Oracle® Communications Subscriber Data Management

Monitoring, Maintaining, Troubleshooting Reference Manual

Release 9.3

910-6865-001 Revision A

March 2014

ORACLE®

Oracle® Communications Monitoring, Maintaining, Troubleshooting Reference Manual, Release 9.3

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter provides general information about manual organization, the scope of this manual, its targeted audience, how to get technical assistance, and how to locate customer documentation on the Customer Support site.

About this document

This document describes the system error messages, entities for the database, OAM&P and the overall system; database operations such as backup and restore, subscriber licenses information, and log files generated by the system and theSNMP.

Scope and audience

This reference manual provides information regarding error messages, entities, database operations, and log files to the users of the Subscriber Data Management system.

Document Organization

This document is organized into the following chapters:

- *Introduction* contains general information about manual organization, the scope of this manual, its targeted audience, how to get technical assistance, and how to locate customer documentation on the Customer Support Site.
- *User Interfaces* describes the interfaces that can be used to configure the system or provision subscribers.
- *Error Notifications* lists error or provisioning notifications.
- *Database Operations* provides backup and restore information.
- *OAM&P* provides information about SNMP, License and OAMP Managers, logs and software version.
- *System* provides all system entities and related operations.

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*.)

Icon	Description
	**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 a detailed description of the available SDM documentation, refer to the *SDM Documentation Roadmap* included with your SDM documentation set.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

    001-888-367-8552

  - **Peru**

    Phone:

    0800-53-087

  - **Puerto Rico**

    Phone:

    1-888-367-8552

  - **Venezuela**

Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

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

1. Log into the *Tekelec Customer Support* site.

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

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

Chapter 2

User Interfaces

Topics:

This chapter describes the user interfaces that allow the operator to configure the system or provision subscribers. The description includes functionalities, command convention, navigation method, command execution, and the GUI symbols used in the WebCI.

Command Line Interface

The Command Line Interface (CLI) is the client OAM&P (Operation, Alarm, Maintenance and Provisioning) application that manages and provisions the Tekelec Subscriber Data Management. The CLI provides a command-line, text-based environment to access the OAM&P. The operator accesses OAM&P functionality by invoking commands in the CLI. Changes made to system configuration or subscriber provisioning data takes effect immediately. The system administrator creates and manages users, their username and password, and assigns users to groups with different access privileges for specific services.

The administrator can perform all tasks through the CLI:

- Create and manage users
- Manage the Dynamic System Configuration
- View, add, delete, and modify subscriber provisioning information
- View and modify configuration data
- View and modify operational aspects of the system
- View and modify system configuration properties
- View current and historical data
- Remote system administration
- System maintenance

Refer to *User Security Management through CLI* in this document for a detailed description of the User Security Management feature, also refer to the "Creating and Managing users for the User Interfaces" section in the *SDM System Configuration - User Guide* for step by step procedures to provision users through the CLI and WebCI.

CLI Command Convention

In this document, system information such as commands, system prompts, and responses, will be represented as follows:

- Command Strings that the user enters appear in bold face:

  `# cli`

  Note: CLI commands are case sensitive. Users must enter the command string exactly as shown, including spaces.

- System Prompts and Responses appear in courier font:

  `1: System []>`

System Identification

The CLI identifies the system ID of the system to which the opened CLI session is connected. The system ID is provided by Tekelec for a specific SDM system and is also used as the Customer Name.

The CLI displays the Customer Name (SystemID) as part of the license information. Display the Customer Name and other license information by executing the DisplayLicense() operation.

`:Oamp[]:OampManager[]:LicenseManager[LicenseId = 6]> DisplayLicense()`

Refer to the *Command Line Interface (CLI)* section of the *SDM System Configuration – User Guide* for instructions on how to start, navigate, or end a CLI session.

CLI Navigation

Navigation diagram

All navigation, provisioning, or configuration in the CLI subsystems is based on entities, attributes, and values.

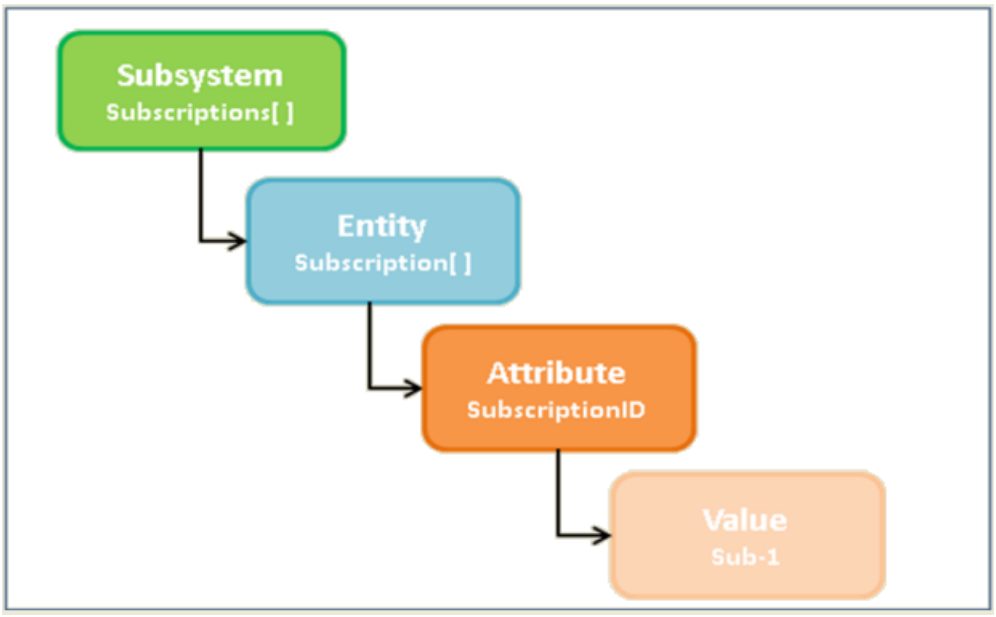


Figure 1: Subsystem Navigation Diagram

Each subsystem, for example, Hlr, Sip, Hss, Database, OAM&P, SS7, System, and Subscriptions, is made up of entities. An entity is a table in a database that contains all the information about the entity. Each entity is defined by one or more attributes, which can be mandatory or optional. An attribute is defined by its value.

For example, the Hlr subsystem contains entities such as Plmn, Algorithm, and MSISDN. The Plmn entity is defined by the PlmnId attribute, which is a mandatory attribute. The PlmnId has a value of `Montreal`.

Navigating through the CLI entails defining instances of entities, that is, by choosing a set of attributes of an entity and assigning a value to each selected attribute, the user creates an instance of the entity. By adding, modifying or deleting attribute values, the user is provisioning a subscriber entity or configuring a system entity.

To connect to the system, refer to section *Accessing the System* in the *SDM System Configuration - User Guide*, and log in with a valid user ID and password.

Command line usage

- System prompt:

```
#
```

- Starting CLI at system prompt:

  ```
  # cli
  ```

- CLI system startup prompt:

  ```
  1 :>
  ```

  The first part of the prompt is the command number, which starts at 1 and auto-increments for each new command entered. This number is used to keep a history log of the commands issued.

- CLI prompt with navigation context:

  ```
  2: System[] >
  ```

  The command number, has incremented.

  The second part of the prompt indicates the current navigation context (`System[]`). This shows where the user is within the navigational levels.

  The third part is the prompt separator (>). The user can enter commands after the prompt separator.

- The subsystems can be accessed from anywhere in the CLI when the command is preceded by a colon (:), which defines an absolute navigation path:

  ```
  2 :Hlr[]:Plmn[PlmnId = Montreal]> :System[]
  3 :System[]>
  ```

CLI commands

This section lists basic Unix shell commands, CLI commands and characters, as well as subsystem access commands.

Basic Unix shell commands

These basic UNIX shell commands facilitate usage of the CLI.

Command	Definition
<CTRL> a	jump to home
quit	exit the CLI
<CTRL> e	jump to end
<CTRL> l	clear screen
<CTRL> u	clear typed line
↑	Use up arrow to scroll up the command history
↓	Use down arrow to scroll down the command history
<CTRL> z	Cancels any change made by the ongoing command by aborting the session.*

Warning:

When using the CLI, the <CTRL> z command does not send the process execution to background, as it typically would. Since there is no need to allow to run the CLI in background, the Tekelec implementation intentionally interprets the <CTRL> z command as an "abort" message and suspends the ongoing command. Basically, the use of the <CTRL> z command cancels any change made by the ongoing command. In some situations, executing this command may produce a core dump of the CLI processes.

However, using the CTRL-Z command will not cause any service outage, nor will it cause data corruption. The same warning also applies for the use of the <CTRL> z command when using the Command File Loader (CmdFileLoader).

CLI commands

Command	Definition
add	Adds a new instance to the system
attributes	Show attributes of an entity
delete	Deletes instances from the system
display	Display the instances
entities	Show sub-entities
help	Display help options
history	Lists history of commands
instances	Display all instances of an entity
key	Show navigation key attributes
modify	Make changes to instances
operations	Show operations
parameters	Show parameters of an operation
quit	Exit the CLI
top	Go to top level
tree	View the command tree
up	Go up one level
version	Displays current version of the software load

CLI characters

Symbol	Definition
*	Indicates a mandatory item
;	Separate multiple attributes or attribute values with a semicolon
,	Separate multiple items in a value list with a comma

Symbol	Definition
.	Specifies the current instance
:	Separates different levels between entities

Subsystem access commands

Command	Definition
Database[]	access Database subsystem
Hlr[]	access HLR subsystem
Oamp[]	access OAM&P subsystem
SS7[]	access SS7 subsystem
System[]	access System subsystem
Sip[]	access SIP functionalities of the Tekelec ngHLR
Hss[]	HSS subsystem
Subscriptions[]	Access Subscriptions subsystem

Operations

The CLI supports the following operations: Display, Add, Modify, and Delete. These operations can be used on entities and instances to provision or modify system parameters.

The supported operands for each operation are listed below.

Table 2: CLI operations

Operation	Supported Operand
Display	=, <, >, >=, <=
Add	=
Modify	=
Delete	=

Command History

A history of all the commands entered can be viewed.

To view all the commands entered, type **history**.

To view the most recent commands, type **history <#>**, where # is used to specify the number of the most recent commands to be displayed.

To view a specific command entered, type **!<command #>**.

Auto-Complete Functionality

The CLI is powered by a contextual auto-complete functionality enabled by the <Tab> key. Using this functionality is by no means necessary for the use of the CLI, but offers great improvements in operational efficiency.

This function aids in navigation as well as provisioning by completing the following command strings:

- Recognized Subsystem, Entity, and Attribute names
- Recognized Values for Attributes when there is a finite number of acceptable values
- Navigation options
- Displaying which Entities are mandatory (marked with an "*")
- Completing grammar

Press the **Tab** key at any time in the CLI for text or grammar completion, information about available Entities and Values for Attributes, and help. If the <**Tab**> key does not complete any further, there is no system-defined acceptable values or the user may insert a sign or closing bracket "]" to continue editing the command.

Attributes

Mandatory Attributes

When using the CLI, some attributes are preceded by an asterisk (*). The asterisk has different meanings depending on the context where it is being used.

When navigating to entities, an attribute with an asterisk indicates a key instance and it is mandatory to continue navigating. When performing an Add operation, the attribute is a mandatory attribute and must be included in the command. In the add operation, a unique instance is being created. For a Modify, Delete, or Display operation, the asterisk indicates the attribute is a key instance, but it is not a mandatory attribute. If no mandatory attributes are specified, then the operation will apply to 0 or more instances.

Inherited Attributes

Attributes that are passed down from a higher level (parent) entity to a lower (child entity) are called inherited attributes . The inherited attributes are passed on when navigating down to lower level entities. In order to access the lower entities, the inherited attributes must be specified in the CLI command string.

In this document, all the attributes are considered to be Read/Write unless noted otherwise.

Command help options

This option displays options available for built-in commands.

Help options show the operator the operations available to perform on the system.

From the directory where the command is stored, type the command name followed by **`-h`** or **`-help`** as shown with the commands below.

Help options are available for commands such as

- **`blueupdate.sh -help`**
- **`cfl -help`** (Command File Loader)
- **`ctl -h`** (Command Template Loader)
- **`CmdTemplateViewer -h`** (Command Template Viewer)

Note: The user must have access privileges to these interfaces and must have logged in successfully before these commands become available.

Web Craft Interface (WebCI)

This chapter provides an overview of the Tekelec GUI: Web Craft Interface (WebCI), with the navigation system, the different operations available and the auto-refresh mechanism.

With the User Security Management feature, not all WebCI operations and functionalities are available to all users. The administrator of the system is in charge to create and manage users, their username and password and assign them to groups with different access privileges for specific services.

Please refer to the *User Security Management* in this document for a more detailed description of the User Security Management feature, also refer to the "Creating and Managing users for the User Interfaces" section in the *SDM System Configuration - User Guide* for step by step procedures to provision users through the CLI and WebCI.

Hereunder are some general descriptions of the WebCI's different characteristics:

System Identification

The WebCI provides to the user an easy way to identify the System ID (System Number given by Tekelec for a specific SDM system, also used as the Customer Name) of the system to which the opened WebCI session is connected to.

The WebCI displays the SystemID in the front page (at user login) as well as in its menu, as part of the System folder name.

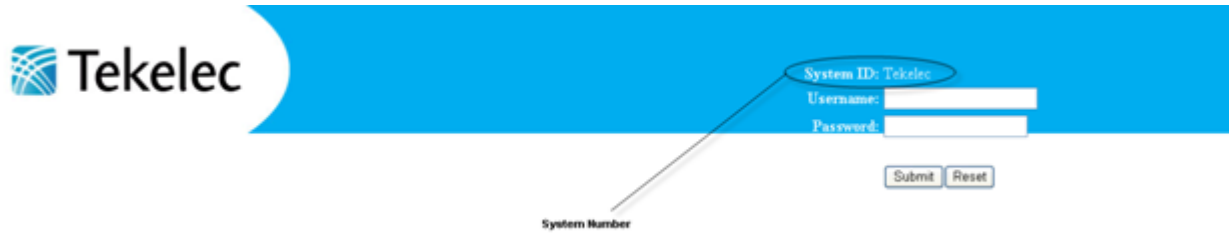


Figure 2: SystemID visible in WebCI front page

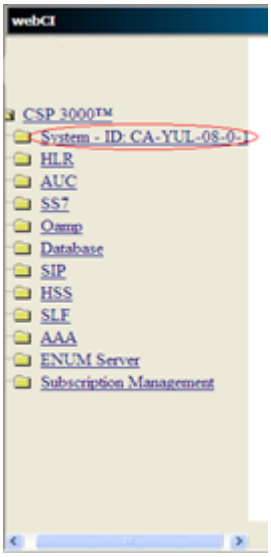


Figure 3: SystemID visible in WebCI front page

Hyperlinks

Hyperlinks take the user to the system configuration or user provisioning tables. Hyperlinks may have one or more sublinks.

Pop-up windows

Pop-up windows appear:

- To display further information, after clicking on a button or on a text highlighted in blue. A provisioning window or simply a confirmation request will appear depending on the operation.
- To request a confirmation of the action to take and always give the chance for the operator to Cancel or proceed with the action.

If the web browser is configured to block pop-up windows, some WebCI screens will not be displayed. To display all WebCI screens, add the address of the Single Board Computer (SBC) to the list of allowed sites. Alternatively, temporarily allow the pop-ups windows to be displayed in order to view the WebCI screens.

Table entry count

- HSS Shared Initial Filtering Criteria
- HSS SLF Public 2 HSS Name (HSS Redirect Host Mapping)

The Web Craft Interface (WebCI) is a web-based application that provides a user friendly graphical user interface (GUI). The WebCI is used to facilitate system configuration, subscriber provisioning, and alarm management.

WebCI navigation

The WebCI main menu is located to the left of the window. The menu provides access to the SDM applications.

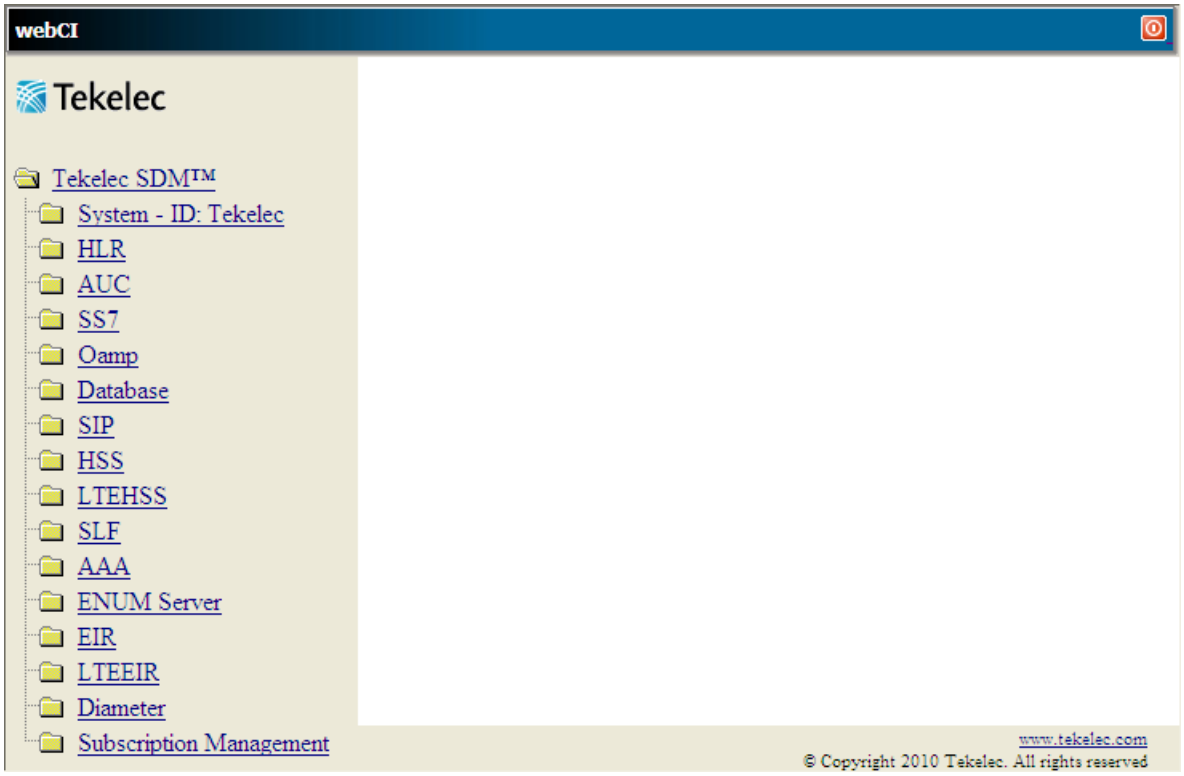


Figure 4: WebCI main window

Clicking the application name or folder opens a submenu. Each submenu item has a specific configuration window.

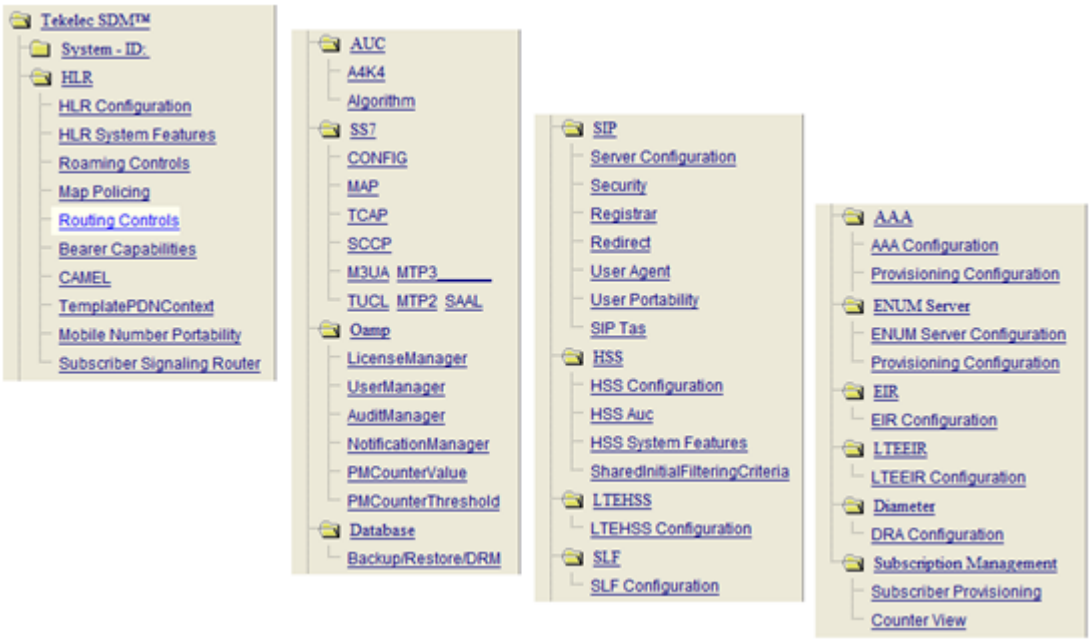


Figure 5: WebCI main menu expanded

These windows may have tabs to access additional configuration settings.

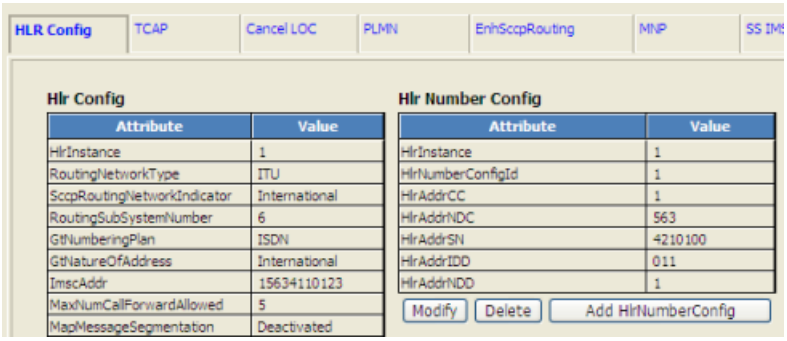


Figure 6: WebCI window tabs

WebCI main menu descriptions

This table describes the purpose of each menu item. The items are listed in order they appear on the menu.

Table 3: WebCI main menu descriptions

Application	Folder	Description
System	**Shelf View**	Provides information on each of the hardware platform's slots (processors) and the services running on each one of them. This window allows to configure the system with identities/services on each slot. This view also allows to perform Switch Overs.
	Shelf Inventory	Displays Shelf information and the software version.
	Service Management	Provisions services to each slot's Identity. Also allows the operator to manage those services on each slot.
	Geo Redundancy View	Provides information on the geo-redundant feature, whether it is enabled or disabled and what the Geo-Redundancy Virtual IP (VIP) address of the peer site is, as well as information on the state of the database. It also allows to enable or disable the feature and to modify the Geo-Redundancy VIP address of the peer site.
	Active Alarm View	Provides a listing of all active alarms existing on the shelf.
	History Alarm View	Provides a listing of all alarms that have occurred as well as those that have been cleared on the system.

HLR	**HLR Configuration**	The HLR Configuration window provisions the HLR through these tabs:
		• **HLR Config:** Provisions
		  • HLR Configuration parameters and activate/deactivate HLR features
		  • HLR Number Configuration

		• HLR SIP Subscriber Information for MAP SRI Interworking with SIP Subscribers • **TCAP:** Allows manual execution of the TCAP out-of-service and TCAP in-service operations. • **Cancel LOC:** Allows manual execution of a Cancel Location and a Cancel GPRS Location. • **PLMN:** Allows manual provisioning of Plmns and Home Plmns. • **Enhanced SCCP Routing:** Allows enhanced control of SCCP Routing. • **MNP:** Allows manual activation/deactivation of the Mobile Number Portability functionality. • **SS IMSI Range:** Allows the provisioning of mulitiple IMSI ranges for the XML Notifications on SS Management feature.
	HLR System Features	Provisions USSD messaging handling parameters such as Service Code, Application Node, and Application Node address. Moreover, it allows to configure the following HLR features: FTN Management, FTN Digits Analysis, XML notification on NDC change, Short Number Translation on RegSS.
	Roaming Controls	Provisions PLMN and IMSI Rejection error causes, VLR/PLMN Definitions, OCPLMN templates, Allowed IMSI ranges and Service Screening Templates.
	MAP Policing	Defines custom templates by provisioning Application Context templates and AcTemplateMapping to associate each of these templates to a node number. It also displays the NodeNumber and NodeNumberAcMapping tables. It also enables the operator to force the Tekelec ngHLR to send MAP_Reset messages to peer nodes.

