sig_oam: pointcode=1-1-1: domain=ansi: linkset=LS1:
relcost=5

Insert: Route: NeName=sig_oam: Pointcode=001-001-001: Domain=ansi: Linkset=LS1:
 Relcost=5

INSERT: ROUTE: NENAME=sig_oam: POINTCODE=001-001-001: DOMAIN=ANSI: LINKSET=LS1:
 RELCOST=5
```

To delete Route_01, use any of the following commands:

```
delete: route: pointcode=1-1-1: domain=ansi: linkset=LS1

Delete: Route: Pointcode=001-001-001: Domain=Ansi: Linkset=LS1

DELETE: ROUTE: POINTCODE=001-001-001: DOMAIN=ANSI: LINKSET=LS1
```

To update the Relative Cost for Route_01 with a value of 10, use any of the following commands:

```
edit: route: pointcode=1-1-1: domain=ansi: linkset=LS1: relcost=10

Edit: Route: Pointcode=001-001-001: Domain=Ansi: Linkset=LS1: Relcost=10

EDIT: ROUTE: POINTCODE=001-001-001: DOMAIN=ANSI: LINKSET=LS1: RELCOST=10
```

Local SCCP Users

Managed object

`lsu`

GUI page updated

SS7/Sigtran > Configuration > Local SCCP Users page

Allowed operations

Table 58: CLI LSU Allowed Configuration Operations shows the operations allowed on the **SS7/Sigtran > Configuration > Local SCCP Users** page. The operation is not case-sensitive; for example, `ENABLE`, `Enable` and `enable` are valid.

Table 58: CLI LSU Allowed Configuration Operations

Operation	Description
Insert	Adds an LSU to the configuration.
Delete	Deletes an LSU from the configuration.

Table 52: CLI Links Allowed Maintenance Operations shows the operations allowed on the **SS7/Sigtran > Maintenace > Local SCCP Users** page. The operation is not case-sensitive; for example, `INSERT`, `insert` and `Insert` are valid.

Table 59: CLI LSU Allowed Maintenance Operations

Operation	Description
Enable	Enables an LSU to the system.
Disable	Disables an LSU to the system.

Required attributes

Table 60: CLI LSU Required Attributes lists the required attributes for the `lsu` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Local SCCP Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Local SCCP Users elements*).

Table 60: CLI LSU Required Attributes

Attributes Name	GUI Field Name	For Operation	Note
pointcode	Local Signaling Point	• Insert • Delete	Point codes are normalized based on the specified SS7 domain. Some examples follow: • ANSI point code 1-1-1 becomes 001-001-001 • ITU-I point code 1-1-1 becomes 1-001-1 • ITU-N point code 00001 becomes 1 and ITU-N point code 000 becomes 0
domain	SS7 Domain	• Insert • Delete	Not applicable
ssn	SSN	• Insert • Delete	Not applicable

Attributes Name	GUI Field Name	For Operation	Note
application	Application Name	• Insert	Not applicable

Optional attributes

Table 61: CLI LSU Optional Attributes lists the optional attributes for the `lsu` managed object. The table maps the command attributes to their corresponding field names on the **SS7/Sigtran > Configuration > Local SCCP Users** page in the GUI.

The attribute names are not case sensitive; however, the attribute values are.

Note: All attribute values must be valid values that are allowed by the GUI (see *Local SCCP Users elements*).

Table 61: CLI LSU Optional Attributes

Attribute Name	GUI Field Name	For Operation	Notes
nename	Signaling Network Element Name	• Insert	In the MD-IWF SS7 Application, where configuration is performed from the SOAM, this parameter is optional.
force	Not applicable.	• Delete	The only valid value is **force=1**. The attribute is used to force the delete operation for an association, irrespective of its Admin State.

Samples

To insert an LSU with a point code of 1-1-1, the domain as ANSI, and an SSN of 5, use any of the following commands:

```
insert: lsu: nename=NO_01: pointcode=1-1-1: domain=ansi: ssn=5:
application=LocalSCCPUser