	Routing Controls	Allows the Network Operator to:
		• Define Destination Router addresses
		• Define Routing Templates for the GSM/IMS Router (MT-SMS/SRI/SRI-LCS/ATI routing). Defining a routing template consist mainly in setting the following:
		  • Routing trigger
		  • Routing type
		  • Destination Router
		  • Default Action
		• Define Routing exceptions (only applies for MT-SMS routing)
		• Define a subscriber IMSI for Redirect Routing (only applies to MT-SMS routing)

	Bearer Capabilities	Provisions different types of Bearer Capability information, each identified by a unique BearerCapName to which MSISDNs can be associated to when provisioning the subscriber profile.
	CAMEL	Provisions the HLR Camel USSD General Csi parameters, Camel GSM Service Control Functionality and the CamelServiceMaskTemplate for enhanced CAMEL handling.
	TemplatePDN Context	This window allows to define PDN Context Templates for the LTE-HSS profiles. Each PDN Context provisioned for a LTE-HSS profile must have a PDN Context Template assigned to it.
	Mobile Number Portability	Provisions the Mnp entity in order to provision the Number Portability data for each "ported" MSISDN and the ImsiForRedirect entity in order to provision the IMSI that must be returned in the SRI-ack when the Tekelec ngHLR redirects the interrogating node to the recipient's network.
	Subscriber Signaling Router	Activates/Deactivates SSR (Subscriber Signaling Router functionality) and provisions SSR Templates and assigns them to an IMSI or IMSI range and to a MSISDN or MSISDN range.
AUC	**A4/K4**	Provisions the A4/K4 Transport Encryption Algorithm by defining A4/K4 combinations.
	Algorithm	Provisions the Authentication algorithms that will be used to authenticate subscribers.
SS7	**CONFIG**	Allows to view the activation status of the SS7 and SIGTRAN links
	MAP	Provisions MAP general parameters, SAP, Application context, and Timer profile.
	TCAP	Provisions TCAP general parameters, SAP, and Timer profile.
	SCCP	Provisions SCCP general parameters, Timer profile, Network SAP, User SAPs, Route, Concerned Area, Global title entries and SCCP addresses.
	M3UA	This is part of the SIGTRAN protocol. It is used to provision M3UA general parameters, Network, Network SAP, SCT SAP, PSP, PS and Route.
	MTP3	Provisions MTP3 general parameters, Network SAP, Timer profile, Signalling points, Combined Linksets, Linksets, Links, and Routes.
	MTP2	Provisions MTP2 general parameters, Service Access Point (SAP), and Timer profiles.

	SAAL	Provisions SAAL general parameters and Service Access Point (SAP).
	TUCL	This is part of the SIGTRAN protocol. It is used to provision the TUCL general parameters and the TUCL Sap (TSap).
Oamp	**License Manager**	Displays the License information and allows to view the number of active subscribers at the end of each month. It also allows to provision active and total thresholds.
	User Management	Manage users, following the USM feature, the group they are in and their password as well as their access privileges.
	AuditManager	Provisions The AuditManager entity: • The Audit log message format (CSV or XML) • The number of days that the old audit log files must be kept in the /export/audit director. • The debug information request in order to request the following debug information to be included in each audit line: slot, module, file and line. By default, this debug information is not included. The AuditInfo entity: • The new AuditInfo entity has been implemented to allow the Network Operator to view the information that is being audited and its audit status: Enable or Disable.
	NotificationManager	Manage notification subscription permissions/properties for each application and users.
	PMCounterValue	Allows to view the current value of OS Resource and HLR Subscriber counters.
	PMCounter Threshold	Allows to view and edit the thresholds implemented for the OS Resource counters.
Database	**Backup/Restore/ DRM**	Performs a manual backup and a restore of the entire database file or individually of some portions of the database. Can also perform an automatic backup of the subscriber's profile data. Also allows to manage the self healing functionality of the system (Database Monitoring Replication).
SIP	**Server Configuration**	Provides information on the SIP Configuration attributes and their values as well as on the Sip IP Configuration.
	Security	Provides information on the SIP Security Configuration attributes and their values.
	Registrar	Provides information on the Registrar Configuration and its Domain and provisions the RegistrationBinding.

	Redirect	Provides information on the SIP Redirect Configuration's attributes and their value.
	User Agent	Provides information on the SIP User Agent Configuration, the SIP User Agent Register Configuration, the User Agent PersistentContact and the IP User Agent Configuration attributes and their values. It also provides information on the UaRegistrationBinding.
	User Portability	Provides access to the NpAorUseRangePrefix table, which defines Address of Record user range prefixes.
	SIP Tas	Allows the Network Operator to conigure Telephony Application Server (TAS) data (Gt, Tt, Prefix, TasId, TasFQDN, OverrideTt, etc.). The SDM extracts the TAS data configured here when redirecting/relaying messages to an external TAS.
HSS	**HSS Configuration**	Provides information on the HSS Configuration, HSS Configuration TCP Listen Address and HSS Configuration SCTP Listen Address, their attributes and their values. Also allows the provisioning of HSS parameters such as HSS Configuration Destination Realm and HSS Configuration Destination Hosts.
	HSS AuC	Allows to configure the Authentication schemas and algorithms that will be used to authenticate IMS subscribers.
	HSS System Features	Provisions • HSS Subscriber configuration parameters, such as HSS Charging Info, HSS S-CSCF Server, HSS Authorized Visited Network and HSS AS Permanent list. • the SPR by defining the Service Indications supported by the SPR from the Sh interface and from the OAM&P provisioning interface, setting the Auto Enrollment feature and data compression level, configure internal receive queue, sequential write/read/write requests, HTTP and XML-REST request processing, and the logging of provisioning requests.
	SharedInitial FilterCriteria	Provision the Shared Initial Filter Criteria feature by allowing to define Shared Initial Filter Criterias and for each of them a list of Shared Service Point Triggers.
LTE-HSS	**LTEHSS Configuration**	The LTEHSS Configuration window provisions the LTE-HSS through these tabs: • **Config:** LTE-HSS Configuration, LTE-HSS Configuration TCP Listen Address and LTE-HSS Configuration SCTP Listen Address, their attributes and their values. Also allows the provisioning of LTE-HSS parameters such as LTE-HSS Configuration

		Destination Realm and LTE-HSS Configuration Destination Hosts. • **PLMN:** Defines allowed PLMNs for specific IMSI Ranges. This is used to allow/disallow roaming to subscribers depending on their IMSI Range and the PLMNs defined in this window. • **GMLCNodeList:** Defines valid GMLC nodes. These nodes are used to validate the GMLC number contained in the RIR (Routing Information Request) to ensure it belongs to a node authorized to request location services (LCS) routing information. • **Realms:** Defines valid LTE-HSS Realms. A host, realm and an IMSI range can be defined. These are used when the LTE-HSS receives a diameter request message from a node in another network and needs to determine the host and realm values to send in the response. It is also used when the LTE-HSS initiates a request message. • **VoLteStnSR:** Specifies the default STN-SR for the corresponding PLMNs when there is no STN-SR for the UE in volatile data. • **ASPermList** Contains a list of each Application Server (AS) that can communicate with the LTE-HSS. The list contains the originating host, the associated allowed data references, and a permission list.
	LTEHSS System Features	The LTEHSS System Features window: • Activates and deactivates LTE-HSS logging • Modifies LTE-HSS log file attributes • Activates and deactivates multiple realm support in the LTE-HSS • Activates and deactivates 3G/4G Roaming Support • Sets IDR Timeout value for STN-SR or T-ADS • Activates and deactivates LTE HSS Roaming Templates feature
	LTEHSS Roaming Templates	The LTEHSS Roaming Templates window provisions LTE-HSS Roaming templates (LRT) and related services through these tabs: • **Global Roaming Templates:** Creates an LRT and associates an IMSI range with an LRT service. • **PLMN:** Defines the PLMN IDs used in the roaming templates. • **Access Restriction:** Creates and defines the service template for allowing subscribers to connect via 2G/3G, 2G/3G/4G, 4G only or have no access. • **APN Filtering:** Creates and defines the service template for screening the APNs that are returned with the subscriber profile.

		• **VPLMN Address Allowed:** Creates and defines the service template for blocking the VPLMN Address Allowed within APNs that are returned to a visited network.
SLF	**SLF Configuration**	Provides information on the SLF Configuration, SLF Configuration TCP Listen Address and SLF Configuration SCTP Listen Address, their attributes and their values. Also allows the provisioning of SLF parameters such as SLF Configuration Destination Realm and SLF Configuration Destination Hosts.
AAA	**AAA Configuration**	Provides information on the AAA Configuration, AAA System Accounting Servers, AAA Network Access Servers and AAA NAS Accounting Servers, their attributes and their values.
	Provisioning Configuration	Provisions the Dynamic IP Address Allocation functionality by allowing to add, display, modify and delete AAA Address Allocation Policies, AAA Address Allocation Ranges and AAA Address Allocation Associations.
ENUM Server	**ENUM Server Configuration**	Allows to provision the following DNS data: • DNS Domain Name List • DNS ENUM User Template • DNS Black List Range • DNS Black List ENUM
	Provisioning Configuration	Allows to view and edit the ENUM Server and DNS Listen Addresses configuration data
EIR	**EIR Configuration**	The EIR configuration window defines: • The common EIR configuration • The IMEI range and associated equipment status for the range • The Diameter host authorized to establish new Diameter connection with EIR application. • Which equipment status to return in ECA if an EMEI has been configured in several lists (White/Grey/Black)
LTEEIR	**LTEEIR Configuration**	The LTE-EIR configuration window configures the Diameter protocol: • Defines Diameter host name and Diameter realm of the EIR for LTE. • Configures IP address for SCTP/TCP connections. • Defines Diameter host authorized to establish new Diameter connection with EIR application. • Defines list of authorized diameter realms

Diameter	**DRA Configuration**	The DRA configuration window configures the Diameter Relay Agent by defining the diameter host name of DRA to connect to the HSS

Subscription Management	**Subscriber Provisioning**	The Subscriber Provisioning window:
		• Defines SubscriptionIDs to represent subscribers.
		• Provisions SIM cards assigned or unassigned to a Subscription ID using one of the following operations:
		  • Assign SIM
		  • Unassign SIM
		  • Swap SIM
		  • Display Deferred Swap
		  • Delete HLR Subscriber using the Delete HLRSubscriber button
		  • Search subscriber profiles
		• View/Modify/Add/Delete Policy subscriber profiles
		• View policy quota and state data using the Policy PublicIdentity search
		• Delete quota data using the Reset Quota button in the Policy PublicIdentity search
		• View/Modify/Add/Delete an SPR Pool
		For each subscriber (SubscriptionID), provisions:
		• IMSIs for the SIM card assigned to the subscriber (SubscriptionID).
		• MSISDNs for the SIM card assigned to the subscriber (SubscriptionID).
		• IMSI-MSISDN associations (Primary and alternate) > Multiple IMSIs
		• HLR Subscriber Profile with a Service Profile in which services such as Call Forward, Call Barring, Closed User Group, Camel Service, Number ID, Call Completion, Call Waiting, and Change Service can be provisioned. Within the Service profile of an HLR Subscriber Profile, an LTE-HSS subscriber profile can also be provisioned.
		• SIP Subscribers and their AddressOfRecords
		• HSS Subscribers and their service profile by allowing to create Private Identities as well as Service Profiles and Public Identities. It also permits to create IMS-HSS Initial Filtering Criteria and link Public Identities for different service Profiles.
		• AAA users by creating AAA User IDs and specifying their Vendor Specific Attributes.
		• ENUM users
		• Link Public Identities to HSS Names for SLF Redirect Host Mapping.

Window display overview

Information shown on the screen provides a snapshot view. To view the current status, refresh the screen by clicking the application name on the main menu.

Note: The Shelf View and Active Alarm screens are dynamically updated. All the other screens provide a static view. Information shown on these screens provides a snapshot view. To view the current status, refresh the screen by clicking the application name on the main menu.

In the WebCI, the system entities are displayed as tables. In each window, a series of tables can be provisioned. The WebCI automatically stores the information provisioned in these tables in the system's corresponding database entities.

The following windows display tabs at the top that provide access to sub-categories of the window:

- HLR folder: HLR Configuration window
- SS7 folder: All windows
- SIP folder: Registrar and User Agent windows

Each tab displays different tables. This allows to keep the WebCI display more organized and the tables regrouped per category.

As an example, the figure below depicts the tabs in the HLR Configuration window:

The WebCI displays all the entities that can be edited by the operator for system configuration and subscriber provisioning. The operator can perform the following from the WebCI:

- System Configuration
- System Maintenance, Troubleshooting, Monitoring

SIM card and subscriber provisioning is usually performed in bulk with the SOAP/XML interface or with the Command File Loader. These interfaces are described in the *Subscriber Provisioning Reference Manual and User Guide*.

The different operations that can be performed to provision each of these tables are displayed in the form of a GUI button and are located nearby or within each table. After clicking on one of these buttons, a provisioning window will appear to allow you to set the values of the table's parameters to provision an entry in the table. In this provisioning window, the parameters identified by a * are mandatory parameters that have to be provisioned to be able to commit the entry.

Some WebCI windows also display buttons that are not specific to a table. These buttons are located independently from any table and they allow to perform operations when troubleshooting the system.

Other WebCI windows display some operations in a different format, with a symbol. For more details on the different operations format the WebCI displays, refer to the next section.

Shelf View

This window displays the information on each of the hardware platform's slots (processors) and the services running on each one of them. This window allows to configure the system with identities/services on each slot. This view also allows to perform Switch Overs.

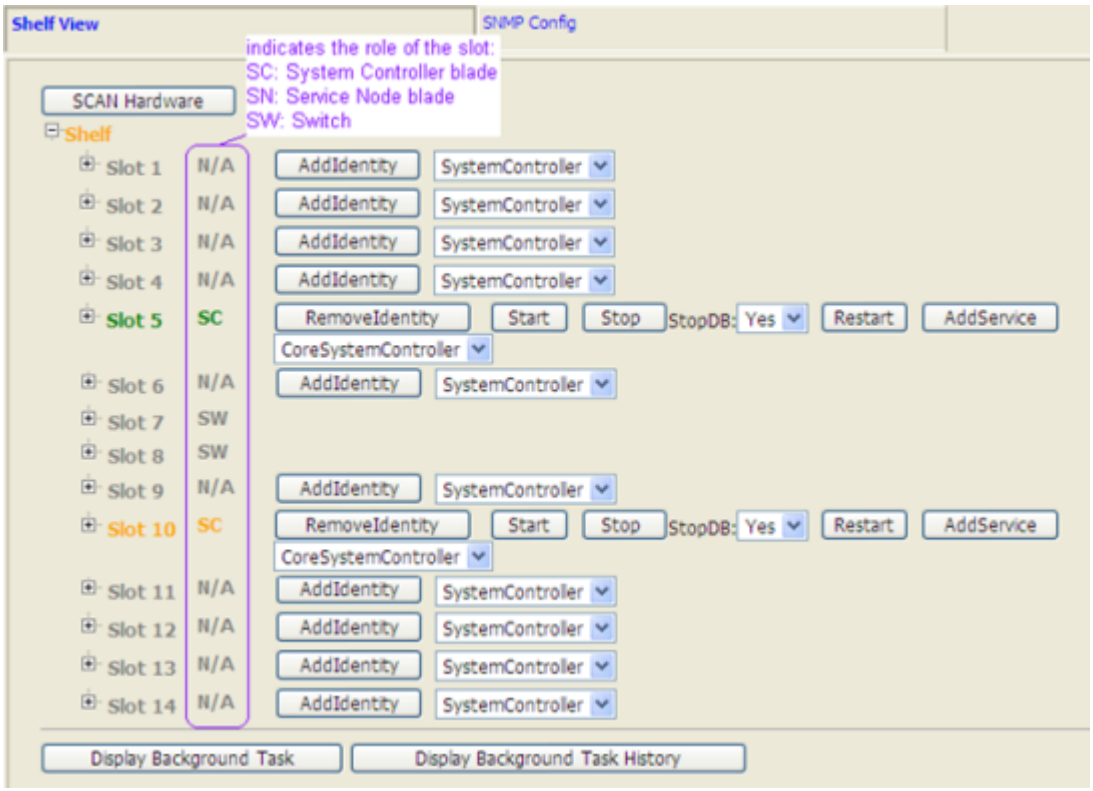
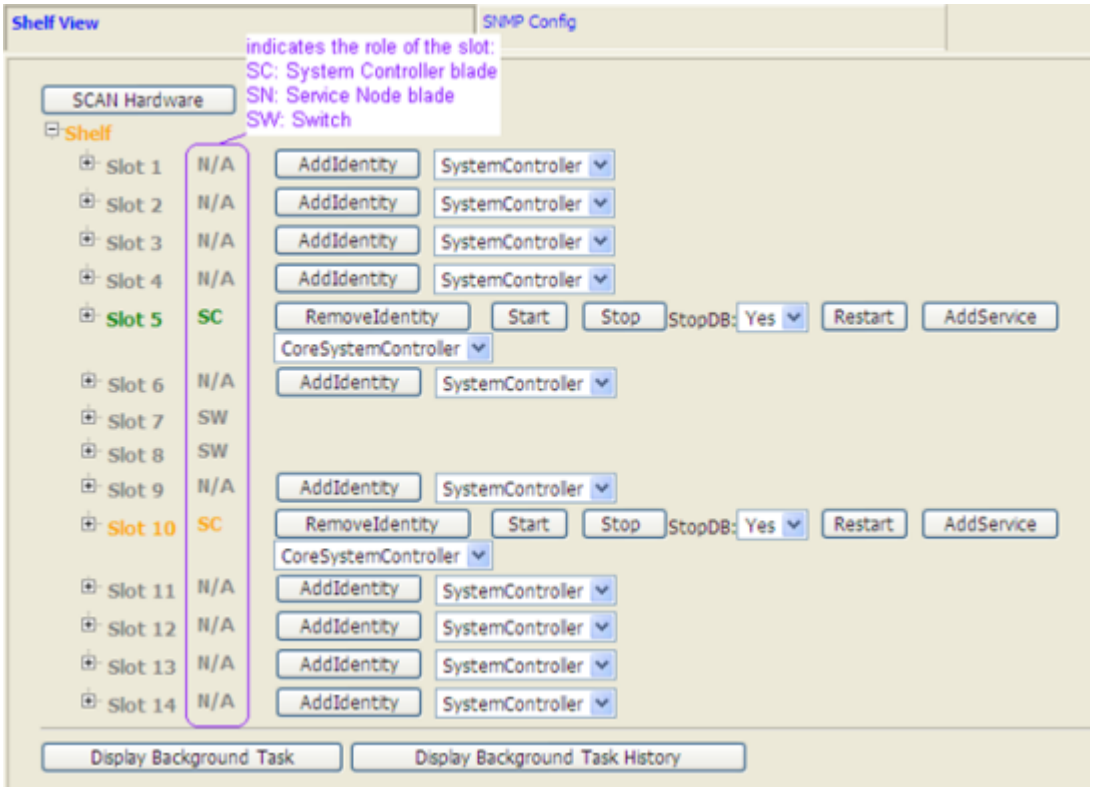


Figure 7: Shelf View Window

As you can see, in the Shelf View window, each slot is preceded by a ⊞ symbol. Clicking on it will display further information about the slot, such as: the services running on the slot and configuration operations that can be performed on the slot. Another ⊞ symbol precedes each slot's service(s), clicking on it will display further details about the processes running within each service and their state: ResourceState, HaRole, OpState, AdminState. For details about these different service states, refer to the "Services running on the system" section of the *SDM Product Description*.

Shelf View

The shelf View tab displays the slot (processor) information for each hardware platform and the services running on each. Use this window to configure the system identities and services per slot and perform switch overs.



In the Shelf View window, each slot is preceded by a Plus ⊞ symbol. Clicking the symbol will display further information about the slot, such as the services running on the slot and the configuration operations that can be performed on the slot. Another Plus ⊞ symbol precedes each slot's service(s), clicking the symbol will display further details about the processes running within each service and their state: ResourceState, HaRole, OpState, AdminState. For details about these different service states, refer to the "Services running on the system" section of the SDM Product Description.

Operations Available

The WebCI allows you to provision tables and perform different operations through buttons.

Some buttons provision the system entities and include add, delete, and modify operations. The buttons are located underneath the table or in each row within the table. They are labeled with the action to be performed, for example 

to add an HLR configuration.

In addition to the provisioning buttons, some operations are represented by symbols. The table provides a list of operations performed by symbols and provides the symbol location within the WebCI.

Table 4: Operations performed by symbols

WebCI folder	WebCI window	Symbol	Location in window	Operation
None (Main WebCI page)	None		Top right corner of Main page.	Logs out of the WebCI and ends the session.
System	**Active Alarm View**		In the last column to the right in the Active Alarm table, for each alarm.	Clears the alarm described in the same row.
System	**Active Alarm View**		Top right corner of the Active Alarm View window.	Acknowledges all alarms.
System	**Active Alarm View**		In the last column to the right in the Active Alarm table, for each alarm.	Acknowledges the alarm described in the same row.
System	**Active Alarm View**		Top right corner of the Active Alarm View window.	Stops the Auto-Refresh mechanism.
System	**Active Alarm View**			Starts the Auto-Refresh mechanism.
Not specific	Not specific		Varies	Displays the previous page or the previous entries in the table.
Not specific	Not specific		Varies	Displays the next page or the next entries in the table.

SS7	**MAP > GSM MAP** **MAP > Application Context** **MAP > GsmMap Timer Profile** **TCAP > Tcap Sap** **TCAP > Tcap Timer Profile** **SCCP > Timer Profile** **M3UA > SCT Sap** **MTP3 > Timer Profile** **MTP2 > MTP2 Sap** **MTP2 > MTP2 Timer Profile**		At the right of the table. It appears for each entry provisioned in this table.	Displays the SS7 layer's Timers Configuration table to allow you to edit the Timers.
SS7	**MAP > GsmMap Sap** **MAP > Application Context** **TCAP > Tcap Sap** **SCCP > Network Sap** **SCCP > User Saps** **SCCP > Route** **SCCP > Concerned Area** **M3UA > Network Sap** **M3UA > SCT Sap** **M3UA > PS** **M3UA > PSP** **MTP3 > Network Sap** **MTP3 > Signalling Point** **MTP3 > Routes** **MTP3 > Links** **MTP2 > MTP2 Sap** **Sigtran > Sigtran Local IP** **Sigtran > Sigtran Remote IP**		At the right of the table. It appears for each entry provisioned in this table.	Displays the parameters that can be modified in the table to allow you to edit an already provisioned entry.

SS7	**MAP > GsmMap Timer Profile** **TCAP > Tcap Timer Profile** **SCCP > Timer Profile** **SCCP > Route** **SCCP > Concerned Area** **SCCP > Global Title Entries** **SCCP > SCCP Addresses** **M3UA > Network** **M3UA > Network Sap** **M3UA > SCT Sap** **M3UA > PS** **M3UA > PSP** **M3UA > Route** **MTP3 > Timer Profile** **MTP3 > Signalling Point** **MTP3 > Combined Linksets** **MTP3 > Linksets** **MTP3 > Routes** **MTP3 > Links** **MTP2 > MTP2 Sap** **MTP2 > MTP2 Timer Profile** **TUCL > Tucl Sap** **SAAL > Saal Sap** **Sigtran > Sigtran Local IP** **Sigtran > Sigtran Remote IP**		At the right of the table. It appears for each entry provisioned in this table.	Deletes the entry already provisioned in the table.
SS7	**TCAP > Tcap Sap**		At the right of the table. It appears for each entry	Deletes unused TCAP dialogues.

			provisioned in this table.	
SS7	**TCAP > Tcap Sap**		At the right of the table. It appears for each entry provisioned in this table.	Deletes unused TCAP invokes.
SS7	**SCCP > Network Sap**		At the right of the table. It appears for each entry provisioned in this table.	Displays the parameters that can be edited to set the Sio Priorities.
SS7	**SCCP > User Saps** **SCCP > Concerned Area**		At the right of the table. It appears for each entry provisioned in this table.	Displays the Concerned PCs.
SS7	**SCCP > Route** **SCCP > Concerned Area**		At the right of the table. It appears for each entry provisioned in this table.	Displays the parameters that allow you to add/edit a backup Point Code for that SCCP Route.
SS7	**M3UA > SCT Sap**		At the right of the table. It appears for each entry provisioned in this table.	Bind s and creates a relation between the Sap user in the corresponding layer and its Sap provider in the lower layer.
SS7	**M3UA > SCT Sap**		At the right of the table. It appears for each entry provisioned in this table.	Deletes the relation between the Sap user in the corresponding layer and its Sap provider in the lower layer.
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	Establishes the PSP association between the Tekelec ngHLR and the remote peer (PSP) through an SctSap.
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	Terminates the association between the Tekelec ngHLR and the remote peer (PSP).
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry	Indicates to the peer that the Application Server process is up and that the SIGTRAN

			provisioned in this table.	applications are ready to receive traffic.
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	Indicates to the peer that the Application Server process is down and that the SIGTRAN applications are no longer ready to receive traffic.
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	Activates the Application Server process (ASP).
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	Deactivates the Application Server process (ASP).
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	The PSP Association is available to carry traffic.
SS7	**M3UA > PSP**		At the right of the table. It appears for each entry provisioned in this table.	The PSP Association is not available to carry traffic.
SS7	**MTP3 > Combined Linksets**		At the right of the table. It appears for each entry provisioned in this table.	Displays the linksets.
SS7	**MTP3 > Linksets**		At the right of the table. It appears for each entry provisioned in this table.	Displays the links.
SS7	**MTP3 > Linksets** **MTP3 > Links**		At the right of the table. It appears for each entry provisioned in this table.	Activates the linkset/link.
SS7	**MTP3 > Linksets** **MTP3 > Links**		At the right of the table. It appears for each entry	Deactivates the linkset/link.

			provisioned in this table.	
SS7	**MTP3 > Links**		At the right of the table. It appears for each entry provisioned in this table.	Blocks the link.
SS7	**MTP3 > Links**		At the right of the table. It appears for each entry provisioned in this table.	Inhibits the link.
SS7	**MTP2 > MTP2 Sap**		At the right of the table. It appears for each entry provisioned in this table.	Activates an MTP2 SAP to bind the MTP2 layer to the MTP3 layer.
SS7	**MTP2 > MTP2 Sap**		At the right of the table. It appears for each entry provisioned in this table.	Deactivates an MTP2 SAP to unbind the MTP2 layer to the MTP3 layer.