Insert: Lsu: NeName=NO_01: Pointcode=001-001-001: Domain=Ansi: Ssn=5:
Application=LocalSCCPUser

INSERT: LSU: NENAME=NO_01: POINTCODE=001-001-001: DOMAIN=ANSI: SSN=5:
APPLICATION=LocalSCCPUser
```

To delete an LSU with a point code of 1-1-1, the domain as ANSI, and an SSN of 5, use any of the following commands:

```
delete: lsu: pointcode=1-1-1: domain=ansi: ssn=5

Delete: Lsu: Pointcode=001-001-001: Domain=Ansi: Ssn=5: Force=1

DELETE: LSU: POINTCODE=001-001-001: DOMAIN=ANSI: SSN=5
```

Glossary

A

Adjacent Server	A server acting as a signaling peer for M3UA signaling. An Adjacent Server connects to one or more MP Servers using reliable IP transport sessions, such as SCTP associations. Only adjacent Remote Signaling Points and adjacent Remote MTP3 Users are hosted on Adjacent Servers.
Adjacent Server Group	A collection of Adjacent Servers that implements a distributed IP signaling function.The group represents a set of Adjacent Servers that share a point code on the signaling gateway.An Adjacent Server Group has a name and a list of Adjacent Servers.
ANSI	American National Standards Institute An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.

C

CLI	Command-line interface

D

DAUD	Destination Audit

D

DAVA	Destination Available
DUNA	Destination Unavailable
DUPU	Destination User Part Unavailable An M3UA management message.

G

GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

I

ITU-I	ITU-International
ITU-N	ITU-National

L

Link	Signaling Link Carries signaling within a Link Set using a specific Association. A Link can belong to only one Link Set and one Association. There is generally one Link per Association in a Link Set.
LNP	Local Number Portability The ability of subscribers to switch local or wireless carriers and still retain the same phone number.
LSP	Local Signaling Point

L

	A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique primary/true point code within a particular SS7 Domain to an MP server.
LSU	Local SCCP User Refers to an Application Configured with a Subsystem Number to handle "rt-on-ssn" traffic for local signaling point code hosted on MP server.

M

M3RL	M3UA Routing Layer A layer invented by Tekelec to enhance M3UA by adding a true routing layer.
M3UA	SS7 MTP3-User Adaptation Layer M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MTP3	Message Transfer Part, Level 3

N

NOAM	Network Operations, Administration, and Maintenance

P

PDU	Protocol Data Unit

R

Remote MTP3 User	See RMU.

R

Remote Signaling Point	See RSP.
RMU	Remote MTP3 User Represents a remote SCCP subsystem to which the Signaling Network Interface forwards signaling. When a message is forwarded from an MSC to an HLR, an RMU must be configured for the subsystem on the HLR.
Route	A signaling path from an LSP to an RSP using a specified Link Set
RSP	Remote Signaling Point Represents an SS7 network node (point code) that signaling must be sent to. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.
RST	Routeset Prohibited Test (Msg)

S

SCCP	Signaling Connection Control Part The signaling connection control part with additional functions for the Message Transfer Part (MTP) in SS7 signaling. Messages can be transmitted between arbitrary nodes in the signaling network using a connection-oriented or connectionless approach.
SCTP	Stream Control Transmission Protocol

S

	An IETF transport layer protocol, similar to TCP that sends a message in one operation. The transport layer for all standard IETF-SIGTRAN protocols. SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SLS	Signaling Link Selector
SOAM	System Operations, Administration, and Maintenance Site Operations, Administration, and Maintenance
STP	Spanning Tree Protocol

T

TFA	TransFer Allowed (Msg)
TFP	TransFer Prohibited (Msg) A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.
TSA	Target Set Address An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target

T

set address across a set of application servers.

U

UDT — Unitdata Transfer

UDTS — Unitdata Transfer Service

An error response to a UDT message.

X

XUDT — Extended Unit Data

XUDTS — Extended Unitdata Service message

An error response to an XUDT message.