Sorting Alarms

From the Active Alarm View and History Alarm View windows, any of the alarm items can be sorted according to the heading names. Clicking on the heading name will toggle between sorting in ascending (shown by up arrow ↑) and descending order (shown by the down arrow ↓).

Auto Refresh

The WebCI has an auto-refresh mechanism that automatically refreshes and updates the Active Alarm View window every 15 seconds. This allows the following:

- The Active Alarm View window to dynamically display current active alarms.
- The WebCI session to remain refreshed and opened even if there is no activity performed on the WebCI for a certain period of time. To achieve this, the user must leave the WebCI opened with the Active Alarm View window opened.

It is possible to manually deactivate/activate the auto-refresh mechanism by performing the following from the Active Alarm View window:

- Stop the auto refresh cycle, by clicking the action button (in the top right corner) when it is red.
- Start the auto refresh cycle, by clicking the action button when it is green.

Note: The auto-refresh mechanism is active by default.

The refresh timer is displayed only for Internet Explorer browser windows. To view timer information, the View Status toolbar must be set to showing.

User Security Management

The SDM system offers its users high security by giving the administrator the capability to make the following user restrictions from any of the supported SDM user interfaces (CLI, WebCI, XML interfaces):

- Manage users by classifying them within groups with specific access privileges and services.
- Manage notifications sent to subscribed users about updates to certain applications (entities/attributes).

The following sections describe the entities and attributes available through the CLI and WebCI to manage user privileges.

User Security Management through WebCI

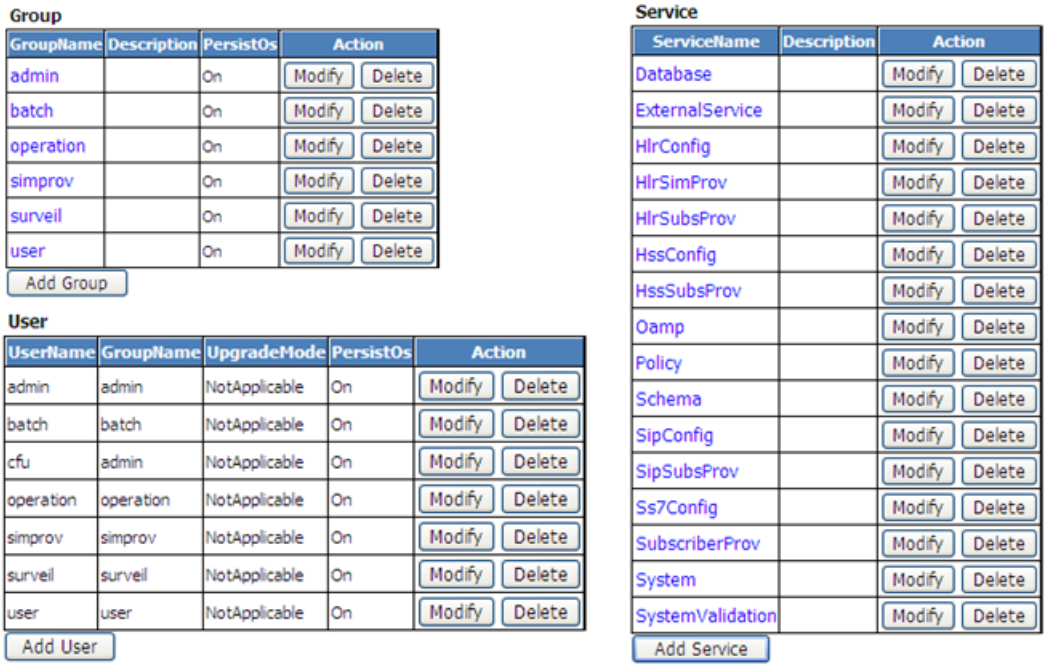


Figure 8: User Manager

The User Management window provides information on the user, its username and password, on the different Groups, its identifier and name, and on the access privileges (access permission) associated to each Group for a specific Service. The User Management window displays the following tables: User, Service, Group and AccessPrivileges. These tables can only be modified by the Admin Group, while each user can change their own password.

Through the WebCI, the administrator of the system, already defined in the admin group, can:

- Create new groups and provision the desired access privileges for each one of them, by provisioning the Group table.

- Modify the access privileges provisioned for each group (including pre-defined groups), by clicking on each GroupName link. This means that the administrator of the system can modify the permissions defined for each service of a specific group.
- Delete groups (including pre-defined groups, except the 'admin' group)
- Create new users and associate them to the right group by provisioning the User table.
- Delete users (including pre-defined users, except the 'admin' user)
- Modify the password of a user or the group to which the user (including predefined users) is associated to, by clicking on the 'Modify' button in the User table.
- Create/Delete services by provisioning the Service table.
  - **Warning:** The predefined services cannot be deleted since these are internal services and a deletion could impact the system.

For instructions on how to provision these tables, refer to the 'Creating and Managing users for the User Interfaces' section of the *SDM System Configuration - User Guide*.

User Security Management through CLI

Users can be managed only by the users in Group Admin, except for the fact that each user can change their own password. Please refer to the "Users" section of the *SDM Product Description* for details on the Admin Group.

This section describes the CLI commands to manage users through the CLI.

User

Name
User

Description

This is used to define users and their user name and password.

CLI Navigation
Oamp[]> SecurityManager[]> User

CLI Inherited Attributes

None

CLI Command Syntax

```
Oamp[]> SecurityManager[]>  add User [UserName = string; Password = string;
 GroupName = string]
```

Operations Permitted

Display, add

Attributes and Values

Table 5: User attributes

Mandatory Attributes	Value Range	Default	Description
UserName	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>"	N/A	Identifier that uniquely identifies a user.
Password	Minimum of 6 characters and up to 64 characters encrypted.	UserName (ex: UserName admin, UserPasswd: admin)	Encrypted password unique for each Group a user is associated to.
GroupName	Made of up to 64 characters in lowercase. Groups already predefined in the system: • operation • surveillance • admin • batch • simprov	N/A	Name of the Group to which the user is associated to. This gives access privileges to a user.
Optional Attributes	**Value Range**	**Default**	**Description**
UpgradeMode		Not Applicable	For future use.
PersistOS	Bool 0 , 1	0	This parameter indicates to the SDM system whether or not to store the user information in the Operating System (OS) in addition to being stored in the database. Once the user information is added to the OS, the user can login to the blade using terminal emulator. • 0=The user information is not stored in the OS, but only in the database. • 1= The user information is stored in the OS in addition to being stored in the database.

CLI Example

```
1 : Oamp[]> SecurityManager[]> display User[UserName = blue1]
```

Group

Name
Group

Description

This is used to define a user group (some are pre-defined at installation of the system), which consists of a group name and the right access granted for each service. A group may be associated to several users.

CLI Navigation
Oamp[]> SecurityManager[]> Group

CLI Inherited Attributes

None

CLI Command Syntax

```
Oamp[]> SecurityManager[]> display Group [GroupName = string]
```

Operations Permitted

Display, modify.

Attributes and Values

Table 6: Group attributes

Mandatory Attribute	Value Range	Default	Description
GroupName	Made of up to 64 characters in lowercase. Groups already predefined in the system: • user • operation • surveillance • admin • batch • simprov	N/A	Name of the Group that regroups users that have been categorized based on their system use and that have the same access privileges and access permission for the different entity services on the system. For more details on each of the predefined Groups, refer to the "Users" section of the *SDM Product Description*.

Mandatory Attribute	Value Range	Default	Description
PersistOS	Bool 0 , 1	0	This parameter indicates to the SDM system whether or not to store the user information in the Operating System (OS) in addition to being stored in the database. Once the user information is added to the OS, the user can login to the blade using terminal emulator. • 0=The user information is not stored in the OS, but only in the database. • 1= The user information is stored in the OS in addition to being stored in the database.
Optional Attribute	**Value Range**	**Default**	**Description**
Description	String (up to 256)	N/A	This parameter allows to give a clear description of the group.

CLI Example

```
1 : Oamp[]> SecurityManagement[]> display Group[GroupName = user]
```

Security Access Privileges

Name
SecurityAccessPrivileges

Description

This entity defines access privileges to a user group by making an association between a user group, a service, and an access permission. Each access privilege gives a single group the access permission (Read/Write/Execute) to a single service.

CLI Navigation
Oamp[]> SecurityManager[]> Group []> SecurityAccessPrivileges

CLI Inherited Attributes
GroupName

CLI Command Syntax

```
Oamp[]> SecurityManager[]> Group [GroupName = string] > display
SecurityAccessPrivileges [ServiceName=char; Permission=integer]
```

Operations Permitted

Display, add, modify

Attributes and Values

Table 7: SecurityAccessPrivileges attributes

Mandatory Attribute	Value Range	Default	Description
ServiceName	Integer except "0" Services that are already predefined in the system: • Database • ExternalService • HlrConfigHlr SimProv • HlrSubsProv • HssConfig • HssSubsProv • Oamp • Policy • Schema • SipConfig • SipSubsProv • Ss7Config SubscriberProv • System	N/A	Identifier that identifies a service and their associated entities. A service is associated to each user group to define to which entities it has access to. Please see *NOTE below for more details on the entities associated to the services.
Optional Attribute	**Value Range**	**Default**	**Description**
Permission	• **1 Read (Display)** • **2 Write (Add/ Modify/Delete)** • **3 ReadWrite** • **4 Execute (Access to entity own operations)** • **5 ReadExecute** • **7 Read WriteExecute**	N/A	Type of action a user group can do to the entities it has access to. Please see **NOTE below for more details on the access permissions allowed by a user group for all the different services.

Important: The User Security Management feature allows any module to supersede any access right, meaning that module could define their own access rights and those rights cannot be overwritten. For example, if a particular entity cannot be added or deleted, the module will prevent the user from adding or deleting the entity.

CLI Example

```
 1 : Oamp[]>
SecurityManager[]> Group[GroupName=user]> display
SecurityAccessPrivileges[ServiceName = Oamp]
```

Predefined services and associated entities

An entity can belong only to one service. The following table displays the different pre-defined services and their associated entities:

Table 8: Predefined services and associated entities

Service	Entities
System	System, Shelf, Slot, SmModule, Alarm, AlarmHistory
Subscriber Provisioning (Subscription)	All entities that are used to provision Subscriptions (SubscriptionID)
HLR Subscriber Provisioning	All entities that are used to provision a HLR subscriber profile.
SIM Provisioning	All entities that are used to provision Sim cards and associate them with IMSIs.
HLR Configuration	All the HLR entities that are used to configure the Tekelec ngHLR.
SS7 Configuration	All SS7/SIGTRAN entities that are used to configure SS7 and SIGTRAN.
HSS Subscriber Provisioning	All the HSS subscriber entities
HSS Configuration	All the HSS entities which are used to configure the HSS.
SIP Subscriber Provisioning	All the SIP subscriber entities
SIP Configuration	All the SIP entities which are used to configure the SIP functionality
Database	Database entity (Backup/Restore/DRM operations)
OAMP	LicenseManagement, UserManagement, NotificationManagement, Performance Management counter.
Schema	All the entities used by the schema: • CacheAttribute • Constraint • ConstraintAttribute • DataType • Entity • LdapAttribute

Service	Entities
	• LdapAttributeCriteriaRelation • LdapAttributeMapping • LdapAttributeMappingCriteria • LdapNamingContexts • LdapObjectClass • LdapObjectClassCriteria • LdapObjectClassCriteriaRelation • LdapRdn • Namespace • Operation • Parameter • PhysicalAccessPath • RDbDataType • Reference • ReferenceParameter • ResourceManager • Schema • Schemaversion • SchemaVersionFile • Token • TokenMaxPerCategory
External Service	Entities that are used to manage external services defined by the Network Operator in the Global Schema.
SystemValidation	All entities used for system validation.
Policy	Subscriber, IdMap, FieldInformation

Access permissions per service and group

Each access privilege gives a single group the access permission (Read/Write/Execute) to a single service. The access privileges table is defined or fined tune by the operators when needed (when a new group is added or an existing group needs to be altered).

Table 9: Predefined access permissions to services per user group

Services/Group	User	Operation	Surveillance	Admin	Batch	Simprov
System	R	RWX	R	RWX		
OAMP	R	R	R	RWX	R	
Database		RWX		RWX		
HLR subscriber prov	RWX			RWX	RWX	

Services/Group	User	Operation	Surveillance	Admin	Batch	Simprov
SIM provisioning	RWX			RWX	RWX	RWX
HLR configuration	RWX		R	RWX		
SS7 configuration	RWX		R	RWX		
SIP subscriber prov	RWX			RWX	RWX	
SIP configuration	RWX		R	RWX		
HSS subscriber prov	RWX			RWX	RWX	
HSS configuration	RWX		R	RWX		
External Service				RWX	RX	
Subscriber Provisioning	RWX			RWX	RWX	
Schema				RWX		
Policy				RWX		

R: Read (Display) W: Write (Add/Modify/Delete) X: eXecute (Access to entity own operations)

Important: The User Security Management feature allows any module to supersede any access right, meaning that a module could define its own access rights and those rights cannot be overwritten. For example, if a particular entity cannot be added or deleted, the module will prevent the user from adding or deleting the entity.

Service

Name
`Service`

Description

In addition to the internal services pre-defined in the system, the Network Operator can use this entity to define/modify/delete external services that regroup entities manually added by the Network Operator in the system's Global Schema.

CLI Navigation
`Oamp[]> SecurityManager[]> Service`

CLI Inherited Attributes

None

CLI Command Syntax

```
Oamp[]> SecurityManager[]> add Service [ServiceName = string; Description
= string]
```

Operations Permitted

Add, display, modify, delete

Attributes and Values

Table 10: Service attributes

Mandatory Attributes	Value Range	Default	Description
`ServiceName`	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>" The pre-defined services are as follows: • System • OAMP • Database • External service • Schema • HLR Subscriber prov • SIM provisioning • HLR configuration • SS7 configuration • SIP subscriber prov • SUP configuration • HSS Subscriber prov • HSS configuration • Subscriber prov • Policy	N/A	Identifier that uniquely identifies a service.
Mandatory Attributes	**Value Range**	**Default**	**Description**

Mandatory Attributes	Value Range	Default	Description
Description	**String** (up to 256)	N/A	Description that defines the service.

CLI Example

```
1 : Oamp[]> SecurityManager[]> display Service[ServiceName = HlrConfig]
```

Notification Security Management

The Oamp folder accesses the Notification Management functionality, which allows the management of users, applications, their notification registrations, and properties.

Notification Security Management through WebCI

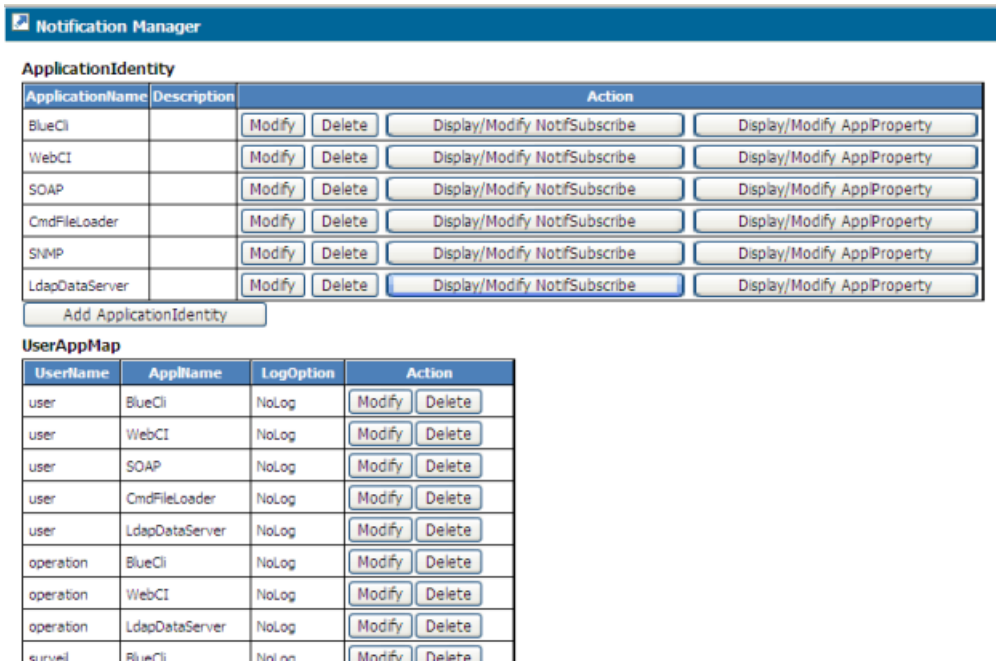


Figure 9: Notification Manager

The Notification Manager window provides information on the applications associated to each user (the applications allowed for each user) and on the applications' notification registration and properties. The user-application combinations are defined in the UserAppMap table. The external applications are defined in the ApplicationIdentity table, each with notification properties and registration permissions that can be defined/deleted in the ApplProperty and NotifSubscribe tables respectively.

For instructions on how to provision these tables, refer to the 'Creating and managing users/applications for the Notifications' section of the *SDM System Configuration - User Guide*.

Notification Security Management through CLI

This section describes the CLI commands that manage which user is allowed to request which type of notification through the CLI.

Only users in the Admin group can manage users, except that all users can change their own password. Refer to the "Users" section of the *SDM Product Description* for details on the Admin group.

Application Identity

Name

ApplicationIdentity

Description

This is used to define applications (application name and description) for which users associated to them will be able to subscribe to receiving notifications.

CLI Navigation

`Oamp[]> NotificationManager[]> ApplicationIdentity`

CLI Inherited Attributes

None

CLI Command Syntax

```
Oamp[]> NotificationManager[]> add ApplicationIdentity [ApplName = string;
Description = string]
```

Operations Permitted

Display, add, modify, delete

Attributes and Values

Table 11: ApplicationIdentity attributes

Mandatory Attribute	Value Range	Default	Description
`ApplName`	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>" The pre-defined applications are: • BlueCli • WebCI • CmdFileLoader • SNMP	N/A	Identifier that uniquely identifies an application.

Mandatory Attribute	Value Range	Default	Description
	• LdapDataServer • PolicyManager		
Optional Attribute	**Value Range**	**Default**	**Description**
Description	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>" The pre-defined applications are: • BlueCli • WebCI • CmdFileLoader • SNMP • LdapDataServer • PolicyManager	N/A	Identifier that uniquely identifies an application.

CLI Example

```
1 : Oamp[]> NotificationManager[]> display ApplicationIdentity[ApplName = BlueCli]
```

Notification Subscribe

Name
NotificationSubscribe

Description

This is used to define an NotificationSubscribe application's notification subscription capabilities: namespace, entity, Attribute. The application can only subscribe to notifications for changes/updates made to the entities' attributes or entity defined here.

CLI Navigation
Oamp[]> NotificationManager[]> ApplicationIdentity[]> NotificationSubscribe

CLI Inherited Attributes
ApplName

CLI Command Syntax

```
Oamp[]> NotificationManager[]> ApplicationIdentity [ApplName = char] > add
NotificationSubscribe [Namespace = char; Entity = char; Attribute= char]
```

Operations Permitted

Add, display, modify, delete

Attributes and Values

Table 12: NotificationSubscribe attributes

Mandatory Attribute	Value Range	Default	Description
Namespace	There are only two Namespaces in the Global Schema: • 'bn' • 'global' (this is only for the Subscription entity)	N/A	Namespace given for the entity in the Global Schema.
Entity	Name of entity in Global Schema.	N/A	Name of the entity for which notifications need to be sent if changes/updates are made.
ApplName	Up to 20 characters except the following: / \ [] : ; | = , + * ^ The pre-defined applications are: Unknown, Framework, SchemaManager, , SystemManager, DataProvider, DpController, OampEventViewer, OampEventMgr, OampManager, OampPerformanceManager, HlrServer, HlrProvManager, HlrWgs, AucServer, SS7Manager, SipServer, SipProvManager, NodeManager, TestModuleType, DpReplicator, BlueCli, WebCI, SOAP, CmdFileLoader, SNMP, HssServer, HssProvManager, SipUa, XmlDataServer, DpProxy, SubscriberManager, LdapDataServer, LteHssServer, LteProvManager, Drm, DataAccessServer, ExternalService, PolicyManager, RasServer, EirProvManager, DraProvManager	N/A	Name of the application that is registered to receive notifications on changes of the configured namespace/entity/attribute. This name should be the same as the name specified by the application in the *InterfaceModuleId* parameter when authenticating with the system through the *RequestUserAuc* operation.
Optional Attribute	**Value Range**	**Default**	**Description**
Attribute	Name of attribute belonging to the entity as defined in the Global Schema.	N/A	Name of the attribute for which notifications need to be sent if changes/updates are made.

CLI Example

```
1 : Oamp[]> NotificationManager[]> display ApplicationIdentity[ApplName = BlueCli]>
 add NotificationSubscribe[Namespace = bn;
Entity=MSISDN;Attribute=DefaultBsg]
```

Application Property

Name
ApplicationProperty

Description

This is used to define the properties of the notifications that must be sent out for each application. It allows the Network Operator to specify the following property for each application/entity for which notifications need to be sent: whether or not the previous value (before update) must be included in the notifications in addition to the current value (after update).

CLI Navigation
Oamp[]> NotificationManager[]> ApplicationIdentity[]> ApplicationProperty

CLI Inherited Attributes

ApplName

CLI Command Syntax

```
Oamp[]> SecurityManager[]> ApplicationIdentity [ApplName = char] > add
ApplicationProperty [Namespace = char; Entity = char; isValueBefore =
0,1]
```

Operations Permitted

Add, display, modify, delete

Attributes and Values

Table 13: ApplicationProperty attributes

Mandatory Attribute	Value Range	Default	Description
Namespace	There are only two Namespaces in the Global Schema: • 'bn' • 'global' (this is only for the Subscription entity)	N/A	Namespace given for the entity in the Global Schema.

Mandatory Attribute	Value Range	Default	Description
Entity	Name of entity in Global Schema.	N/A	Name of the entity for which notifications need to be sent if changes/updates are made.
Optional Attribute	**Value Range**	**Default**	**Description**
isValueBefore	**Bool 0 , 1**	**0**	This parameter indicates whether or not the previous value (before update of entity) must be sent in the notification in addition to the current value (after update of entity). For example, if the 'ValueBefore' property is set to 'On' for the MSISDN entity on the WebCI application, all the changes made to that entity (for example, on DefaultBsg) from this application will trigger a notification sending the previous DefaultBsg value (before update) and the current DefaultBsg value (after update).

CLI Example

```
1 : Oamp[]> NotificationManager[]> display ApplicationIdentity[ApplName = BlueCli]>
 add ApplicationProperty[Namespace = bn; Entity=MSISDN]
```

User Application Map

Name
UserApplicationMap

Description

This is used to define user-application combinations. Each user account must have one or several applications (as defined in the ApplicationIdentity entity) associated to it. The same user can have different applications associated to it with different logging properties. To achieve this, different entries with the same user name must be created in the UserApplicationMap entity.

CLI Navigation
Oamp[]> NotificationManager[]> UserApplicationMap

CLI Inherited Attributes

None

CLI Command Syntax

```
Oamp[]> NotificationManager[]> add UserApplicationMap [UserName=string;
ApplName=char; LogOption=0,1,2,3]
```

Operations Permitted

Display, add, modify, delete

Attributes and Values

Table 14: UserApplicationMap attributes

Mandatory Attributes	Value Range	Default	Description
UserName	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>" The pre-defined users are: • user • operation • surveillance • admin • batch • simprov	N/A	Identifier that uniquely identifies a user.
ApplName	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>" The pre-defined applications are: • Cli • WebCI • CmdFileLoader • SNMP • LdapDataServer • PolicyManager	N/A	Identifier that uniquely identifies an application.
Optional Attributes	**Value Range**	**Default**	**Description**
LogOption	• **0 NoLog** • **1 LogAll** • **2 LogRead** • **3 LogMod**	**0**	This parameter indicates which of the following logging options the SDM system should follow for each user-application combination: **0 NoLog**: No logs are saved by the system.

Mandatory Attributes	Value Range	Default	Description
			1 LogAll: The system saves logs for all the actions taken by this user on this application. WARNING: This could impact the performance of the system during high traffic. **2 LogRead**: The system saves logs only for the reading actions taken by this user on this application. **3 LogMod**: The system saves logs only for the modifying actions taken by this user on this application.

CLI Example

```
1 : Oamp[]> NotificationManager[]> add
UserApplicationMap[UserName=admin;ApplName=WebCI]
```

External Connections and Requests Logging

This section describes the 'ExternalConnectionLog' and 'RequestLog' entities that allow to view the logs generated by the SDM system on the external connections and the received requests.

As for the logging of external connections, a log is generated in the following cases:

- a new connection is established to the SDM's XmlDataServer
- an existing connection is terminated
- a failed attempt to connect is performed
- a connection is terminated by the server.

As for the logging of requests, a log is generated when allowed or denied requests are received from an interface. Take note that by default, the SDM system doesn't generate logs for received requests. The logging of requests is configurable (either from the CLI or WebCI) by the Network Operator and can be turned on (activated) or off (deactivated) for different users and applications, by setting the Oamp UserApplicationMap entity's 'LogOption' parameter to the desired value. For details on the 'UserApplicationMap' entity and its parameters, refer to *Notification Security Management* in this document. For instructions on how to provision the 'UserApplicationMap' entity, refer to the "Creating and Managing users/applications for the Notifications" section of the *SDM Monitoring,Maintaining,Troubleshooting-User Guide.*

Important: In the event where a very high number of subscribers are provisioned in the system in bulk within a seven day period, it is recommended that you turn off the logging of requests for all users/applications by setting the Oamp UserApplicationMap entity's 'LogOption' parameter to 'NoLog'. In the event where the 'ExternalConnectionLog' and

'RequestLog' entities become overflown with logs, contact the Tekelec *Customer Care Center* to perform a manual clean-up of the logs.

External Connections and Requests Logging Through CLI

The logs generated by the SDM system for external connections and requests are stored in the 'ExternalConnectionLog' and 'RequestLog' entities respectively. The logs generated within the last seven days are kept stored in these entities. A clean-up job is performed automatically by the system every day at midnight to delete the logs older than seven days.

This section describes the 'ExternalConnectionLog' and 'RequestLog' entities and their parameters as well as the CLI navigation path and commands to provision them.

External Connection Log

Name

`ExternalConnectionLog`

Description

This is used to store the logs generated by the system every time a new connection is established to the SDM's XmlDataServer, an existing connection is terminated, or a failed attempt to connect is performed.

CLI Navigation

```
Oamp[]> NotificationManager[]> ExternalConnectionLog
```

CLI Inherited Attributes

None

CLI Command Syntax

```
Oamp[]> NotificationManager[]> display ExternalConnectionLog []
```

Operations Permitted

`Display`

Attributes and Values

Table 15: ExternalConnectionLog Mandatory Logs

Attribute	Value Range	Default	Description
`UserName`	**`string`**	N/A	The name of the user connecting
`ApplName`	Up to 20 characters except the following: "/ \ [] : ; | = , + * ^ <>"	N/A	The name of the application connecting

Attribute	Value Range	Default	Description
	The pre-defined applications are: BlueCli WebCI CmdFileLoader SNMP LdapDataServer		
ConnectionId	**integer**	N/A	Identifier that uniquely identifies a connection.
ConnectionOper	**0,1,2,3,4**	N/A	Type of operation performed on the connection. 0: Connect - The connection is established 1: Disconnect - The connection is terminated by the client 2: Timeout - The connection is terminated by the inactivity timeout 3: ServerDisconnect - The connection is terminated by the server 4: AuthenticationFailed - The connection is refused due to a bad authentication
ConnectionTimestamp	Timestamp in format: day**MMM DD hh:mm:ss YYYY**	N/A	The time of the operation. MMM = month DD = date hh = hour mm = minute ss = second YYYY = year

CLI Example

```
1 : Oamp[]> NotificationManager[]> display
ExternalConnectionLog[UserName=admin;ApplName=SNMP]
```

Request Log

Name
RequestLog

Description

This is used to store the logs generated by the system for the requests received, as per configured in the Oamp UserApplicationMap entity's 'LogOption' parameter.

CLI Navigation
Oamp[]> NotificationManager[]> RequestLog

CLI Inherited Attributes

None

CLI Command Syntax
Oamp[]> NotificationManager[]> display RequestLog []

Operations Permitted
Display

Attributes and Values

Table 16: RequestLog Attributes

Attribute	Value Range	Default	Description
ReqTimestamp	Timestamp in format: day**MMM DD hh:mm:ss YYYY**	N/A	The time at which the request is received. MMM = month DD = date hh = hour mm = minute ss = second YYYY = year
ReqTimestampMsec		N/A	The millisecond portion of the timestamp
RequestType	**0,1**	N/A	Type of request received: 0: InputRequest received from the client 1: Notification sent to the client

Attribute	Value Range	Default	Description
ConnectionId	**integer**	N/A	Identifier that uniquely identifies a connection. As per defined in the 'ExternalConnectionLog' entity.
RequestXml	**XML string**	N/A	This parameter contains the whole request and the result of the execution in XML format.

CLI Example

```
1 : Oamp[]> NotificationManager[]>display RequestLog[ConnectionId = 123456]
```

Chapter 3

Error Notifications

Topics:

This chapter lists and describes the error notifications seen in various subsystems.

HLR Error Notifications

The following tables provide a list and a description of the error notifications for the HLR subsystem.

HLR Provisioning Notifications

Table 17: HLR Provisioning Error Notifications

ID	Notification Name	Description
5001	**InvalidEntity**	HlrProvManager received a request for an invalid entity.
5002	**InvalidImsiLength**	HlrProvManager received a request with an invalid IMSI – Incorrect number of digits.
5003	**InvalidImsiDigit**	HlrProvManager received a request with an invalid IMSI - Some digits are not numbers.
5004	**InvalidCallForwardBsgStatus**	HlrProvManager received a request with the invalid call forward states.
5005	**InvalidAocCAocIStatus**	HlrProvManager received a request provisioning an conflicted AocC and AocI status.
5006	**RejectDueToCallBarring RelationOnBsg**	Rejection: Call Barring relation on some Bsg.
5007	**RejectDueToCallForward RelationOnBsg**	Rejection: Call Forwarding relation on some Bsg.
5008	**RejectDueToCallWaiting RelationOnBsg**	Rejection: Call Waiting relation on some Bsg.
5009	**RejectDueToInvalidCugInterlock**	Rejection: Invalid interlock value.
5010	**RejectDueToInvalidNetworkType**	Rejection: Invalid network type.
5011	**RejectDueToInvalidNetworkPlan**	Rejection: Invalid network plan.
5012	**RejectDueToExistingPrefCidData**	Rejection: There is an existing preferred carrier-id.
5013	**RejectDueToOdbValidation**	Rejection: The ODB request is not validation.
5014	**RejectDueToUnsupportedCamelPhase**	Rejection: Unsupported Camel Phase. Please retry with Camel = 1 or 2.
5015	**RejectDueToInvalidCallBar SubsOption**	Rejection: The provision of Call Barring Subscription Option must include a valid Password.

ID	Notification Name	Description
5016	**RejectDueToIrrelevantCall FwdTypeForNoRplyCndTimer**	Rejection: The provision of NoReplyCondTimer is irrelevant to the given call forward type.
5017	**RejectDueToTS10Rule**	Rejection: When the Teleservice Service list contains TS10, do not add any other TS1x serie.
5018	**RejectDueToTS20Rule**	Rejection: When the Teleservice Service list contains TS20, do not add any other TS2x serie.
5019	**RejectDueToTS60Rule**	Rejection: When the Teleservice Service list contains TS60, do not add any other TS6x serie.
5020	**RejectDueToTS90Rule**	Rejection:When the Teleservice Service list contains TS90, do not add any other TS9x serie.
5021	**RejectDueToTS00Rule**	Rejection: When the Teleservice Service list contains TS00, do not add any other TSxx serie.
5022	**RejectDueToBS20Rule**	Rejection: When the Bearer Service list contains BS20, do not add any other PadAccessCa services.
5023	**RejectDueToBS30Rule**	Rejection: When the Bearer Service list contains BS30, do not add any other BS3x serie.
5024	**RejectDueToBS18Rule**	Rejection: When the Bearer Service list contains BS18, do not add any other dataCDS services.
5025	**RejectDueToBS28Rule**	Rejection: When the Bearer Service list contains BS28, do not add any other DataPDS services.
5026	**RejectDueToBS00Rule**	Rejection: When the Bearer Service list contains BS00, do not add any other BSxx serie.
5027	**RejectDueToZoneCodeLimit Capacity**	Rejection: The maximum number(10) of zone-code for that PLMN is reached.
5028	**RejectDueToInvalidCallFwdType**	The requested Call Forward type is not valid.
5029	**RejectDueToInvalidBsgId**	The requested BSG ID is not valid.
5030	**RejectDueToMissingFtn ForBsgState**	Missing forward-to-number when try to change the state for the given BSG.

ID	Notification Name	Description
5031	RejectDueToInvalidCallFwd StateForFtn	Invalid BSG state when provisioned forward-to-number.
5032	InvalidSubscriberCountRequest	Received an invalid Subscriber Count request - possible requests are GetImsiCount, GetMsIsdnCount or GetSimIdCount.
5033	CaughtDbSyncError	HlrProvManager caught synchronous database error.
5034	RejectDueToUnsupportedCCBS	Invalid parameter: Camel-CCBS is camel-phase3+ feature.
5035	RejectDueToInvalidDest NumbLength	Invalid parameter: A valid destination number length value is between [1 and 15].
5036	RejectDueToTooMuchDest NumbLength	Invalid parameter: The destination number length list cannot contain more 3 values.
5037	RejectDueToDestNumberCriteria ListExceedLimit	Invalid parameter: The number of Destination Number Criteria should not exceed 10.
5038	RejectDueToAnInvalidDest NumberLength	Invalid parameter: Invalid destination numbers is detected.
5039	RejectDueToCamelBsTsServ CriteriaListExceedLimit	Invalid parameter: The of total number Basic Service(Tele-service and Bearer-service) Criteria should not exceed 5.
5040	RejectDueToCugBsServList ExceedLimit	Invalid parameter: The of total number Basic Service(Tele-service and Bearer-service) should not exceed 32.
5041	RejectDueToCamelBsServCriteria ListExceedLimit	Invalid parameter: The Bearer-Service list Criteria exceeds the limit. The maximum number of basic-service criteria is 5.
5042	RejectDueToCamelTsServCriteria ListExceedLimit	Invalid parameter: The Tele-Service list Criteria exceeds the limit. The maximum number of basic-service criteria is 5.
5043	RejectDueToInvalidCamelSSEvent	Invalid Camel SS-Event: The supported Camel SS-Event are ECT, CD, MPTY.
5044	RejectDueToCamelSSEventList ExceedLimit	The number of Camel SS-Event exceeds the limit Invalid.
5045	RejectDueToInvalidDestination NumberCriteria	Invalid parameter: Invalid destination number is detected.
5046	RejectDueToInvalidBsInBs CriteriaList	The bearer-service criteria list contains invalid value(s).

ID	Notification Name	Description
5047	**RejectDueToInvalidTsInTs CriteriaList**	The tele-service criteria list contains invalid value(s).
5048	**RejectDueToInvalidCarrierId**	Rejection due to invalid Carrier-Id.
5049	**RejectDueToBS10Rule**	Rejection: When the Bearer Service list contains BS10, do not add any other dataCDA services.
5050	**RejectDueToBS40Rule**	Rejection: When the Bearer Service list contains BS40, do not add any other BS4x serie.
5051	**RejectDueToBS50Rule**	Rejection: When the Bearer Service list contains BS50, do not add any other BS5x serie.
5052	**RejectDueToBS60Rule**	Rejection: When the Bearer Service list contains BS60, do not add any other BS6x serie.
5053	**InvalidDeleteOperation**	Rejection: Request to delete this entity denied.
5054	**RejectDueToInvalid ProvisionState**	Rejection: Invalid provisioning state detected.
5055	**InvalidAltMsIsdnData**	Rejection: Alternate MSISDN value already exists in database as MsIsdn or AltMsIsdn.
5056	**UnsupportedMultiImsiDataUpdate**	Rejection: Operation modify %1 not supported.
5057	**InvalidRequest**	Invalid request not processed.
5058	**DatabaseError**	Got database error while processing request.
5059	**RejectDueToInvalidUssd ServiceCode**	Invalid Ussd-Service-Code: The valid ranges are 100-149, 70-79.
5060	**RejectDueToInvalidUssdAppNode**	Invalid Ussd-Application-Node.
5061	**RejectDueToInvalidUssd AppNodeAddress**	Invalid Ussd-Application-Node-Address.
5062	**DuplicateImsiError**	Imsi value is already provisioned as Alternate Imsi.
5063	**DuplicateMsIsdnError**	MsIsdn value is already provisioned as Alternate MsIsdn.
5064	**DuplicateImsiRangeError**	ImsiRange value is already configured in HlrNumberConfig.

ID	Notification Name	Description
5065	**UnsupportedIntraPlmnImsi RangeUpdate**	Must update a IntraPlmnImsiRange with an existing HPLMN and HlrNumberConfig.
5066	**UnsupportedIntraPlmnImsi RangeDelete**	Invalid Intra Plmn ImsiRange to delete
5067	**HlrNumberInUseError**	Could not delete a HLR Number used by provisioned subscribers.
5068	**UnexistingImsiRangeError**	Imsi must be within a configured IntraPlmnImsiRange.
5069	**InvalidRequestError**	Invalid request, rejection by the Hlr-Provisioning-Manager.
5070	**EmptyParameterForOperation**	Rejection: parameters required for this operation.
5071	**NodeNumberTooLong**	Rejection: The node number should have 15 digit maximum.
5072	**UnableToResetNodeAcVersion**	Rejection: Unable to reset the node-ac-version in the data base.
5073	**NonValidGsmScfId**	Rejection: Unable to reset the node-ac-version in the data base.
5074	**OperationNotSupportedYet**	Rejection: The requested operation is not supported yet.
5075	**MaxNumberSubsLicenseViolation**	Rejection: The maximum number of subscribers authorized by the license is reached.
5076	**DeleteSubsprofileNotAllowed**	Rejection: Please use DeleteSubsProfile operation available at Hlr[] !
5077	**RejectDueToInvalidMccLength**	Rejection: MCC Length not valid!
5078	**RejectDueToInvalidMncLength**	Rejection: MNC Length not valid!
5079	**RejectAddVlrToDefaultOCPlmn**	Rejection: Cannot add VLR to the default OCPlmn !
5080	**RejectDeleteDefaultOCPlmn**	Rejection: Cannot delete default OCPlmn !
5081	**RejectDueToInvalidVlrNumLength**	Rejection: Vlr Number Range Length not valid!
5082	**DuplicateOCPlmnConfigError**	HlrOCPlmnConfig already exists.
5083	**RejectMobileStationNotDefined**	Rejection: Subscriber Profile and Mobile Station must be defined before MultiImsi.

ID	Notification Name	Description
5084	**InvalidPublishedDisplayedFlags**	Rejection: Invalid Displayed and/or Published values for duplicated AltImsi/AltMsIsdn. Published = %1, Displayed = %2 required !
5085	**InvalidDisplayedFlag**	Rejection: Invalid Displayed value for duplicated AltImsi. Displayed = %1 required !
5086	**InvalidPublishedFlag**	Rejection: Invalid Published value for duplicated AltMsIsdn. Published = %1 required !
5087	**InvalidAltImsiData**	Rejection: Alternate IMSI value already exists in database as Imsi or AltImsi.
5088	**InvalidMultiImsiData**	Rejection: Invalid AltImsi/AltMsIsdn pair.
5089	**InvalidCriteria**	Rejection: Operation with Invalid Criteria.
5090	**InvalidPublishedDisplayed FlagsToBeRemoved**	Rejection: Specify message here .....
5091	**R99DefinedCantModifyR97**	Rejection: Defined as a R99 PDP, cannot modify R97/98 part.
5092	**R97DefinedCantModifyR99**	Rejection: Defined as a R97/98 PDP, cannot modify R99 part.
5093	**CannotModifyR99nR97**	Rejection: Cannot modify R99 and R97/98 PDP QoS.
5094	**IncompleteQoS**	Rejection: Incomplete QoS.
5095	**InvalidQoSValue**	Rejection: Invalid QoS value.
5096	**RejectAddCSISuppressTo DefaultOCPlmn**	Rejection: Cannot add ServiceKeyToSuppress to the default OCPlmn!
5097	**OperationNotSupportedYet**	Rejection: The requested operation is not supported yet.
5098	**InvalidSubModule**	Request for invalid submodule [%1].
5099	**InitializationFailed**	HlrProvisioningManager failed initialization %1.
5100	**UnsupportedIntraPlmn ImsiRangeInsert**	Must insert a IntraPlmnImsiRange referencing an existing HPLMN and HlrNumberConfig.
5101	**UnsupportedHplmnDelete**	Hplmn is referenced by an existing IntraPlmnImsiRange.

ID	Notification Name	Description
5102	**UnsupportedHlrNumber ConfigDelete**	HlrNumberConfig is referenced by an existing IntraPlmnImsiRange.
5103	**ImsiRangeInUseError**	Could not delete a IntraPlmnImsiRange Number used by provisioned subscribers.
5104	**SimNotProvisionedForThisImsi**	Sim Not Provisioned For This Imsi.
5105	**InvalidCClength**	Invalid Country Code: incorrect number of digits.
5106	**RejectDueToCugSubsInfo ExceedLimit**	The of total number Cug Subscription Info should not exceed the limit.
5107	**MapPolicyDisabled**	Map Policy is disabled, requested action is rejected.
5108	**MapPolicyActionOn DefaultTemplate**	Map Policy: Operation on Default Template is not authorized.
5109	**MapPolicyBadAcVersion**	Map Policy: Requested AC Version is not supported.
5110	**CugFeatureInvalidBsgId**	CUG Feature: BSG is not covered by any CUG for this subscriber.
5111	**CugFeatureInvalidCugIndex**	CUG Feature: Invalid CUG index for this subscriber.
5112	**CugFeatureInvalidCugPrefIndex**	CUG Feature: This CUG index cannot be used as a Preferential CUG index (outgoing calls barred).
5113	**RejectDefaultSmsRelay**	Sms Redirect: Operation not allowed for default SmsRelay.
5114	**RejectUpdateAssignedRelay**	Sms Redirect: Sms Relay in use - operation not allowed.
5115	**RejectDefaultSmsTemplate**	Sms Redirect: Operation not allowed for default MtSmsTemplate.
5116	**RejectAssignDefaultRelay**	Sms Redirect: Invalid SmsRelay for MtSmsRedirectTemplate.
5117	**RejectOperationReferenced Instance**	Operation not allowed - reference restriction.
5118	**UnsupportedHplmnCountryDelete**	Hplmn Country is referenced by an existing IntraPlmnImsiRange.

ID	Notification Name	Description
5119	**InvalidInputpdpAddress**	GPRS Context: Invalid Input for pdpAddress, only letter/digit/hyphen/dot are permitted
5120	**InvalidInputaccessPointName**	GPRS Context: Invalid Input for accessPointName, only letter/digit/hyphen/dot are permitted
5121	**RejectDueToInvalidTemplateId**	Rejection: TemplateId must be between 1 and %1 !
5122	**RejectAddTemplate**	Rejection: Default Template with TemplateId = %1 must be created first!
5123	**RejectDeleteTemplate**	Rejection: Cannot delete Default Template - TemplateId = %1 for all not default PLMNs must be deleted first!
5124	**RejectInvalidOperationOn DefaultEntity**	Rejection: Invalid operation on Default Template
5125	**UnsupportedIntraPlmnImsi UpdateKey**	Update of the ImsiRange is not allowed
5126	**DisabledSubscriber**	Operation not allowed because subscriber is disabled
5127	**InvalidFTNRule**	Invalid FTN Rule, FTN Rule cannot be set to NULL
5128	**InvalidInputNDC**	Invalid Input for NDC, only digits or * are allowed
5129	**InvalidNDClength**	Invalid National Destination Code: incorrect number of digits
5130	**DeleteDefaultCC**	Deletion of the default Country Code is not allowed
5131	**ModifyNDCMethodDefaultCC**	Modification of the NDC Method for the default Country Code is not allowed
5132	**NonOverlappingNDCList**	Overlapping of NDC per Country Code is not allowed in the NDC List
5133	**InvalidPdpContextIdRange**	Invalid Pdp Context Id: range is 1-50
5134	**DataproviderSessionNull**	Dataprovider or Session pointer is NULL
5135	**MandatoryParameterMissing**	Mandatory Parameter Missing: %1
5136	**RejectDueToInvalidCauseValue**	Invalid parameter: CauseValue must be between 1 and 127

ID	Notification Name	Description
5137	RejectDueToTooMuchCauseValue	Invalid parameter: CauseValue list cannot contain more than 5 values
5138	RejectDueToInvalidCamelPhase	Rejection: Invalid Camel Phase for CSI
5139	RejectDueToInvalidAttributeValue	Rejection: Invalid value for attribute %1
5140	UpdateAttributeNotAllowed	Rejection: Modify operation not allowed for %1
5141	RejectDueToTooMuchAnalyzedInfoCrit	Rejection: D-CSI Cannot have more than 10 AnalyzedInfoCriteria
5142	AttributeIsNull	Cannot set attribute %1 to null
5143	CCNDC15DigitsMax	Country Code and National Destination Code cannot have more than 15 digits
5144	RejectDeleteProvisionedCamel	Rejection: Cannot delete Camel if ProvisionedState = 1
5145	RejectDeleteProvisionedCsi	Rejection: Cannot delete Csi if ProvisionedState = 1
5146	DstNumberOverlap	Rejection: Destination number overlaps existing number
5147	BadValueNotReachableReason	Invalid value for notReachableReason (subsState != NetDetNotReachable
5148	MissingValueNotReachableReason	Missing value for notReachableReason
5149	BadValueSubsState	Invalid value for subsState (notReachableReason != None)
5150	DuplicateAlertMsIsdn	Rejection: MsIsdnAlertInd value already exists in database as MsIsdn or AltMsIsdn of another subscriber
5151	MapPolicyNoTemplateId	Map Policy: No value provided for TemplateId
5152	HlrNumberConfigIdNotSpecified	HlrNumberConfigId is not specified in the request
5153	HlrSipSubscriberInfo	Hlr SipSubscriber Info: %1
5154	HlrMnp	Mobile Number Portability: %1
5155	RejectDueToInvalidHLRSPID	The provided HLR Service Profile is not valid.

ID	Notification Name	Description
5156	CannotModifyHlrSPID	The HLR Service Profile ID cannot be modified in the MsIsdnImsiProfileAssociation table.
5157	CannotFindSubscriptionID ofMSISDN	Cannot find the Subscription ID of the MSISDN.
5158	CannotFindSubscriptionID ofHlrSPID	HLR Service Profile ID doesn't exist for the Subscription ID.
5159	CannotFindSubscriptionIDofSIM	Cannot find the Subscription ID of the SIM.
5160	SIMIDofIMSInotFound	SIM Id of the provided IMSI not found.
5161	MaximumOneSameImsiDisplayed	Maximum one same IMSI can be displayed in the MsIsdnImsiProfileAssociation table.
5162	AllSameMSISDNSameSIMID	All the IMSI associate to same MSISDN must have the same SIM ID.
5163	SubscriptionIDnotSameImsiAnd Msisdn	Subscription ID is not the same for the IMSI and the MSISDN.
5164	SubscriptionIDnotSameImsiAnd HlrSPID	Subscription ID is not the same for the IMSI and the HLR Service Profile ID.
5165	SubscriptionIDnotSameMsisdn AndHlrSPID	Subscription ID is not the same for the MSISDN and the HLR Service Profile ID.
5166	CannotProvisionNonDisplayed MsisdnFirst	Cannot provision non-displayed MsIsdn for one IMSI if the IMSI doesn't have a displayed MsIsdn.
5167	DisplayedMsisdnRemovedLast	Displayed MSISDN of an IMSI must be removed last.
5168	OneDisplayedMsisdnAtAllTime	Each IMSI must have one displayed MsIsdn at all time.
5169	CannotChangeImsiDisplayed IfStillOtherSameImsi	Cannot change IMSI of a displayed MSISDN if there are other same IMSI with non-displayed MSISDN.
5170	InvalidCriteriaMsIsdnImsi ProfileAssociation	InvalidCriteria: Delete operation for MsIsdnImsiProfileAssociation requires Imsi, MsIsdn and HLR Service Profile ID
5171	CannotModifyMsIsdnFromMSISDN table	Cannot modify MsIsdn of the MSISDN table.
5172	ImsiNotProvisionedInSimImsiMap	Imsi Not Provisioned in the SimImsiMap table.

ID	Notification Name	Description
5173	CannotModifySubscriptionID	The Subscription ID cannot be modified in the MsIsdnImsiProfileAssociation table.
5174	SubscriptionIDnotSame ImsiAndSubscriptionID	Subscription ID is not the same for the IMSI and the Subscription ID.
5175	SubscriptionIDnotSame MsisdnAndSubscriptionID	Subscription ID is not the same for the MSISDN and the Subscription ID.
5176	OnlyHLRServiceProfile1Allowed	Cannot Provision HLR Service Profile ID, only HLR Service Profile ID 1 is allowed.
5177	HlrSsr	Subscriber Signaling Router: %1
5178	MaximumOneCSI	Rejection: Maximum One Camel Phase for this CSI.
5179	RejectAddPlmnData	Rejection: Default Plmn must be added first to OCPLMN Template Id = %1
5180	RejectDeletePlmnData	Rejection: Default Plmn must be deleted last.
5181	OCPlmnInvalidPlmnId	Invalid PlmnId: %1
5182	OCPlmnInvalidTemplateId	Invalid OCPlmn TemplateId: %1
5183	OCPlmnInvalidServiceScreen TemplateId	Invalid Service Screening TemplateId: %1
5184	OCPlmnInvalidNodeRange	Invalid Input: NodeRange is empty.
5185	OCPlmnInvalidImsiRange	Invalid Input: ImsiRange is empty.
5186	OCPlmnInvalidAction	Invalid Action: %1
5190	MaximumLengthSmallerThan MinimumLength	Maximum Length is Smaller Than MinimumLength.
5191	MinimumLengthGreaterThan MaximumLength	Minimum Length is Greater Than Maximum Length.
5192	SimProvAucServerNull	Sim Provisioning: AucServer pointer is NULL.
5193	ServiceKeyNotApplicableSSCSI	Cannot update ServiceKey: ServiceKey not applicable for SS-CSI.
5194	CugFeatureInvalidBsgOperation	CUG Feature: BSG is still in use by CugFeature and cannot be removed.
5195	SimProvAucHashNull	Sim Provisioning: Auc Hash pointer is NULL.
5196	SubscriptionIDnotSameHLRSPID AndSubscriptionID	Subscription ID is not the same for the HLR Service Profile ID and the Subscription ID.

ID	Notification Name	Description
5197	**SharedMSISDNStillInUse SubscriptionID**	Shared MSISDN still used in association where the SubscriptionID of association is not the same as SubscriptionID of the MSISDN.
5198	**SharedMSISDNStillInUseSimID**	Shared MSISDN still used in association where the SIM ID of all association for the MSISDN is not the same.
5199	**MaxOneSimReachable**	Maximum 1 SIM can be reachable per MSISDN.
5200	**SameMSISDNonSameSIMSame Reachable**	Same MSISDN on same SIM must have the same reachable value.
5201	**NoUpdateReachableFor MultipleAssociation**	Cannot update Reachable flag of MSISDN if it's set for multiple IMSI, use operation.
5202	**MSISDNAlreadyReachableOn OtherSim**	The MSISDN is already reachable on another SIM, only one SIM can be reachable at a time per MSISDN.
5203	**SimIdOfImsiDifferentOfSimId**	The SimId of the Imsi provided in parameters is not equal to the SimId provided in parameters.
5204	**SSInteractionWithCallBarring**	SS activation rejected due to Interaction with CB.
5205	**SSInteractionWithCallForward**	SS activation rejected due to Interaction with CF.
5206	**BadSSProvisioning**	SS activation rejected due to bad SS provisioning.
5207	**FtnGenericError**	SS activation rejected due to invalid FTN.
5208	**FtnEmpty**	SS activation rejected due to empty FTN.
5209	**FtnTifCsiInteraction**	SS activation rejected due to interaction with TIF-CSI.
5210	**FtnOdbInteraction**	SS activation rejected due to interaction with ODB rules
5211	**FtnBoicInteraction**	SS activation rejected due to interaction with BOIC rules.
5212	**FtnMgmtRulesInteraction**	SS activation rejected due to interaction with FTN Management rules.
5213	**CfInvalidStateTransition**	Invalid State Transition for Call Forward BSG.
5214	**CbInvalidStateTransition**	Invalid State Transition for Call Barring BSG.

ID	Notification Name	Description
5215	**SSInteractionMptyCh**	SS MultiParty and CallHold have a provisioning interaction.
5216	**SSInteractionWithODB**	SS activation rejected due to Interaction with ODB.
5217	**SSInteractionEctCh**	SS Explicit Call Transfer and CallHold have a provisioning interaction: CallHold is required for Explicit Call Transfer.
5218	**SSInteractionTS11Mpty**	Cannot provision Multi Party if TeleService TS11 is not provision.
5219	**CannotRemoveProvFlagCW**	Cannot remove the Call Waiting provisioning flag if a Call Waiting Activation Station (BSG) is still provision.
5220	**CannotRemoveProvFlag**	Cannot remove %1 if BSG is still provisioned.
5230	**CannotRemoveProvFlagCB**	Cannot remove the Call Barring provisioning flag for a specific Barring ID if there are still BSG provision for the corresponding Barring ID.
5231	**CannotRemoveProvFlagCF**	Cannot remove the Call Forward provision state flag for a specific Call Forward Type if there are still BSG provision for the corresponding Call Forward Type.
5232	**CannotModifyBsg**	Cannot manipulate Bsgs if %1 is in unprovisioned state.
5233	**SSInteractionTSBS**	Cannot provision Supplementary Service if the corresponding TeleService/BearerService are not provision.
5234	**SSInteractionTS11**	Cannot provision Supplementary Service if the TeleService TS11 is not provision.
5235	**TS11SSInteraction**	Cannot remove TeleService TS11 if Supplementary Service (CallHold, MultiParty or Explicit Call Transfer) is provision.
5236	**TSBSSSInteraction**	Cannot remove TeleService/Bearer Service if corresponding Supplementary Service are still provision.
5237	**FtnChangeError**	Invalid State Transition - FTN change not allowed"
5238	**FtnEmptyError**	Invalid State Transition - FTN not allowed
5239	**FtnRequiredError**	Invalid State Transition - FTN required

ID	Notification Name	Description
5240	CannotUpdateDisplayedFlag	Cannot update displayed flag in MsIsdnImsiProfileAssociation table, use operation ModifyDisplayedMSISDN()
5241	MemoryAllocationError	Error allocating memory
5242	NoResultDB	Could not get results from database.
5243	TooManyResultDB	Too many results returned from database.
5244	CannotUpdateDelete	Cannot Update/Delete %1, instance doesn't exist.
5245	SimTypeAlgorithmNameMissing	SIM and USIM Sim type's must have an AlgorithmName valid, %1.
5246	Ki32HexCharMissing	Missing Mandatory Attributes: Ki32HexChar.
5247	PrefixInvalid	Destination Router Prefix parameter is invalid, valid digits: 0-9, a-e, A-E.
5248	InvalidDefaultImsiLength	Invalid IMSI - Incorrect number of digits, IMSI must be 5 to 15 digits.
5249	RouterAddressInvalid	Destination Router Address parameter is invalid, valid digits: 0-9, a-e, A-E.
5250	TableNotSupported	Cannot Add/Update/delete data, this table is not supported for the current release.
5251	SSCodeNotSupportedLCS	SSCode Not Supported in the current release: SSCode can only be set to universalClass (177) or plmnOperatorClass (180).
5252	PPRAddressLengthNotValid	PPRAddress length Not valid, PPRAddress must contain at least 10 Hexadecimal characters.
5253	HGMLCAddressLengthNotValid	HGMLCAddress length Not valid, HGMLCAddress must contain at least 10 Hexadecimal characters.
5254	PPRAddressNotValid	PPRAddress Not valid, PPRAddress must be in Hexadecimal.
5255	HGMLCAddressNotValid	HGMLCAddress Not valid, HGMLCAddress must be in Hexadecimal.
5256	InternalClientNotPresentPlmnOperatorClass	PlmnOperatorClass must contain at least one Internal Client.
5257	MaxOneOCPLMNDataPerPLMN	Maximum one OCPLMN Template Definitions (OCPLMN_DATA) per PLMN for OCPLMN Template Id = %1

ID	Notification Name	Description
5258	MaxTwoOCPLMNDataPerDefaultPLMN	Maximum two OCPLMN Template Definitions (OCPLMN_DATA) per default PLMN for OCPLMN Template Id = %1
5259	MaxOneAppNodeTypeVLR_SGSNPerPLMN	Cannot use Applicable Node Type VLR_SGSN if there is more than one OCPLMN Template Definitions (OCPLMN_DATA) per default PLMN for OCPLMN Template Id = %1

HLR Server Errors

Table 18: HLR Server Error Notifications

ID	Notification Name	Description
200	BadHlrInterfaceType	Bad Hlr Interface Type (HlrInterfaceType) in the Service Option (SmServiceOption), supported value are e1 or t1
201	SlotAlreadyAssign	The Slot is already assign to an GsmMapSap
202	NoAvailableSlotInGsmMapSap	There is no available slot in GsmMapSap table
203	SlotNotFoundInInGsmMapSap	The slot is not assign to any GsmMapSap
9000	InvalidRequest	HlrServer received an invalid request from CLI, HLR only supports Display and Delete requests.
9001	InvalidCriteria	HlrServer received a request with an invalid criteria, version 1.1 only supports the criteria - where Imsi = imsiValue.
9002	InvalidEntity	HlrServer received a request for an invalid entity.
9003	InvalidAttribute	HlrServer received a request for an invalid attribute.
9004	InvalidImsi	HlrServer cannot retrieve IMSI for parameter list.
9005	UnknownImsi	HlrServer received a request for an unknown Imsi.
9006	NotGprsImsi	HlrServer received a request for an unknown Imsi.
9007	OperationNotSupported	HlrServer received an unknown operation.
9010	AucInvalidRequest	AucServer received an invalid request from CLI.

ID	Notification Name	Description
9011	**AucInvalidCriteria**	AucServer received an invalid criteria from CLI.
9012	**AucInvalidEntity**	AucServer received an invalid entity from CLI.
9013	**AucInvalidAttribute**	AucServer received an invalid attribute from CLI.
9014	**InvalidFileName**	AucServer received an invalid file name from CLI.
9015	**InvalidOperatorVariantValue**	AucServer received an invalid operator variant value from CLI -Op32HexChar value must be 32 hexadecimal digits.
9016	**InvalidKiValue**	AucServer received an invalid Ki value from CLI -Ki32HexChar value must be 32 hexadecimal digits.
9017	**InvalidPUKValue**	AucServer received an invalid PUK value from CLI- PUK value must be 10 decimal digits.
9018	**InvalidPUK2Value**	AucServer received an invalid PUK2 value from CLI - PUK2 value must be 10 decimal digits.
9019	**GotDBError**	AucServer received a DB error.
9020	**InvalidRValue**	AucServer received an invalid R value from CLI - R values must be max 4 hexadecimal digits.
9021	**InvalidCValue**	AucServer received an invalid C value from CLI - C values must be 32 hexadecimal digits.
9022	**UnsupportedAlgoTypeUpdate**	AucServer received invalid request - can not modify AlgorithmType.
9023	**MaxNumberOfAlgorithmsReached**	AucServer reject - Max number of Algorithms reached.
9024	**InvalidSubmodule**	HlrServer received a request destined for invalid submodule [%1].
9025	**A4K4IndexInvalid**	A4K4 index table invalid [%1].
9026	**K4EncryptionError**	K4 encryption error.
9027	**K4Invalid**	K4 invalid.
9028	**A4K4AlgoIdNotProvided**	K4 invalid.

ID	Notification Name	Description
9029	**A4K4KiDecryptionError**	Cannot decrypt Ki with A4K4.
9030	**A4K4NotActivated**	Cannot decrypt Ki with A4K4.
9031	**A4Invalid**	A4 invalid.
9032	**ManufactureIdEmpty**	The Manufacture Id cannot be empty.
9033	**MapResetInProgress**	MapReset %1.
9034	**SameImsi**	Imsi Swap: OldImsi = NewImsi, cannot swap.
9035	**InvalidOldImsi**	Imsi Swap: OldImsi doesn't exist, cannot swap.
9036	**NewImsiNotFound**	Imsi Swap: NewImsi not found in the AucSim table, cannot swap.
9037	**NewImsiNotFree**	Imsi Swap: NewImsi exist (not free), cannot swap.
9041	**HLRinOverload**	HLR is in Overload
9042	**ImsiSwapMultiImsiProvision**	Imsi Swap: Multi-IMSI provision for the old IMSI, cannot swap
9043	**AddSIMErrorSimAlreadyExist**	AddSIM error: SimId already exist in AucSim table.
9044	**CannotFindEntrySimSwapDeferred**	Cannot find entry in SimSwapDeferred table: cannot Cancel Sim Swap Deferred.
9045	**AddSIMInvalidPrimaryImsiLength**	AddSIM error: Invalid Primary IMSI - Incorrect number of digits, IMSI must be 5 to 15 digits.
9046	**AddSIMInvalidAlternateImsiLength**	AddSIM error: Invalid Alternate IMSI (IMSI2 to IMSI15) - Incorrect number of digits, IMSI must be 5 to 15 digits.
9047	**AddSIMErrorSubscriptionID doesNotExist**	AddSIM error: SubscriptionID doesn't exist in the Database in table Subscription (Case sensitive). This error occurs if the Network Operator uses the operation AddSIM() and provides a SubscriptionID that is not in the database in the table Subscription or if the SubscriptionID is not exactly the same in the table Subscription (Case Sensitive).
9048	**DeleteHLRSubscriberSubIDNotFound**	SubscriptionID not found in the database.

ID	Notification Name	Description
9100	**ImsiOrSimIDNotPresent**	IMSI or SIM ID not provided while trying to insert IMSI in SimImsiMap table.
9101	**MaximumOnePrimaryImsiPerSim**	Maximum One Primary IMSI per SIM.
9102	**CaughtException**	Caught Exception %1
9105	**CannotProvisionImsiIfNo PrimaryImsi**	Cannot provision multi-IMSI in SIM if primary IMSI is not provision, primary IMSI must be provision first.
9106	**CannotDeletePrimaryImsiIf NotLast**	Cannot delete Primary IMSI if there is others IMSI on the SIM, Primary IMSI must be removed last.
9107	**SimSwapSameSim**	Old SIM ID and New SIM ID must be different.
9108	**OldSimNotFound**	Old SIM Not Found in the Database (AucSim).
9109	**NewSimNotFound**	New SIM Not Found in the Database (AucSim).
9110	**SimSwapSubscriptionIDNotSame**	Subscription ID of new SIM is different of the Subscription ID of the Old SIM or is not NULL.
9111	**SimSwapNoImsiNewSim**	No IMSI found on the new SIM card.
9112	**SimSwapNoImsiOldSim**	No IMSI found on the old SIM card.
9113	**SimSwapNewImsiUsed**	One of the IMSI of the new SIM card is used in the MsIsdnImsiProfileAssociation table.
9114	**SimSwapAutoMapFail**	AutoMap fail: Cannot Map all alternate IMSI (MCC/MNC).
9115	**SimSwapDeferredFailToInsert**	Sim Swap Deferred: Inserting row in SimSwapDeferred failed.
9116	**SimSwapNotEnoughImsiNewSim**	Number of IMSI of new SIM card must be greater or equal to number of different IMSI provision in MsIsdnImsiProfileAssociation for Old SIM card.
9117	**SimSwapCannotCreateTransaction**	Sim Swap: Cannot create new transaction.
9118	**SimSwapRollbackDueTo RequestFail**	Sim Swap: Rollback on all request executed due to one or many request failing.
9119	**AssignSimNoSubscriptionID**	Subscription ID was not provided in the AssignSIM operation.
9120	**NoSimID**	SIM ID was not provided in the operation.

ID	Notification Name	Description
9121	**CannotFindSimID**	Cannot find SIM ID in the Database (AucSim table).
9122	**SimCannotUpdateExisting SubscriptionID**	SIM has already a subscriptionID: Cannot Assign SIM.
9123	**AssignSimCannotUnassignIf ImsiUsed**	Cannot Unassign SIM if the IMSI(s) of the SIM are use in the MsIsdnImsiProfileAssociation table.
9124	**NoSimForSubscriptionID**	No SIM found with the subscription ID.
9126	**DeleteHLRSubscriberImsiOr SubscriptionID**	Must provide IMSI or SubscriptionID, not both or none.
9127	**DeleteHLRSubscriberCannot FindImsiWithSubscriptionID**	Cannot find the SubscriptionID with the provided IMSI.
9128	**ModifyDisplayedMSISDN CannotFindOldDisplayed**	Cannot find the value of displayed flag for IMSI-OldMsIsdn.
9129	**ModifyDisplayedMSISDNOld DisplayedNotTrue**	Displayed flag of IMSI-OldMsIsdn is not equal to 1.
9130	**CannotCreateNewRequest**	Displayed flag of IMSI-OldMsIsdn is not equal to 1.
9131	**ModifyDisplayedMSISDNCannot FindNewDisplayed**	Cannot find the value of displayed flag for IMSI-NewMsIsdn.
9132	**ModifyDisplayedMSISDNNew DisplayedNotFalse**	Displayed flag of IMSI-NewMsIsdn is not equal to 0.
9133	**CannotCreateTransaction**	Cannot create new transaction
9134	**CommitTransactionFail**	Commit Transaction Fail.
9135	**RollbackDueToRequestFail**	Rollback on the transaction for all request executed due to one or many request failing.
9136	**SimSwapInputSubscriptionIDNot SameOldSubscriptionID**	Input Subscription ID is different of the Subscription ID of the Old SIM.
9139	**FeatureOperationError**	FeatureOperationError: %1
9140	**SimSwapNewSimIntraPlmnImsi RangeNotFound**	Sim Swap Fail: All IMSI of the New SIM Id must be within a configured IntraPlmnImsiRange.
9141	**SimOpCorrupted**	Cannot Provision SIM: Op32HexChar (Operator Variant) is corrupted.

ID	Notification Name	Description
9142	**CannotUnassignSimNo SubscriptionID**	SIM has no subscriptionId: Cannot Unassign SIM.
9143	**SriRoutingActivated**	Sri Routing has been activated.
9144	**SriRoutingDeactivated**	Sri Routing has been deactivated.
9200	**SsrError**	SSR Error: %1
9201	**SsrWarning**	SSR Warning: %1
9202	**SsrNotice**	SSR Notice: %1
9904	**DlgReinitWrongRangeParameter**	HlrServer has received a wrong parameter range for dialogue reinitiation.
9905	**DlgReinitDBRequestFail**	HlrServer encountered an error during a database request.
9906	**DlgReinitUnknownError**	HlrServer encountered error during the provisioning of dialogue reinitiation.

SS7 Error Notifications

The following tables provide a list and a description for CLI, General, MAP, MTP2, MTP3, SCCP, and TCAP error notifications.

Table 19: CLI Error Notifications

Error ID	Description
10006	The description for this error ID can be one of the following:
	CLI (Validation)
	Invalid input parameter. Invalid 'PhyNumber' value.
	Invalid input parameter. Invalid 'Speed' value.
	Invalid input parameter. Invalid 'Mtp2ProtocolVariant' value.
	Invalid input parameter. Invalid 'ServiceIndicator' value.
	Invalid input parameter. Invalid 'Mtp3ProtocolVariant' value.
	Invalid input parameter. Invalid 'NetworkIndicator' value.
	Invalid input parameter. Invalid 'SignallingType' value.
	Invalid input parameter. Invalid 'PcLength' value.
	Invalid input parameter. Invalid 'SlsRange' value.

Error ID	Description
	Invalid input parameter. Invalid 'PcType' value.
	Invalid input parameter. Invalid 'RestartReqProcedure' value.
	Invalid input parameter. Invalid 'RouteDirection' value.
	Invalid input parameter. Invalid 'SccpProtocolVariant' value.
	Invalid input parameter. Invalid 'RouteVariant' value.
	Invalid input parameter. Invalid 'ReplicatedMode' value.
	Invalid input parameter. Invalid 'PeerNwSupport' value.
	Invalid input parameter. Invalid 'ActionType' value.
	Invalid input parameter. Invalid 'Format' value.
	Invalid input parameter. Invalid 'OddEven' value.
	Invalid input parameter. Invalid 'NatAdd' value.
	Invalid input parameter. Invalid 'NumPlan' value.
	Invalid input parameter. Invalid 'EncSch' value.
	Invalid input parameter. Invalid 'RtgInd' value.
	Invalid input parameter. Invalid 'HdrOpt' value.
	Invalid input parameter. Invalid 'TcapProtocolVariant' value.
	Invalid input parameter. Invalid 'RetOpt' value.
	Invalid input parameter. Invalid 'ProtocolClass' value.

Table 20: General Error Notifications

Error ID	Description
10000	Unsupported request type received on Standby Side.
	Unsupported request type received on Active Side.
10001	Request to insert unsupported entity denied. For this entity use the Create Method within the appropriate LayerManager.
	Request to insert unsupported entity denied. Unsupported entity.
10002	Request to update unsupported entity denied. Update Request on multiple instances is not supported by the SS7 module.
	Request to update unsupported entity denied. Unsupported entity.
10003	Request to delete unsupported entity denied. Delete Request on multiple instances is not supported by the SS7 module.

Error ID	Description
	Request to delete unsupported entity denied. To delete an OamTimerVal, his corresponding TimerProfile shall be delete (Mtp2TimerProfile, Mtp3TimerProfile ...). Then the OamTimerVal entity will be automatically deleted.
	Request to delete unsupported entity denied. Unsupported entity.
10006	The description for this error ID can be one of the following:
	Application Context
	Parsing of Application Context Name failed. Shall be of length 0 or 8.
	Parsing of Alternative Context Name failed. Shall be of length 0 or 8.
10007	The description for this error ID can be one of the following:
	GSM stack manager init failed
	Could not assume slot-id from hostname
	SS7 stack manager init failed
	bluemain(): Cannot create application
	SS7 stack manager init wgs observer failed
	SS7 stack manager init failed. Unable to retrieve the WGS ORLs from the database.
	Memory allocation failed.
	GsmMapLayer - smMaActvTsk() failed.
10008	**SS7FaultTolerantHighAvailabilityFailure**
	Description of this error ID can be one of the following:
	RyChannelCfg
	RyChannelCfg::enable - Channel not configured yet
	RyChannelCfg::reEnable - Couldn't enable the RY channel
	SgStackManager
	SgStackManager::enableSg - Couldn't enable SG
	SgStackManager::disableSg - Could not disable SG
	SgStackManager::enableAlarm - Couldn't enable SG alarm
	SgStackManager::disableAlarm - Couldn't disable SG alarm
	SgStackManager::enableNode - Couldn't enable node %d
	SgStackManager::disableNode - Couldn't disable node %d
	SgStackManager::statusIndication - Error - Received Status indication for SG_LO_API!!!
10009	**SS7FaultTolerantHighAvailabilityWarning**

Error ID	Description
	Description of this error ID can be one of the following:
	Couldn't get SG location from DB. Error: %d
	Confirmation received with unknown transaction Id
	SgStackManager
	SgStackManager::smSgActvTskCallback - Unknown event
	SgStackManager::configConfirm - Config request failed with reason = %d for transaction = %d
	SgStackManager::controlConfirm - Control request failed with reason = %d for transaction = %d
	SgStackManager::statusConfirm - Node Status request failed with reason = %d for transaction = %d
	SgStackManager::statusConfirm - Entity Status request failed with reason = %d for transaction = %d
	SgStackManager::statusConfirm - RSet info request failed with reason = %d for transaction = %d
	ShStackManager
	The ShStackManager will use this error to report trace indication that will include the date and time, the source and destination, the transaction ID and the event/status/reason.
10010	**SS7MandatoryParameterMissing** This error ID can have multiple different descriptions depending on the use case. If there is a parameter missing in an operation on the OAM (addition/modification/deletion), this alarm will be used to report it.
10011	**SS7DoesNotExist** This error ID can have multiple different descriptions depending on the use case. It is generally used in the SS7 stack manager to report missing elements.
10012	**SS7InvalidID** This error ID can have multiple different descriptions depending on the use case. It is generally used in the SS7 stack manager to report a problem with an identifier in the OAM operation (addition/modification/deletion).
10014	**SS7SuaError** SuaConvergenceLayer::sua_unitdata_req() failed with error =%d
10015	**SS7LdfAlarmError**
	Description of this error ID can be one of the following:
	Mtp3StackManager

Error ID	Description
	Mtp3StackManager - SmMiLdnStaInd Alarm received: category=%d event=%d cause=%d
	SccpStackManager
	SccpStackManager - SmMiLdpStaInd Alarm received: category=%d event=%d cause=%d
	TcapStackManager
	TcapStackManager - SmMiLdtStaInd Alarm received: category=%d event=%d cause=%d
	M3uaStackManager
	M3uaStackManager - SmMiLdvStaInd Alarm received: category=%d event=%d cause=%d
	M3uaStackManager - SmMiLdvStaCfm received:
	M3uaStackManager - SmMiLdvTrcInd received:
	M3uaStackManager - SmMiLdvCntrlCfm received:
10018	The description for this error ID can be one of the following:
	Received an operation for an entity that doesn't support that operation.
	Update request with unsupported criteria denied.
	Delete request with unsupported criteria denied.
	Ss7StackManager
	Ss7StackManager::unprotectCallback called but standby procId unknown.
	Ss7StackManager::unprotectCallback - invalid peer state.
	Ss7StackManager::checkpointCallback - invalid message type.
	Ss7StackManager::queryWgsLinkStatus() - unable to publish query message.
	Ss7StackManager::ryChannelStatusCb - unable to publish link status.
	RyStackManager
	RyStackManager::receiveChannelAnnounceMessage - unable to re-enable server channel.
	RyStackManager::receiveChannelAnnounceMessage - unable to re-enable client channel.
	RyStackManager::processorDisconnectTimeout - timer not found.
	RyStackManager::disconnect - procId not found.
	RyStackManager::RyChannelCfg::reEnable - not configured.
	RyStackManager::getIpAddress ioctl SIOCGIFADDR failed.
	RyStackManager::receiveChannelAnnounce - unknown message type

Error ID	Description
	RyStackManager::SmMiLryCfgCfm - invalid transaction id
	RyStackManager::RyChannelCfg::initialize - unknown channelType
	RyStackManager::RyChannelCfg::cntrlCfm - unknown transId
	SgStackManager
	SgStackManager::enableSg - couldn't enable sg.
	SgStackManager::enableSs7Layer - couldn't enable SS7 layers.
	SgStackManager::enableMapGsm - couldn't enable map gsm.
	SgStackManager::disableSg - couldn't disable sg.
	SgStackManager::disableSs7Layer - couldn't disable SS7 layers.
	SgStackManager::disableMapGsm - couldn't disable map gsm.
	SmMiLryStsCfm
	SmMiLryStsCfm - unknown elmnt

Table 21: MAP Error Notifications

Error ID	Description
10006	The description for this error ID can be one of the following:
	GsmMapGenCfg
	Reference of the MapGsmTimerProfile to set is NULL.
	Creation of the GenCfg failed at the SS7 stack interface.
	The SignallingFrameSize maximum value is 272.
	Updating the SignallingFrameSize of this GenCfg, failed at the SS7 stack interface.
	GsmMapLayerManager
	Maximal Number of GsmMapTimerProfiles has been reached.
	A GsmMapSap cannot be created before a GsmMapGenCfg object.
	Reference on the tcapSap is NULL.
	Maximal Number of GsmMapSaps has been reached.
	Only one GsmMap Gen Config can be created.
	Maximal Number of ApplicationContexts has been reached.
	Reference of the GsmMapTimerProfile to delete is NULL.
	GsmMapTimerProfile cannot be deleted because there is either a GsmMapSap of an ApplicationContext referencing it. Delete first every entities referencing this GsmMapTimerProfile.

Error ID	Description
	Reference of the GsmMapSap to delete is NULL.
	Enabling all the GsmMapSaps failed at the SS7 stack interface.
	Disabling all the GsmMapSaps failed at the SS7 stack interface.
	Enabling the alarm for the GsmMap Layer failed at the SS7 stack interface.
	Disabling the alarm for the GsmMap Layer failed at the SS7 stack interface.
	Enabling the debug print for the GsmMap Layer failed at the SS7 stack interface.
	Disabling the debug print for the GsmMap Layer failed at the SS7 stack interface.
	Enabling the tracing for the GsmMap Layer failed at the SS7 stack interface.
	Disabling the tracing for the GsmMap Layer failed at the SS7 stack interface.
	GsmMapSap
	Maximal Number of ApplicationContexts per GsmMapSap has been reached.
	One of the ApplicationContext to associate with this GsmMapSap is NULL.
	Creation of the GsmMapSap resource failed at the SS7 stack interface.
	The SSN maximum value is 255.
	Activation of the GsmMapSap failed at the SS7 stack interface.
	Enabling of trace generation for the sap failed at the SS7 stack interface.
	Disabling of trace generation for the sap failed at the SS7 stack interface.
	Reference of the GsmMapTimerProfile to set is NULL.
	Modification of the GsmMapSap failed at the SS7 stack interface.
	Allowable range for GsmMap msg priority is from 0 to 3.
	Updating this GsmMapSap failed at the SS7 stack interface.
10007	The description for this error ID can be one of the following:
	GsmMapLayerManager::readCurrentConfiguration() error when initializing the SS7 GSMMAP Layer.
	GsmMapLayerManager::readCurrentConfiguration() NullPointerException when initializing the SS7 GSMMAP Layer.
	GsmMapLayerManager::readCurrentConfiguration() IllegalOperationException when initializing the SS7 GSMMAP Layer.
	GsmMapLayerManager::readCurrentConfiguration() TooManyInstancesException when initializing the SS7 GSMMAP Layer.
	GsmMapLayerManager::readCurrentConfiguration() Unexpected Exception when initializing the SS7 GSMMAP Layer.

Table 22: MTP2 Error Notification

Error ID	Description
10006	The description for this error ID can be one of the following:
	MTP2LayerManager
	Maximal Number of Mtp2TimerProfiles has been reached.
	Maximal Number of Mtp2Saps has been reached.
	Reference of the Mtp2TimerProfile to delete is NULL.
	Mtp2TimerProfile cannot be deleted because there is an Mtp2Sap referencing it. Delete first every entities referencing this Mtp2TimerProfile.
	Reference of the Mtp2Sap to delete is NULL.
	Mtp2Sap cannot be deleted because there is a Link referencing it. Delete first every entities referencing this Mtp2Sap.
	Enabling the alarm for the Mtp2 Layer failed at the SS7 stack interface.
	Disabling the alarm for the Mtp2 Layer failed at the SS7 stack interface.
	Enabling the debug print for the Mtp2 Layer failed at the SS7 stack interface.
	Disabling the debug print for the Mtp2 Layer failed at the SS7 stack interface.
	Enabling the flow control for the Mtp2 Layer failed at the SS7 stack interface.
	Disabling the flow control for the Mtp2 Layer failed at the SS7 stack interface.
	MTP2Sap
	Channel number for ANSI variant shall be between 0 - 23 inclusively.
	Channel number for ANSI variant shall be between 0 - 23 inclusively. Creation of the Mtp2Sap resource failed at the SS7 stack interface.
	Activation of the Mtp2Sap failed at the SS7 stack interface.
	Reference of the Mtp2TimerProfile to set is NULL.
	The protocol variant of the Mtp2TimerProfile to assign is not the same as this Mtp2Sap.
	Modification of the Mtp2Sap failed at the SS7 stack interface.
	The maximum msg size for a Sap when the service provider is MTP2 is 272.
	Enabling the flow control for the Mtp2Sap failed at the SS7 stack interface.
	Disabling the flow control for the Mtp2Sap failed at the SS7 stack interface.
	Enabling the trace for the Mtp2Sap failed at the SS7 stack interface.
	Disabling the trace for the Mtp2Sap failed at the SS7 stack interface.
	Updating this Mtp2Sap failed at the SS7 stack interface.
10007	The description for this error ID can be one of the following:

Error ID	Description
	Mtp2LayerManager::readCurrentConfiguration() error when initializing the SS7 MTP2 Layer.
	Mtp2LayerManager::readCurrentConfiguration() NullPointerException when initializing the SS7 MTP2 Layer.
	Mtp2LayerManager::readCurrentConfiguration() IllegalOperationException when initializing the SS7 MTP2 Layer.
	Mtp2LayerManager::readCurrentConfiguration() TooManyInstancesException when initializing the SS7 MTP2 Layer.
	Mtp2LayerManager::readCurrentConfiguration() Unexpected Exception when initializing the SS7 MTP2 Layer.

Table 23: MTP3 Error Notifications

Error ID	Description
10006	The description for this error ID can be one of the following:
	CombinedLinkSet
	Reference of the linkset is NULL.
	Link
	Reference on the linkSetBelongingTo is NULL.
	Creation of the Link failed at the SS7 stack interface.
	Reference on the mtp2Sap is NULL.
	The protocol variant of the Mtp3TimerProfile shall be the same as the DPC assigned to this Link.
	Activation of the Link failed at the SS7 stack interface.
	Deactivation of the Link failed at the SS7 stack interface.
	Inhibition of the Link failed at the SS7 stack interface.
	Unhibition of the Link failed at the SS7 stack interface.
	Inition of Processor Outage for the Link failed at the SS7 stack interface.
	Inition of Processor Recovered for the Link failed at the SS7 stack interface.
	Enabling of trace generation for the Link failed at the SS7 stack interface.
	Disabling of trace generation for the Link failed at the SS7 stack interface.
	The Mtp2Sap protocol variant has to be the same type of the dpc assigned to this link.
	Updating the Mtp2Sap connection with this Link, failed at the SS7 stack interface.
	Reference on the timerProfile is NULL.

Error ID	Description
	Updating the Timer values for this Link, failed at the SS7 stack interface.
	Updating the Msg Priority for this Link, failed at the SS7 stack interface.
	Updating the CLink flag for this Link, failed at the SS7 stack interface.
	Updating the Max SLT try for this Link, failed at the SS7 stack interface.
	Updating the P1QLen for this Link, failed at the SS7 stack interface.
	Updating the P2QLen for this Link, failed at the SS7 stack interface.
	Updating the P3QLen for this Link, failed at the SS7 stack interface.
	Updating the discard priority for this Link, failed at the SS7 stack interface.
	Updating the Link Selection Code for the link test of this Link, failed at the SS7 stack interface.
	Updating the Test pattern of this Link, failed at the SS7 stack interface.
	Updating this Link failed at the SS7 stack interface.
	LinkSet
	One of the CombinedLinkset that this LinkSet belong to is NULL.
	Creation of the LinkSet failed at the SS7 stack interface.
	Activation of the LinkSet failed at the SS7 stack interface.
	Deactivation of the LinkSet failed at the SS7 stack interface.
	Reference of the link is NULL.
	Maximal Number of Link per Linkset has reach his limit.
	Update of this LinkSet failed at the SS7 stack interface.
	MTP3GenCfg
	Creation of the GenCfg failed at the SS7 stack interface.
	Reference of the timerProfile is NULL.
	Updating the Timers of this GenCfg, failed at the SS7 stack interface.
	Updating the Ssf valid Flag of this GenCfg, failed at the SS7 stack interface.
	Updating this GenCfg, failed at the SS7 stack interface.
	MTP3LayerManager
	Maximal Number of Mtp3TimerProfiles has been reached.
	Maximal Number of SignallingPoints has been reached.
	A signalling point already exist for this pointCode.
	Only one OwnSignallingPoints can be created.
	Reference on the cmbLinkSet is NULL.

Error ID	Description
	Reference on the dpc is NULL.
	A route cannot be of type UP for a Remote Signalling Point (DPC).
	A route cannot be of type DOWN for a Local Signalling Point (OPC).
	Maximal Number of Routes has been reached.
	This dpc cannot be assigned to this route, because it has already been asigned to another route.
	A Mtp3NSap cannot be created before an Own Signalling Point.
	Maximal Number of Mtp3NSaps has been reached.
	Reference on the adjDpc is NULL.
	Reference on the cmbLinkSetBelongingTo is NULL.
	A linkset cannot be created before an Own Signalling Point.
	Maximal Number of LinkSets has been reached.
	Maximal Number of Links has been reached.
	Maximal Number of Links per LinkSet has been reached.
	A CombinedLinkset cannot be created before an Own Signalling Point.
	Maximal Number of CombinedLinkSets has been reached.
	Only one Mtp3 Gen Config can be created.
	Mtp3TimerProfile cannot be deleted because there is either a Route, Link or Mtp3GenCfg referencing it. Delete first every entities referencing this Mtp3TimerProfile.
	Reference on the signallingPoint is NULL.
	SignallingPoint cannot be deleted because there is either a Link, LinkSet, Mtp3Route, SccpRoute, SccpAddress, ConcernedArea or SccpUSap referencing it. Delete first every entities referencing this SignallingPoint.
	Reference on the Route is NULL.
	Reference on the linkSet is NULL.
	LinkSet cannot be deleted because there is a Link belonging to it. Delete first every Links belonging to this LinkSet.
	Reference on the CombinedLinkSet is NULL.
	CombinedLinkSet cannot be deleted because there is LinkSets belonging to it. Delete first every LinkSets belonging to this CombinedLinkSet.
	CombinedLinkSet cannot be deleted because there is Mtp3Route referencing it. Delete first every Mtp3Route referencing this CombinedLinkSet.
	Reference on the link is NULL.

Error ID	Description
	Reference on the mtp3NSap is NULL.
	Mtp3NSap cannot be deleted because there is Routes associated with it. Delete first the Route.
	Reference on the ownSignallingPoint is NULL.
	OwnSignallingPoint (OPC) cannot be deleted.
	Enabling the alarm for the Mtp3 Layer failed at the SS7 stack interface.
	Disabling the alarm for the Mtp3 Layer failed at the SS7 stack interface.
	Enabling the debug print for the Mtp3 Layer failed at the SS7 stack interface.
	Disabling the debug print for the Mtp3 Layer failed at the SS7 stack interface.
	MTP3Nsap
	Creation of the Mtp3NSap resource failed at the SS7 stack interface.
	Activation of the Mtp3NSap failed at the SS7 stack interface.
	Deactivation of the Mtp3NSap failed at the SS7 stack interface.
	Reference of the signallingPoint to set is NULL.
	The SignallingPoint associated with a Mtp3NSap shall be an Own Signalling Point
	Updating the Own Signalling Point attached to this Mtp3NSap failed at the SS7 stack interface.
	Reference of the upperSap is NULL.
	Updating this Mtp3NSap failed at the SS7 stack interface.
	Route
	Creation of the Route failed at the SS7 stack interface.
	Reference of the timerProfile is NULL.
	The protocol variant of the timerProfile to set as to be the same as the DPC assigned to this Route.
	Updating the Timers of this Route, failed at the SS7 stack interface.
	Updating the Broadcast Flag of this Route, failed at the SS7 stack interface.
	Updating this Route, failed at the SS7 stack interface Reference of the mtp3NSap is NULL.
	SignallingPoint
	Invalid SignallingPointCode. Correct format (ANSI) is xxx.xxx.xxx where the maximum value can be 255.255.255.
	Invalid SignallingPointCode. Correct format (ITU) is x.xxx.x where the maximum value can be 7.255.7.
	Creation of the OwnSignallingPoint resource failed at the SS7 stack interface.

Error ID	Description
	Modification of the OwnSignallingPoint resource failed at the SS7 stack interface.
	For ITU, BICI & CHINA Networks, the MTP3 Restart Procedure shall be either RESTART_PROCEDURE_NO, RESTART_PROCEDURE_ITU88 or RESTART_PROCEDURE_ITU92.
	For ANSI Networks, the MTP3 Restart Procedure shall be either RESTART_PROCEDURE_NO, RESTART_PROCEDURE_ANS.
	For ITU International Networks, the Route Set Congestion Test shall be set to true.
	For ANS, ANS96 & CHINA Networks, the Route Set Congestion Test shall be set to true.
	The MTP3 Route Set Congestion Test can be set only for DPC.
	For ITU International Networks, the Multiple Congestion Priority shall be set to false.
	For ANS & ANS96 Networks, the Multiple Congestion Priority shall be set to true.
	The MTP3 Multiple Congestion Priority can be set only for DPC.
	For ITU Networks, the MTP3 Transfer Restrict Route Management is supported only for National Network, therefore should be set to false.
	The MTP3 Transfer Restrict Route Management can be set only for OPC.
	ConcernedArea
	Maximal Number of BackupPC per ConcernedArea has been reached.
	Maximal Number of ConcernedPC per ConcernedArea has been reached.
	The SSN maximum value is 255.
	Reference of the backupPC to add is NULL.
	This BackupPointCode has already be added to this ConcernedArea.
	Reference of the backupPC to remove is NULL.
	Reference of the concernedPC to add is NULL.
	Reference of the concernedPC to remove is NULL.
10007	The description for this error ID can be one of the following:
	Mtp3LayerManager::readCurrentConfiguration() error when initializing the SS7 MTP3 Layer.
	Mtp3LayerManager::readCurrentConfiguration() NullPointerException when initializing the SS7 MTP3 Layer.
	Mtp3LayerManager::readCurrentConfiguration() IllegalOperationException when initializing the SS7 MTP3 Layer.
	Mtp3LayerManager::readCurrentConfiguration() TooManyInstancesException when initializing the SS7 MTP3 Layer.

Error ID	Description
	Mtp3LayerManager::readCurrentConfiguration() Unexpected Exception when initializing the SS7 MTP3 Layer.

Table 24: SCCP Error Notifications

Error ID	Description
10006	The description for this error ID can be one of the following:
	SCCPGenCfg
	Creation of the GenCfg failed at the SS7 stack interface.
	Allowable range for Subsystem Out Of Service grant is from 1 to 10.
	Maximum number of Restriction Level is 8.
	Maximum number of Restriction Sub Level is 4.
	Allowable range for Connection Threshold is from 1 to 10.
	Allowable range for Queue Threshold is from 1 to 10.
	Updating the Management Status flag of this GenCfg, failed at the SS7 stack interface.
	Allowable range for Subsystem Out Of Service grant is from 1 to 10.
	Updating the SogThresh of this GenCfg, failed at the SS7 stack interface.
	Updating the MaxRstLvl of this GenCfg, failed at the SS7 stack interface.
	Updating the MaxRstSubLvl of this GenCfg, failed at the SS7 stack interface.
	Updating the conThresh of this GenCfg, failed at the SS7 stack interface.
	Updating the queThresh of this GenCfg, failed at the SS7 stack interface.
	Updating the itThresh of this GenCfg, failed at the SS7 stack interface.
	Reference of the timerProfile is NULL.
	Updating the timers value of this GenCfg, failed at the SS7 stack interface.
	SCCPLayerManager
	Maximal Number of Concerned Area has been reached.
	Maximal Number of GlobalTitle has been reached.
	A SccpRoute cannot be created before an SccpGenCfg object.
	Reference on the dpc is NULL.
	Reference on the sccpNSap is NULL.
	Maximal Number of SccpRoute has been reached.
	This dpc cannot be assigned to this route, because it has already been asigned to another route.

Error ID	Description
	A SccpNSap cannot be created before a SccpGenCfg object.
	Reference on the mtp3NSap is NULL.
	Maximal Number of SccpNSap has been reached.
	A SccpUSap cannot be created before an SccpGenCfg object.
	Maximal Number of SccpUSap has been reached.
	Maximal Number of SccpTimerProfiles has been reached.
	Reference on the globalTitle is NULL.
	Reference on the action is NULL.
	Reference on the sccpAddress is NULL.
	When the Routing Indicator is 'route base on GT', the reference on the globalTitle cannot be NULL.
	When the Routing Indicator is 'route base on PC_SSN', the reference on the Signalling Point Code cannot be NULL.
	Maximal Number of SccpAddress has been reached.
	Reference on the rule is NULL.
	Maximal Number of Actions per Association has been reached.
	Only one Sccp Gen Config can be created
	Reference on the ConcernedArea is NULL.
	Reference on the GT is NULL.
	GlobalTitleEntry cannot be deleted because there is a SccpAddress dependency with it. Delete first all the entities that have dependency on that GlobalTitleEntry.
	Reference on the sccpRoute is NULL.
	SccpRoute cannot be deleted because there is ConcernedAreas associated with it. Delete first all the entities that have dependency on that entity.
	Reference on the sccpNSap is NULL.
	SccpNSap cannot be deleted because there is either a SccpUSap or SccpRoute associated with it. Delete first all the entities that have dependency on that entity.
	Reference on the sccpUSap is NULL.
	Reference on the timerProfile is NULL.
	SccpTimerProfile cannot be deleted because there is either a SccpNSap or SccpGenCfg associated with it. Delete first every entities that have dependency with this SccpTimerProfile.
	Reference on the rule is NULL.
	Reference on the action is NULL.

Error ID	Description
	Reference on the association is NULL.
	Reference on the addressMap is NULL.
	Reference on the sccpAddress is NULL.
	Disabling all the SccpUSaps failed at the SS7 stack interface.
	Enabling the alarm for the Sccp Layer failed at the SS7 stack interface.
	Disabling the alarm for the Sccp Layer failed at the SS7 stack interface.
	Enabling the debug print for the Sccp Layer failed at the SS7 stack interface.
	Disabling the debug print for the Sccp Layer failed at the SS7 stack interface.
	Enabling the auditing of connection state for the Sccp Layer failed at the SS7 stack interface.
	Disabling the audit of connection state for the Sccp Layer failed at the SS7 stack interface.
	SCCPNSap
	Creation of the NSAP failed at the SS7 stack interface.
	Maximal Number of Sio Priorities has been reached.
	Allowable range for Connection Threshold is from 1 to 10.
	The MessageLength maximum value is 272.
	Activation of the NSAP failed at the SS7 stack interface.
	Deactivation of the NSap failed at the SS7 stack interface.
	Enabling of trace generation for the SccpNSap failed at the SS7 stack interface.
	Disabling of trace generation for the SccpNSap failed at the SS7 stack interface.
	Updating the Max Length Msg delivered to the Mtp3NSap , failed at the SS7 stack interface.
	Reference of the sccpTimerProfile to set is NULL.
	The protocol variant of the timerProfile to set has to be the same as this NSAP.
	Updating the timers of this SccpNSap, failed at the SS7 stack interface.
	Allowable range for Connection Threshold is from 1 to 10.
	Updating the hopCount of this SccpNSap, failed at the SS7 stack interface.
	Updating the sio priority presence flag of this SccpNSap, failed at the SS7 stack interface.
	Updating the sio priorities of this SccpNSap, failed at the SS7 stack interface.
	Updating this SccpNSap failed at the SS7 stack interface.
	SCCPRoute

Error ID	Description
	Creation of the SccpRoute failed at the SS7 stack interface.
	Maximal Number of BackupPC per Route has been overpass.
	Maximal Number of ConcernedAreas per Route has been overpass.
	Updating the status of this Route, failed at the SS7 stack interface.
	Updating the ReplicatedMode of this Route, failed at the SS7 stack interface.
	For ITU88,ITU92,ANS88,ANS92 and ANS96 Route Network Type, the support shall be set to ROUTE_NW_NARROWBAND.
	Updating the SccpPeerNetworkSupport of this Route, failed at the SS7 stack interface.
	Reference of the backupPC to add is NULL.
	Maximal Number of BackupPC per Route has been reached.
	This BackupPointCode has already be added to this SccpRoute.
	Updating the BackupPc list of this Route, failed at the SS7 stack interface.
	Reference of the backupPC to remove is NULL.
	Reference of the concernedArea to add is NULL.
	Maximal Number of ConcernedAreas per Route has been reached.
	Updating the ConcernedArea list of this Route, failed at the SS7 stack interface.
	Reference of the concernedArea to remove is NULL.
	Removing the concernedArea failed at the SS7 stack interface.
	Updating this SccpRoute failed at the SS7 stack interface.
	SCCPUSap
	Creation of the USAP failed at the SS7 stack interface.
	Maximal Number of Concerned Point Code per USAP has been overpass.
	Creation of the USAP failed at the SS7 stack interface.
	Activation of the USAP failed at the SS7 stack interface.
	Deactivation of the USap failed at the SS7 stack interface.
	Reference of the concernedPC to add is NULL.
	This ConcernedPointCode has already be added to this USAP.
	Updating the concerned points code of this USAP, failed at the SS7 stack interface.
	Reference of the concernedPc to remove is NULL.
	Reference of the TcapSap to set is NULL.
10007	The description for this error ID can be one of the following:

Error ID	Description
	SccpLayerManager::readCurrentConfiguration() error when initializing the SS7 SCCP Layer.
	SccpLayerManager::readCurrentConfiguration() NullPointerException when initializing the SS7 SCCP Layer.
	SccpLayerManager::readCurrentConfiguration() IllegalOperationException when initializing the SS7 SCCP Layer.
	SccpLayerManager::readCurrentConfiguration() TooManyInstancesException when initializing the SS7 SCCP Layer.
	SccpLayerManager::readCurrentConfiguration() Unexpected Exception when initializing the SS7 SCCP Layer.

Table 25: TCAP Error Notifications

Error ID	Description
10006	The description for this error ID can be one of the following:
	TCAPLayerManager
	Maximal Number of TcapTimerProfiles has been reached.
	Maximal Number of TcapSaps has been reached.
	Reference of the TcapTimerProfile to delete is NULL.
	TcapTimerProfile cannot be deleted because there is a TcapSap referencing it. Delete first every entities referencing this TcapTimerProfile.
	Reference of the TcapSap to delete is NULL.
	Enabling all the TcapSaps failed at the SS7 stack interface.
	Disabling all the TcapSaps failed at the SS7 stack interface.
	Enabling the alarm for the Tcap Layer failed at the SS7 stack interface.
	Disabling the alarm for the Tcap Layer failed at the SS7 stack interface.
	Enabling the debug print for the Tcap Layer failed at the SS7 stack interface.
	Disabling the debug print for the Tcap Layer failed at the SS7 stack interface.
	Enabling the tracing for the Tcap Layer failed at the SS7 stack interface.
	Disabling the tracing for the Tcap Layer failed at the SS7 stack interface.
	TCAPSap
	Creation of the TcapSap resource failed at the SS7 stack interface.
	Activation of the TcapSap failed at the SS7 stack interface.
	Deleting all the unused dialogues of the TcapSap failed at the SS7 stack interface.
	Deleting all the unused invokes of the TcapSap failed at the SS7 stack interface.

Error ID	Description
	Reference of the TcapTimerProfile to set is NULL.
	Modification of the TcapSap failed at the SS7 stack interface.
	Updating this TcapSap failed at the SS7 stack interface.
10007	The description for this error ID can be one of the following:
	TcapLayerManager::readCurrentConfiguration() error when initializing the SS7 TCAP Layer.
	TcapLayerManager::readCurrentConfiguration() NullPointerException when initializing the SS7 TCAP Layer.
	TcapLayerManager::readCurrentConfiguration() IllegalOperationException when initializing the SS7 TCAP Layer.
	TcapLayerManager::readCurrentConfiguration() TooManyInstancesException when initializing the SS7 TCAP Layer.
	TcapLayerManager::readCurrentConfiguration() Unexpected Exception when initializing the SS7 SCCP Layer.

SIP Error Notifications

SIP Provisioning Error Notifications

Table 26: SIP Provisioning Error Notifications

ID	Notification Name	Description
15000	**DatabaseError**	Internal Database error.
15001	**LimitOverflow**	Modify multiple records with password not supported
15002	**MaxAorsPerProfile**	Maximum number of AORs for this subscriber has been reached.
15003	**InvalidIpAddress**	Invalid host name - bad IP address.
15004	**InvalidPort**	Invalid port.
15005	**InvalidUsernamePassword**	Invalid provided username and password.
15006	**InvalidUsernamePasswordDb**	Invalid provided username and password in the DB.
15007	**InvalidUsername**	Invalid provided username.

ID	Notification Name	Description
15008	**InvalidPassword**	Invalid provided password.
15009	**InvalidUsernameDb**	Invalid username in the DB.
15010	**InvalidPasswordDb**	Invalid password in the DB.
15011	**InvalidCriteria**	Invalid criteria.
15012	**DeleteOperationForbidden**	Delete operation not allowed in this context.
15013	**InvalidUser**	Invalid user.
15014	**InvalidService**	Service not allowed in this context.
15015	**RegBindingCleanupFailure**	The registration binding could not be deleted.
15016	**ModifyOperationForbidden**	Modify operation not allowed in this context.
15017	**InvalidHost**	Invalid Host.
15018	**AddOperationForbidden**	Add operation not allowed in this context.
15019	**MultipleRecordsDeletion Forbidden**	Multiple records deletion not supported.
15020	**MultipleRecordsUpdateForbidden**	Multiple records update not supported.
15021	**InitializationFailed**	SipProvisioningManager failed initialization.
15022	**InvalidDirectoryNumber**	Invalid Directory number provided.
15025	**SipMaxNumberSubsLicense Violation**	Rejection: The maximum number of SIP subscribers authorized by the license is reached!
15026	**RedirectOverrideProvLimit Reached**	Already at the maximum limit of Redirect Override URI for this AOR.
15027	**RedirectOverrideMultipleI nsertForbidden**	Insert Request received contains more attributes than expected…
15028	**RedirectOverrideInvalid CanonicalUri**	Invalid Canonical URI provided.
15029	**MultipleAorRecordsDeletion WithDifferentSubscription IDForbidden**	Multiple AOR records deletion with different subscription IDs is forbidden.
15030	**SipInvalidCriteria**	SubscriptionID is a mandatory deletion criteria.
15031	**MultipleSipTlsCertPrivKey NotAllowed**	Multiple SIP TLS certificates and private keys not allowed

ID	Notification Name	Description
15032	**TlsInvalidAttribute**	Attempt to insert/modify SIP TLS attribute not allowed
15033	**InvalidTlsCertificate**	Invalid SIP TLS certificate
15034	**InvalidTlsPrivateKey**	Invalid SIP TLS private key
15035	**MandatoryTlsAttributeMissing**	Mandatory SIP TLS attribute is missing
15036	**NullReceivedFromXDS**	Provisioning request received from XDS manager contains a NULL pointer
15037	**InvalidProvRequestReceived**	Provisioning request received from XDS manager is Invalid.
15038	**AorDomainNameNotFound**	AorDomainName NOT found for AorDomainId %1
15039	**MandatoryAorDomainParameter Missing**	Mandatory AorDomain parameter missing
15040	**QvalueOutOfRange**	Qvalue out of 0[.000] - 1[.000] range
15041	**InvalidNpAorUserRangePrefix**	Invalid Prefix received for feature NP AOR user range.
15042	**InvalidNpAorUserRangeContact**	Invalid Contact received for feature NP AOR user range.
15043	**InvalidNpAorUserRangeRuleId**	Invalid RuleId received for feature NP AOR user range.
15044	**InvalidNpAorUserRangeIsMNPRule**	Invalid MNP Routing Config received for feature NP AOR user range.
15045	**InvalidUpdateNpAorUserRange IsMNPUsed**	NP AOR user range parameter 'isMNPRoutingRuleUsed' cannot be updated for an existing prefix.
15046	**TasIdCannotBeDeleted**	TasId %1 cannot be deleted.
15047	**TasGtMandatoryParameterMissing**	SIP TAS GT mandatory parameter missing.
15048	**GtInvalid**	SIP TAS Gt parameter is invalid, valid digits: 0-9, a-e, A-E.
15049	**TasFqdnInvalid**	SIP TAS FQDN parameter is invalid
15050	**RegistrationBindingCleanup TimeOutOfRange**	Value out of HH:MM range.
15051	**RejectOperationReferenced Instance**	Operation not allowed - reference restriction.

ID	Notification Name	Description
15052	DnPropagationError	Cannot propagate DirectoryNumber [%1] from AddressOfRecord to RegistrationBinding.
15053	TasIdCannotBeUpdated	Cannot update the TasId, TasFqdn and Gt of TasId 0.
15054	MandatoryParameterMissing	%1 mandatory parameter missing.
15055	PrefixInvalid	SIP TAS Prefix parameter is invalid, valid digits: 0-9, a-e, A-E
15056	InvalidDefaultImsiLength	Invalid IMSI - Incorrect number of digits, IMSI must be 5 to 15 digits.

SIP Server Errors

Table 27: SIP Server Error Notifications

ID	Notification Name	Description
8000	StackServerConstructorFailed	Radvision error code is %1.
8001	StackServerDestructorFailed	Radvision error code is %1.
8002	StackPolicyMgrRegCallbackFailed	Radvision error code is %1.
8003	StackProxyMgrRegCallbackFailed	Radvision error code is %1.
8004	StackRegistrarMgrRegCallback Failed	Radvision error code is %1.
8005	StackPolicyMgrDeregCallback Failed	Radvision error code is %1.
8006	StackProxyMgrDeregCallback Failed	Radvision error code is %1.
8007	StackRegistrarMgrDeregCallback Failed	Radvision error code is %1.
8008	ApplicationPoolConstructor Failed	Radvision error code is %1.
8009	GettingApplicationPoolFailed	Radvision error code is %1.
8010	GettingApplicationPoolPage Failed	Radvision error code is %1.
8011	AcceptUnknownValidMessage Failed	Radvision error code is %1.

ID	Notification Name	Description
8012	**RejectUnknownInvalidMessage Failed**	Radvision error code is %1.
8013	**StoreConstructorFailed**	Dataprovider error code is %1.
8014	**LocationDatabaseUpdateFailed**	Radvision error code is %1 and Dataprovider error code is %2.
8015	**LocationDatabaseLookupFailed**	Radvision error code is %1.
8016	**LocationDatabaseSelect RegistrationBindingFailed**	Dataprovider error code is %1.
8017	**LocationDatabaseConvert RegistrationBindingFailed**	Radvision error code is %1.
8018	**AcceptValidRegistrationFailed**	Radvision error code is %1.
8019	**LocationDatabaseRemoveFailed**	Radvision error code is %1 and Dataprovider error code is %2.
8020	**LocationDatabaseDeleteExpired RegistrationFailed**	Dataprovider error code is %1.
8021	**RejectInvalidRegistrationFailed**	Radvision error code is %1.
8022	**ConfigurationConstructorFailed**	Dataprovider error code is %1.
8023	**InitializationFailed**	N/A
8024	**InmConnectionFailed**	Connection error code is %1.
8025	**AcceptOptionsRequestFailed**	Radvision error code is %1.
8026	**RejectOptionsRequestFailed**	Radvision error code is %1.
8027	**RejectUnknownValidMessageFailed**	Radvision error code is %1.
8028	**OperationFailure**	The operation failed.
8029	**IneffectiveTraceParameters**	The operation is ineffective with the current parameters.
8031	**StackActivationFailure**	SIP stack activation failure.
8032	**RedirectError**	Sip redirect error - Radvision error code: %1 for AOR: %2.
8033	**RedirectAddRegBindingError**	Sip redirect error - Radvision error code: %1 for AOR: %2.
8035	**FatalErrorFailModule**	Fatal Error Occurred: Module failure on ERROR: %1.

ID	Notification Name	Description
8036	DbMgrInitFailure	Cannot initialize Dbmgr.
8037	RvActiveObjInitFailure	Cannot initialize RvActiveObj.
8038	RequestManagerInitFailure	Cannot initialize SipRequestManager.
8039	AuthenticationFailure	Register authentication failure: RV error code: %1
8040	InviteMapCleanup	InviteMap - items deleted: %1
8041	ErrorNotInActiveState	Request discarded. SipServer not in active state.
8047	RadvisionError	Radvision error code [%1].
8048	DbError	DB error code [%1].
8049	LoadBalancingProxyError	Load Balancing Proxy Error: %1
8050	RedirectOverrideError	Redirect Override Error: %1
8051	RedirectOverrideParseUriError	Redirect Override : Could not parse contact URI : %1 for AOR : %2
8052	RedirectOverrideAddUriError	Redirect Override : Radvision error : %1 receive while adding Contact URI for AOR : %2
8053	RegClientNotEnabled	Request discarded. RegClient (SipUa) not in active state.
8054	InvalidSlotId	Request discarded. Invalid SlotId.
8055	TlsError	Unable to start the RV TLS engine.
8056	RedirectNpAorUserRangePrefix AddUriError	Redirect NP : Radvision error : %1 receive while adding NP AOR User Range Prefix Contact URI for AOR : %2

SIP User Agent Errors

Table 28: SIP User Agent Error Notifications

ID	Notification Name	Description
18000	StackUaConstructorFailed	Radvision constructor failed with error code: %1
18001	StackUaDestructorFailed	Radvision destructor failed with error code: %1

ID	Notification Name	Description
18005	**SendFirstRegisterError**	Send first register request failed for AOR %1.
18006	**SendRegisterRefreshError**	Send register refresh request failed for AOR %1.
18007	**FirstRegisterFailed**	First register failed for AOR %1, SIP error code %2.
18008	**RegisterRefreshFailed**	Register refresh failed for AOR %1, SIP error code %2.
18009	**GsmContactError**	No GSM contact provisioned.
18010	**DbError**	DataProvider error %1.
18011	**ConfigurationConstructorFailed**	SIPUA configuration constructor failed with error: %1
18012	**NoProvisionedAorForImsi**	No provisioned AOR for IMSI %1.
18013	**InvalidContactError**	Invalid Contact provisioned: %1
18014	**InitializationFailed**	Initialization failed.
18015	**ActivationFailed**	Activation failed.
18016	**RegFailureNotificationError**	Error %1 on notification to HLR of SIP registration failure for IMSI %2.
18017	**ErrorNotInActiveState**	Request discarded. Not in active state.
18018	**ErrorRequestNotSupported**	Request not supported.
18019	**ErrorProcessingLocationUpdate**	Error %1 processing location update for IMSI %2.
18020	**OperationFailure**	The operation failed.
18021	**IneffectiveTraceParameters**	The operation is ineffective with the current parameters.
18024	**FatalErrorFailModule**	Fatal Error Occurred: Fail module on ERROR: %1.
18027	**AorDomainNotFound**	AorDomainName for AorDomainId [%1] not found.

IMS-HSS/LTE-HSS Error Notifications

The following tables provide a list and a description of the error notifications that can be generated for the IMS-HSS and for the LTE-HSS.

HSS Provisioning Notifications for IMS-HSS and LTE-HSS

Table 29: HSS Provisioning Error Notifications For The IMS-HSS And The LTE-HSS

ID	Notification Name	Description
16001	**InvalidEntity**	HssProvManager received a request for an invalid entity.
16002	**InvalidTransactionOrContext**	HssProvManager received a invalid transaction or invalid context.
16003	**SystemFailsToProcessRequest**	HssProvManager fails to process the request.
16024	**InvalidAttribute**	Fails to process the request due to invalid attribute.
16025	**InvalidFQDN**	Fails to process the request due to invalid FQDN.
16026	**InvalidDiameterIdent**	Fails to process the request due to invalid Diameter ID.
16027	**InvalidTCPPort**	Fails to process the request due to invalid TCP Port.
16028	**InvalidSCTPPort**	Fails to process the request due to invalid SCTP Port.
16049	**ConfigUpdateWhileHssRunning**	Configuration changes not allowed while HSS Service is running.
16051	**TcpOrSctpMustBeEnabled**	Either TCP or SCTP must be enabled for this feature.
16052	**TwoServicesSameLocalFQDN**	Two IMS/LTE services cannot have the same local FQDN.
16071	**VipBindingError**	Unable to bind the virtual IP.
16143	**InvalidTimeFormat**	Invalid time format. (YYYY-MM-DD hh:mm:ss)

HSS Provisioning Notifications for IMS-HSS only

Table 30: HSS Provisioning Error Notifications Only For The IMS-HSS

ID	Notification Name	Description
16004	**InvalidPrimaryCharging CollectionFunction**	Fails to process the request due to invalid primary charging collection function.
16005	**InvalidSecondaryCharging CollectionFunction**	Fails to process the request due to invalid secondary charging collection function.
16006	**InvalidPrimaryEvent ChargingFunction**	Fails to process the request due to invalid primary event charging function.
16007	**InvalidSecondaryEvent ChargingFunction**	Fails to process the request due to invalid secondary event charging function.
16008	**InvalidServerName**	Fails to process the request due to invalid server name.
16009	**InvalidPrivateIdentity**	Fails to process the request due to invalid private identity.
16010	**InvalidPublicIdentity**	Fails to process the request due to invalid public identity.
16011	**InvalidASName**	Fails to process the request due to invalid AS-name.
16012	**InvalidSipMethod**	Fails to process the request due to invalid sip method.
16013	**InvalidGroupList**	Fails to process the request due to invalid group list.
16014	**InvalidVisitedNetwIdentifier**	Fails to process the request due to invalid visited network identifier.
16015	**MissingChargingId**	Fails to process the request due to missing chargingId
16016	**MissingScscfCapabilitiesId**	Fails to process the request due to missing ScscfCapabilitiesId
16017	**MissingServiceProfileId**	Fails to process the request due to missing ServiceProfileId
16018	**MissingPublicIdentity**	Fails to process the request due to missing PublicIdentity.
16019	**MissingPrivateIdentity**	Fails to process the request due to missing PrivateIdentity.

ID	Notification Name	Description
16020	**MissingImsSubscriptionId**	Fails to process the request due to ImsSubscriptionId
16021	**MissingInitialFilterCriteriaId**	Fails to process the request due to missing InitialFilterCriteriaId
16022	**MissingServicePointTriggerId**	Fails to process the request due to missing ServicePointTriggerId
16023	**MissingRoamingProfileId**	Fails to process the request due to missing RoamingProfileId
16029	**InvalidLocalRealm**	Fails to process the request due to invalid Local Realm.
16030	**InvalidAssociationOfPrivate IdAndImplicitRegistrationSet**	Fails to process the request due to invalid association of privateId-and-ImplicitRegistrationSet.
16031	**HssConfigDeletionNotAllowed**	Deletion from HssConfig table not allowed.
16032	**SCTPAddressTableModNotAllowed**	SCTP address data exists; modification not allowed.
16033	**TCPAddressTableModNotAllowed**	TCP address data exists; modification not allowed
16034	**InvalidCryptedSecretKey**	Fails to process the request due to invalid CryptedSecretKey.
16035	**InvalidServicePointTriggerId**	Fails to process the request due to Invalid ServicePointTriggerId.
16036	**InvalidDataReference**	Fails to process the request due to invalid DataReference.
16037	**InvalidPermissionList**	Fails to process the request due to invalid PermissionList.
16038	**InvalidServicePointTriggerId**	Fails to process the request due to Invalid ServicePointTriggerId.
16039	**MissingServiceTemplate ProfileId**	Fails to process the request due to missing ServiceTemplateProfileId
16040	**MissingServiceTemplate InitialFilterCriteriaId**	Fails to process the request due to missing ServiceTemplateInitialFilterCriteriaId
16041	**MissingServiceTemplate PointTriggerId**	Fails to process the request due to missing ServiceTemplatePointTriggerId

ID	Notification Name	Description
16042	**InvalidHssName**	Fails to process the request due to invalid HSS Name
16043	**MissingAuthAucName**	Missing AuthSchema or AlgoName value
16044	**AuthSchemaNotProvisioned**	AuthSchema is not provisioned
16045	**AuthSchemaCannotBeAdded**	Adding a new AuthSchema is forbidden
16046	**AuthSchemaCannotBeDeleted**	Removing an AuthSchema is forbidden.
16047	**AuthSchemaCannotBeModified**	Modifying an AuthSchema is forbidden.
16048	**SharedIfcLinkedToSP**	Cannot delete a Shared IFC that is linked to a Service Profile.
16050	**HssOrSlfMustBeEnabled**	Either HSS or SLF must be enabled on this slot.
16053	**TwoServicesSameLocalTCPPort**	Two IMS/LTE services cannot have the same local TCP Port.
16054	**TwoServicesSameLocalSCTPPort**	Two IMS/LTE services cannot have the same local SCTP Port.
16072	**HssMissingContactAddress**	When a Private Identity is administratively registered, a contact address SIP URI is mandatory.
16073	**HssEmptyARattributes**	Administrative registration requires non-empty Administrative CSCF in IMS subscription and non-empty contact address in private identity.
16078	**MissingSharedIfcId**	Fails to process the request due to missing SharedSetIfcID.
16079	**HssARPrivateIdentityExists**	Cannot update: at least one administratively registered private identity exists.
16083	**IncompatibleTrafficPriority**	Traffic Priority should not be set for this Schedule Type value.
16084	**MandatoryTrafficPriority**	Traffic Priority should be set for this Schedule Type value.
16085	**IncompatibleMaximumSustained TrafficRate**	Maximum sustained traffic rate should not be set for this Schedule Type value.
16086	**MandatoryMaximumSustained TrafficRate**	Maximum sustained traffic rate should be set for this Schedule Type value.

ID	Notification Name	Description
16087	**IncompatibleMinimum ReservedTrafficRate**	Minimum Reserved Traffic Rate should not be set for this Schedule Type value.
16088	**MandatoryMinimumReserved TrafficRate**	Minimum Reserved Traffic Rate should be set for this Schedule Type value.
16089	**IncompatibleMaximum TrafficBurst**	Maximum Traffic burst should not be set for this Schedule Type value.
16090	**IncompatibleToleratedJitter**	Tolerated jitter should not be set for this Schedule Type value.
16091	**IncompatibleMaximumLatency**	Maximum latency should not be set for this Schedule Type value.
16092	**MandatoryMaximumLatency**	Maximum latency should be set for this Schedule Type value.
16093	**IncompatibleUnsolicited GrantInterval**	Unsolicited Grant Interval should not be set for this Schedule Type value.
16094	**MandatoryUnsolicited GrantInterval**	Unsolicited Grant Interval should be set for this Schedule Type value.
16095	**IncompatibleSDUSize**	SDU Size should not be set for this Schedule Type value.
16096	**IncompatibleUnsolicited PollingInterval**	Unsolicited Polling Interval should not be set for this Schedule Type value.
16097	**MandatoryUnsolicited PollingInterval**	Unsolicited Polling Interval should be set for this Schedule Type value.
16098	**OutOfRangeScheduleType**	Schedule Type is out of range.
16104	**AllAttributesAreMandatory**	All attributes are mandatory: missing attribute.
16105	**ObjectAlreadyExists**	Possible internal or provisioning error: an Object with the same key attributes already exists.
16106	**InvalidIPAddress**	Cannot parse provided parameter to valid IP address.
16107	**UnableToFindOBject**	Possible internal or provisioning error: unable to find object.
16115	**BadPskPasswdFormat**	PSK Password must be in Hexadecimal format.
16116	**ProvBadPskC0Format**	C0 value must be in Hexadecimal format.

ID	Notification Name	Description
16126	**SystemFailsToReadFileOr Directory**	Unable to read or access file or directory.
16127	**FailsToParsePEMFile**	Unable to parse PEM-formatted file: please check content.
16128	**TooManyPkeys**	At most one DSA and one RAS private keys can be provisioned.
16131	**HssMaxNumberSubsLicense Violation**	Rejection: The maximum number of HSS subscribers authorized by the license is reached!
16134	**SlfMaxNumberSubsLicense Violation**	Rejection: The maximum number of SLF subscribers authorized by the license is reached!
16139	**SLFEntriesPerSubAtLimit**	Already at the maximum limit of SLF entries for this subscription.
16140	**IfcWithSameTagHasDifferent AsName**	All IFC's associated with this DSAI Tag must have the same AS Name.
16141	**AnotherIfcHasSameDsaiTag**	Another IFC linked with this IFC's DSAI Tag; AS Name change disallowed.
16144	**DeleteServProfWithPublicID**	Cannot delete Service Profile associated with an existing Public Identity.
16300	**DNSMissingMandatoryParam**	DNS Listen Address, DNS Port and DNS Netmask are mandatory.
16301	**DNSMaxListenAddrReached**	DNS Max number of Listen Address has been reached (max is 2).
16302	**DNSUnexpectedInternalError**	DNS unexpected internal error when processing the request.
16303	**DNSInvalidIpPort**	DNS invalid listen port number.
16304	**DNSListenAddressAlreadyAAA**	The DNS Listen Address is already configured as a AAA Listen Address.
16305	**DNSDefaultDomainName AlreadyDefined**	A default DNS Enum Domain Name has already been defined.
16306	**DNSEnumUsersPerSubAtLimit**	Already at the maximum limit of Enum Users for this subscription.
16307	**DNSInvalidEnumUserId**	Invalid EnumUserId.
16308	**DNSNoDomainNameId**	No DomainNameId provided, and no default value found in the Domain Name List.
16309	**DNSRemovingPlusGivesDuplicate**	Removing the leading '+' results in a duplicate EnumUserId.

ID	Notification Name	Description
16310	DNSNoDomainIdCriteria	EnumDomainNameId must be provided as criteria for this command.
16311	DNSMissingDNAttributes	Both EnumDomainName and DefaultEnumDomainName attributes must be provided for this command.
16312	DNSNoDomainNameCriteria	EnumDomainName must be provided as criteria for this command.
16313	DNSNoEnumUserTemplateId	DNSEnumUserTemplateId must be provided as criteria for this command.
16314	DNSNoUserIdDomainIdCriteria	Both EnumUserId and EnumDomainNameId must be provided as criteria for this command.
16315	DNSInvalidEnumUserTemplateId	EnumUserTemplateId must be an integer greater than zero.
16316	DNSTemplateNotValid	EnumUserTemplateId is not provisioned in EnumUserTemplate.
16317	DNSTemplateNotProvisioned	All DNSEnumUser fields must be provisioned if DNSEnumUserTemplateId is not provided.
16318	DNSTemplateInUse	The template with this EnumUserTemplateId is referenced by Enum Users.
16319	DNSInvalidEnumDomainNameId	EnumDomainNameId is not provisioned in DNSDomainNameList.
16320	DNSInvalidAttributeValue	Invalid Attribute value provided in this command.
16321	DNSRegExpMandatory	NAPTR RegExp is missing. Field is mandatory.
16322	DNSInvalidEnumName	Invalid EnumName.
16323	DNSInvalidEnumRange	Invalid EnumRange.

LTE Provisioning Notifications

Table 31: LTE Provisioning Error Notifications

ID	Notification Name	Description
17300	OneLteFeatureMustBeEnabled	Feature cannot be disabled: at least one feature has to be enabled, LTE HSS and/or EIR per slot.-

ID	Notification Name	Description
17301	TwoServicesSameLocalFQDN	Two LTE/IMS services cannot have the same local FQDN.
17302	TwoServicesSameLocalTCPPort	Two LTE/IMS services cannot have the same local TCP Port.
17303	TwoServicesSameLocalSCTPPort	Two LTE/IMS services cannot have the same local SCTP Port.
17304	InvalidFQDN	Fails to process the request due to invalid FQDN.
17305	InvalidAttribute	Invalid attribute.
17306	InvalidDiameterIdent	Fails to process the request due to invalid Diameter ID.
17307	SystemFailsToProcessRequest	LTE Prov Manager cannot process request.
17308	InvalidTimeFormat	Invalid time format. (YYYY-MM-DD hh:mm:ss)
17309	InvalidTCPPort	Fails to process the request due to invalid TCP Port.
17310	InvalidSCTPPort	Fails to process the request due to invalid SCTP Port.
17311	ConfigUpdateWhileLteRunning	Configuration changes not allowed while LTE Service is running.
17312	TcpOrSctpMustBeEnabled	Either TCP or SCTP must be enabled for this feature.
17313	LteImsSameLocalFQDN	LTE HSS/EIR cannot have the same local FQDN as IMS HSS/SLF.
17314	VipBindingError	Unable to bind the virtual IP.
17315	InvalidEntity	LteProvManager received a request for an invalid entity.
17316	CannotDeleteDefaultPDNContext	The default PDN context cannot be deleted.
17317	InvalidPDNContextIdentifier	PDNContextIdentifier can't have a value of zero.

AAA Error Notifications

The following table provides a list and a description of the error notifications for the AAA 3000. Since the AAA functionalities are integrated in the HSS process, the AAA Error Notifications are generated by the HssProvisioningMgr process.

Table 32: AAA Error Notifications Generated By The HSS Provisioning Manager

ID	Notification Name	Description
16055	**AAAConfigCannotBeModified**	Modifying AAA Config is not allowed. Configuration is static.
16056	**AAAModificationNotAllowed**	Modification is not allowed for that entity. Please delete and create another one.
16057	**AAAUnexpectedExpectedError**	Unexpected error raised in AAA server. Please check log file.
16058	**AAAMissingNAS**	Missing NAS Name parameter.
16059	**AAAMissingAccountingServer**	Missing Remote Accounting Server IP Address.
16060	**AAAMissingAccountingPort**	Missing Remote Accounting Server Port.
16061	**AAAMissingSharedSecret**	Missing Shared Secret Key.
16062	**AAAMissingAAAAcctPort**	Missing AAA Accounting port.
16063	**AAAMissingAAAAcctIP**	Missing AAA Accounting IP address
16064	**AAAMissingAAAListPort**	Missing AAA Listening port.
16065	**AAAMissingAAAListenIP**	Missing AAA Listening IP address.
16066	**AAAOverlapInAddressRange**	Overlap in AAA IP Address range.
16067	**AAAErrorInIPAddressForma**	Error in IP Address Format.
16068	**AAAMissingUserName**	Missing User Name.
16069	**AAAInvalidIPAddressRange**	Invalid IP AddressRange.
16070	**AAAMaxInstanceConnection Reached**	Max Instance Connection Reached per AAA Instance. Cannot configure new NAS for new AAA Listen Address.
16074	**AAAListenIpPortMismatch**	All AAA Listen Ports must have the same value for this AAA Listen IP Address.

ID	Notification Name	Description
16075	**AAANasIpPortConflict**	All NAS ports for a NAS IP Address must have distinct non-default values.
16076	**AAAPrimarySystemAcctServer Exists**	A primary system accounting server already exists.
16077	**AAAPrimaryNasAcctServerExists**	A primary accounting server already exists for this NAS.
16080	**AAANoSuchAddressPool**	Specified address pool name not found.
16099	**AAAMissingAddrPoolParam**	Address Pool Parameter Missing.
16100	**AAAMissingCalledStnParam**	Called Station Parameter Missing.
16101	**AAAMissingParameter**	Operation Parameter Missing.
16102	**AAANoAddressesAvailable**	No Addresses Available In Specified Address Pool.
16103	**AAAAddressAlreadyAssigned ForUser**	IP Address Already Assigned For User and Called Station.
16117	**AAAMissingAuthenticationServer**	Missing Remote Authentication Server IP Address.
16118	**AAAMissingAuthenticationPort**	Missing Remote Authentication Server Port.
16119	**AAAMissingAssociationType**	Association Type Parameter Missing.
16120	**AAAMissingIsRealm**	IsRealm Parameter Missing.
16121	**AAAMissingRealmOrCalledStn**	Realm Or Called Station Parameter Missing.
16122	**AAANoStaticIPAvailable**	Cannot allocate static IP: no available IP in pool.
16123	**AAAStaticIPAddressNotFound**	User has no associated static IP address.
16124	**AAAMissingNASId**	Missing NAS Identifier parameter.
16125	**AAANASEarlyIMSConf**	When configuring an Early-IMS APN, IMPI Selection and Failure Action must not be empty.
16137	**AaaMaxNumberSubsLicense Violation**	Rejection: The maximum number of AAA subscribers authorized by the license is reached!
16138	**AAAListenAddressAlreadyDNS**	The AAA Listen Address is already configured as a DNS Listen Address.

ID	Notification Name	Description
16142	AAAAddressUsageDataForWrongType	Can only compute address usage data for type ADDRESS_POOL.
16143	InvalidTimeFormat	Invalid time format. (YYY-MM-DD hh:mm:ss)

EIR Provisioning Notifications

The following is a list of the Equipment Identity Register (EIR) provisioning notifications.

Table 33: EIR Provisioning Error Notifications

ID	Notification Name	Description
17500	CannotAddEIRGlobalConfigEntry	Cannot add an entry into EIRGlobalConfig table when one entry already exists.
17501	InvalidAttribute	Invalid attribute.
17502	DeleteFromEIRGlobalConfigNotAllowed	EIRGlobalConfig must have one entry so don't allow delete.
17503	SystemFailsToProcessRequest	Eir Prov Manager cannot process request.
17504	OperationNotSupported	Error: The requested operation is not supported.
17505	DbOperationFailed	Error executing a DB operation.
17506	SubscriptionIDNotFound	Cannot find the SubscriptionID.
17507	AddRespCfgNotAllowed	Adding to EirResponseConfig table not allowed.
17508	DeleteRespCfgNotAllowed	Deleting from EirResponseConfig table not allowed.
17509	InvalidIMEI	The IMEI must have 14 digits, and optionally a valid 15th check-digit.

DRA Provisioning Notifications

The following is a list of the Diameter Relay Agent (DRA) provisioning notifications.

Table 34: DRA Provisioning Error Notifications

ID	Notification Name	Description
17700	**InvalidAttribute**	Invalid attribute.
17701	**SystemFailsToProcessRequest**	DRA Prov Manager cannot process request.
17702	**InvalidHost**	Invalid Host.
17703	**InvalidRealm**	Invalid Realm.

SPR Error Notifications

The operator uses event logs to troubleshoot the SDM. Each SPR event in the event log is preceded by the date, time, the originating blade and the originating module.

Table 35: SPR Error Notifications lists the SPR Error Notifications. The interface that is used determines whether or not an error code appears in the SPR Error Notifications. A Yes indicates the error is generated and appears in the SPR error log. A No means the error is not generated and does not appear in the SPR error log.

Table 35: SPR Error Notifications

Error Code	Description	XML-REST interface	XML-SOAP interface
70110	Subscriber field not found for *sub*	Yes	No
70111	Subscriber field not found for key/value *key/value*	Yes	Yes
70112	Account id *id* not found	Yes	No
70120	Unable to create Subscriber	Yes	No
70121	Failure creating Subscriber *sub*	Yes	Yes
70130	Unable to replace Subscriber	Yes	No
70140	Subscriber already exists for key: *key* value: *value*	Yes	Yes
70141	Value for AccountId already exists *id*	Yes	Yes
70210	*OpaqueData* not found for key/value: *key/value*	Yes	Yes
70211	No *OpaqueData* found in Subscriber	Yes	No
70220	Invalid encoding for *OpaqueData* data	Yes	Yes
70230	Given key is unknown *key*	Yes	Yes
70231	Key not found for *sub*	Yes	No

Error Code	Description	XML-REST interface	XML-SOAP interface
70310	MSISDN *msisdn* not found	Yes	No
70340	Value for MSISDN already exists *msisdn*	Yes	Yes
70410	IMSI *imsi* not found	Yes	No
70440	Value for IMSI already exists *imsi*	Yes	Yes
70510	NAI *nai* not found	Yes	No
70520	Invalid value for NAI *nai*	Yes	Yes
70540	Value for NAI already exists *nai*	Yes	Yes
70610	Billing day *dd* not found	Yes	No
70620	Billing day should be an integer between 0 and 31 *dd*	Yes	No
70640	Value for Billing Day already exists *dd*	Yes	Yes
70710	Entitlement *ent* not found	Yes	No
70810	Tier *tier* not found	Yes	No
70840	Tier already exists *tier*	Yes	Yes
71110	CUSTOM*num* - *value* not found	Yes	No
71140	Value for CUSTOM*num* already exists *value*	Yes	Yes

Table 36: Policy Provisioning Error Notifications (RAS only)

Error Code	Description
MSR4000	Invalid content request data supplied.
MSR4001	Subscriber not found.
MSR4002	Subscriber field not found.
MSR4003	Key value already exists.
MSR4004	Unique key not found for subscriber.
MSR4005	Field does not support multiple values and value for field already exists.
MSR4049	UnknownType.
MSR4050	Unknown key, the key provided in the request is invalid.
MSR4051	The value provided for the field is invalid.
MSR4053	Subscriber and field exist but the value provided is incorrect, applies to delete field value.

Error Code	Description
MSR4054	Invalid XML Encoding Specified. Resend with UTF-8 encoding.
MSR4055	PoolHasMembers (cannot delete a pool that is not empty of users).
MSR4099	Unexpected server error has occurred.

Database Error Notifications

The following provides a listing of the database error notifications.

Table 37: Database Error Notifications

ID	Notification Name	ID	Notification Name
1004	CantCreateFile	1024	ErrorOnRead
1005	CantCreateTable	1025	ErrorOnRename
1006	CantCreateDb	1026	ErrorOnWrite
1007	DbCreateExist	1027	FileUsed
1008	DbDropExists	1028	FilsortAbort
1009	DbDropDelete	1029	FormNotFound
1010	DbDropRemoveDirectory	1030	GetErrano
1011	CantDeleteFile	1031	IllegalHa
1012	CantFindSystemRec	1032	KeyNotFound
1013	CantGetStat	1033	NotFormFile
1014	CantGetWd	1034	NotKeyfile
1015	CantLock	1035	OldKeyfile
1016	CantOpenFile	1036	OpenAsReadonly
1017	FileNotFound	1037	Outofmemory
1018	CantReadDir	1038	OutOfSortmemory
1019	CandSetWd	1039	UnexpectedEof
1020	Checkread	1040	ComCountError
1021	DiskFull	1041	OutOfResources
1022	DupKey	1042	BadHostError

ID	Notification Name	ID	Notification Name
1023	ErrorOnClose	1043	HandshakeError
⟵	<-----	⟵	<-----
1044	DbaccessDeniedError	1064	ParseError
1045	AccessDeniedError	1065	EmptyQuery
1046	NoDbError	1066	NonuniqTable
1047	UnknownComError	1067	InvalidDefault
1048	BadNullError	1068	MultiplePriKey
1049	BadDbError	1069	TooManyKeys
1050	TableExistsError	1070	TooManyKeyParts
1051	BadTableError	1071	TooLongKey
1052	NonUniqError	1072	KeyColumnDoesNotExits
1053	ServerShutdown	1073	BlobUsedAsKey
1054	BadFieldError	1074	TooBigFieldLength
1055	WrongFieldWithGroup	1075	WrongAutoKey
1056	WrongGroupField	1076	Ready
1057	WrongSumSelect	1077	NormalShutdown
1058	WrongValueCount	1078	GotSignal
1059	TooLongIdent	1079	ShutdownComplete
1060	DupFieldname	1080	ForcingClose
1061	DupKeyname	1081	IpsockError
1062	DuplicateEntry	1082	NoSuchIndex
1063	WrongFieldSpec	1083	WrongFieldTerminators
⟵	<-----	⟵	<-----
1084	BlobsAndNoTerminated	1104	TooBigSelect
1085	TextfileNotReadable	1105	UnknownError
1086	FileExistsError	1106	UnknownProcedure
1087	LoadInfo	1107	WrongParamcountToProcedure
1088	AlterInfo	1108	WrongParametersToProcedure
1089	WrongSubKey	1109	UnknownTable
1090	CantRemoveAllFields	1110	FieldSpecifiedTwice

ID	Notification Name	ID	Notification Name
1091	CantDropFieldOrKey	1111	InvalidGroupFundUse
1092	InsertInfo	1112	UnsupportedExtension
1093	InsertTableUsed	1113	TableMustHaveColumns
1094	NoSuchThread	1114	RecordFileFull
1095	KillDeniedError	1115	UnknownCharacterSet
1096	NoTablesUsed	1116	TooManyTables
1097	TooBigSet	1117	TooManyFields
1098	NoUniqueLogfile	1118	TooBigRowsize
1099	TableNotLockedForWrite	1119	StackOverrun
1100	TableNotLocket	1120	WrongOuterJoin
1101	BlobCantHaveDefault	1121	NullColumnInIndex
1102	WrongDbName	1122	CantFingUdf
1103	WrongTableName	1123	CantInitializeUdf
—<	<-----	—<	<-----
1124	UdfNoPaths	1144	IllegalGrantForTable
1125	UdfExists	1145	GrantWrongHostOrUser
1126	CantOpenLibrary	1146	NoSuchTable
1127	CantFindDlEntry	1147	NonexistingTableGrant
1128	FunctionNotDefined	1148	NotAllowedCommand
1129	HostIsBlocked	1149	SyntaxError
1130	HostNotPrivileged	1150	DelayedCantChangeLock
1131	PasswordAnonymousUser	1151	TooManyDelayedThreads
1132	PasswordNotAllowed	1152	AbortingConnection
1133	PasswordNoMatch	1153	NetPacketTooLarge
1134	UpdateInfo	1154	NetReadErrorFromPipe
1135	CantCreateThread	1155	NetFcntlError
1136	WrongValueCountOnRow	1156	NetPacketsOutOfOrder
1137	CantReopenTable	1157	NetUncompressError
1138	InvalidUseOfNull	1158	NetReadError
1139	RegexpError	1159	NetReadInterrupted
1140	MixOfGroupFuncAndFields	1160	NetErrorOnWrite

ID	Notification Name	ID	Notification Name
1141	NonexistingGrant	1161	NetWriteInterrupted
1142	TableaccessDeniedError	1162	TooLongString
1143	ColumnaccessDeniedError	1163	TableCantHandleBlob
——<	<-----	——<	<-----
1164	TableCantHandleAutoIncrement	1184	NewAbortingConnection
1165	DelayedInsertTableLocked	1185	DumpNotImplemented
1166	WrongColumnName	1186	FlushMasterBinlogClosed
1167	WrongKeyColumn	1187	IndexRebuild
1168	WrongMrgTable	1188	Master
1169	DupUnique	1189	MasterNetRead
1170	BlobKeyWithoutLength	1190	MasterNetWrite
1171	PrimaryCantHaveNull	1191	FtMatchingKeyNotFound
1172	TooManyRows	1192	LockOrActiveTransaction
1173	RequiresPrimaryKey	1193	UnknownSystemVariable
1174	NoRaidCompiled	1194	CrashedOnUsage
1175	UpdateWithoutKeyInSafeMode	1195	CrashedOnRepair
1176	KeyDoesNotExits	1196	WarningNotCompleteRollback
1177	CheckNoSuchTable	1197	TransCacheFull
1178	CheckNotImplemented	1198	SlaveMustStop
1179	CantDoThisDuringAnTransaction	1199	SlaveNotRunning
1180	ErrorDuringCommit	1200	BadSlave
1181	ErrorDuringRollback	1201	MasterInfo
1182	ErrorDuringFlushLogs	1202	SlaveThread
1183	ErrorDuringCheckpoint	1203	TooManyUserConnections
——<	<-----	——<	<-----
1204	SetConstantsOnly	1224	MixingNotAllowed
1205	LockWaitTimeout	1225	DupArgument
1206	LockTableFull	1226	UserLimitReached
1207	ReadOnlyTranscation	1227	SpecificAccessDeniedError
1208	DropDbWithReadLock	1228	LocalVariable

ID	Notification Name	ID	Notification Name
1209	CreateDbWithReadLock	1229	GlobalVariable
1210	WrongArguments	1230	NoDefault
1211	NoPermissionToCreateUser	1231	WrongValueForVar
1212	UnionTablesInDivverentDir	1232	WrongTypeForVar
1213	LockDeadlock	1233	VarCantBeRead
1214	TableCantHandleFulltext	1234	CantUseOptionHere
1215	CannotAddForeign	1235	NotSupportedYet
1216	NoReferencedRow	1236	MasterFatalErrorReadingBinlog
1217	RowIsReferenced	1237	SlaveIgnoredTable
1218	ConnectToMaster	1238	IncorrectGlobalLocalVar
1219	QueryOnMaster	1239	WrongForeignKeyDefinition
1220	ErrorWhenExecutingCommand	1240	KeyReferenceDoNotMatchTable Reference
1221	WrongUsage	1241	WrongOperand
1222	WrongNumberOfColumnsInSelect	1242	SubqueryNo1Row
1223	CantUpdateWithReadlock	1243	UnknownStmtHandler
---<	<-----	---<	<-----
1244	CorruptHelpDb	1264	WarnDataOutOfRange
1245	CyclicReference	1265	WarnDataTruncated
1246	AutoConvert	1266	WarnUsingOtherHandler
1247	IllegalReference	1267	CantAggregate2Collations
1248	DerivedMustHaveAlias	1268	DropUser
1249	SelectReduced	1269	RevokeGrants
1250	TableNameNotAllowedHere	1270	CantAggregate3Collations
1251	NotSupportedAuthMode	1271	CantAggregateNCollation
1252	SpatialCantHaveNull	1272	VariableIsNotStruct
1253	CollationCharsetMismatch	1273	UnknownCollation
1254	SlaveWasRunning	1274	SlaveIgnoreSSLParam
1255	SlaveWasNotRunning	1275	ServerIsInSecureAuthMode
1256	TooBigForUncompress	1276	WarnFieldResolved
1257	ZlibZMemError	1277	BadSlaveUnitlCond

ID	Notification Name	ID	Notification Name
1258	ZlibZBufError	1278	MissingSkipSlave
1259	ZlibZDataError	1279	UntilCondIgnored
1260	CutValueGroupConcat	1280	WrongNameForIndex
1261	WarnTooFewRecords	1281	WringNameForCatalog
1262	WarnTooManyRecords	1282	WarnQcResize
1263	WarnNullToNotNull	1283	BadFtColumn
——<	<-----	——<	<-----
1284	UnknownKeyCache	1304	AlreadyExists
1285	WarnHostnameWontWork	1305	DoesNotExists
1286	UnknownStorageEngine	1306	DropFailed
1287	WarnDeprecatedSyntax	1307	StoreFailed
1288	NonUpdatableTable	1308	LilableMismatch
1289	FeatureDisabled	1309	LabelRedefine
1290	OptionPreventsStatement	1310	LabelMismatch
1291	DuplicatedValueInType	1311	UNINIT_VAR
1292	TruncatedWrongValue	1312	BADSELECT
1293	TooMuchAutoTimestampCols	1313	BADRETURN
1294	InvalidOnUpdate	1314	BADSTATEMENT
1295	UnsupportedPs	1315	UPDATE_LOG_DEPRECATED_IGNORED
1296	GetErrmsg	1316	UPDATE_LOG_DEPRECATED_TRANSLATED
1297	GetTemporaryErrmsg	1317	QUERY_INTERRUPTED
1298	UnknownTimeZone	1318	WRONG_NO_OF_ARGS
1299	WarnInvalidTimestamp	1319	COND_MISMATCH
1300	InvalidCharacterString	1320	NORETURN
1301	WarnAllowedPacketOverflowed	1321	NORETURNEND
1302	ConflictingDeclarations	1322	BAD_CURSOR_QUERY
1303	NoRecursiveCreate	1323	BAD_CURSOR_SELECT
——<	<-----	——<	<-----
1324	CURSOR_MISMATCH	1344	FPARSER_EOF_IN_UNKNOWN_PARAMETER
1325	CURSOR_ALREADY_OPEN	1345	VIEW_NO_EXPLAIN

ID	Notification Name	ID	Notification Name
1326	CURSOR_NOT_OPEN	1346	FRM_UNKNOWN_TYPE
1327	UNDECLARED_VAR	1347	WRONG_OBJECT
1328	WRONG_NO_OF_FETCH_ARGS	1348	NONUPDATEABLE_COLUMN
1329	FETCH_NO_DATA	1349	VIEW_SELECT_DERIVED
1330	DUP_PARAM	1350	VIEW_SELECT_CLAUSE
1331	DUP_VAR	1351	VIEW_SELECT_VARIABLE
1332	DUP_COND	1352	VIEW_SELECT_TMPTABLE
1333	DUP_CURS	1353	VIEW_WRONG_LIST
1334	CANT_ALTER	1354	WARN_VIEW_MERGE
1335	SUBSELECT_NYI	1355	WARN_VIEW_WITHOUT_KEY
1336	STMT_NOT_ALLOWED_IN_SF_OR_TRG	1356	VIEW_INVALID
1337	VARCOND_AFTER_CURSHNDLR	1357	SP_NO_DROP_SP
1338	CURSOR_AFTER_HANDLER	1358	SP_GOTO_IN_HNDLR
1339	CASE_NOT_FOUND	1359	TRG_ALREADY_EXISTS
1340	FPARSER_TOO_BIG_FILE	1360	TRG_DOES_NOT_EXIST
1341	FPARSER_BAD_HEADER	1361	TRG_ON_VIEW_OR_TEMP_TABLE
1342	FPARSER_EOF_IN_COMMENT	1362	TRG_CANT_CHANGE_ROW
1343	FPARSER_ERROR_IN_PARAMETER	1363	TRG_NO_SUCH_ROW_IN_TRG
——<	<-----	——<	<-----
1364	NO_DEFAULT_FOR_FIELD	1384	DIFF_GROUPS_PROC
1365	DIVISION_BY_ZERO	1385	NO_GROUP_FOR_PROC
1366	TRUNCATED_WRONG_VALUE_FOR_FIELD	1386	ORDER_WITH_PROC
1367	ILLEGAL_VALUE_FOR_TYPE	1387	LOGGING_PROHIBIT_CHANGING_OF
1368	VIEW_NONUPD_CHECK	1388	NO_FILE_MAPPING
1369	VIEW_CHECK_FAILED	1389	WRONG_MAGIC
1370	PROCACCESS_DENIED_ERROR	1390	PS_MANY_PARAM
1371	RELAY_LOG_FAIL	1391	KEY_PART_0
1372	PASSWD_LENGTH	1392	VIEW_CHECKSUM
1373	UNKNOWN_TARGET_BINLOG	1393	VIEW_MULTIUPDATE
1374	IO_ERR_LOG_INDEX_READ	1394	VIEW_NO_INSERT_FIELD_LIST
1375	BINLOG_PURGE_PROHIBITED	1395	VIEW_DELETE_MERGE_VIEW

ID	Notification Name	ID	Notification Name
1376	FSEEK_FAIL	1396	CANNOT_USER
1377	BINLOG_PURGE_FATAL_ERR	1397	XAER_NOTA
1378	LOG_IN_USE	1398	XAER_INVAL
1379	LOG_PURGE_UNKNOWN_ERR	1399	XAER_RMFAIL
1380	RELAY_LOG_INIT	1400	XAER_OUTSIDE
1381	NO_BINARY_LOGGING	1401	XAER_RMERR
1382	RESERVED_SYNTAX	1402	XA_RBROLLBACK
1383	WSAS_FAILED	1403	NONEXISTING_PROC_GRANT
——<	<-----	——<	<-----
1404	PROC_AUTO_GRANT_FAIL	1424	SP_NO_RECURSION
1405	PROC_AUTO_REVOKE_FAIL	1425	TOO_BIG_SCALE
1406	DATA_TOO_LONG	1426	TOO_BIG_PRECISION
1407	SP_BAD_SQLSTATE	1427	M_BIGGER_THAN_D
1408	STARTUP	1428	WRONG_LOCK_OF_SYSTEM_TABLE
1409	LOAD_FROM_FIXED_SIZE_ROWS_TO_VAR	1429	CONNECT_TO_FOREIGN_DATA_SOURCE
1410	CANT_CREATE_USER_WITH_GRANT	1430	QUERY_ON_FOREIGN_DATA_SOURCE
1411	WRONG_VALUE_FOR_TYPE	1431	FOREIGN_DATA_SOURCE_DOESNT_EXIST
1412	TABLE_DEF_CHANGED	1432	FOREIGN_DATA_STRING_INVALID_CANT_CREATE
1413	SP_DUP_HANDLER	1433	FOREIGN_DATA_STRING_INVALID
1414	SP_NOT_VAR_ARG	1434	CANT_CREATE_FEDERATED_TABLE
1415	SP_NO_RETSET	1435	TRG_IN_WRONG_SCHEMA
1416	CANT_CREATE_GEOMETRY_OBJECT	1436	STACK_OVERRUN_NEED_MORE
1417	1383FAILED_ROUTINE_BREAK_BINLOG	1437	TOO_LONG_BODY
1418	BINL1383OG_UNSAFE_ROUTINE	1438	WARN_CANT_DROP_DEFAULT_KEYCACHE
1419	BINLOG_C1383REATE_ROUTINE_NEED_SUPER	1439	TOO_BIG_DISPLAYWIDTH
1420	1302EXEC_STMT_WITH_OPEN_CURSOR	1440	XAER_DUPID
1421	STMT_HAS_NO_OPEN_CURSOR	1441	DATETIME_FUNCTION_OVERFLOW
1422	COMMIT_NOT_ALLOWED_IN_SF_OR_TRG	1442	CANT_UPDATE_USED_TABLE_IN_SF_OR_TRG

ID	Notification Name	ID	Notification Name
1423	NO_DEFAULT_FOR_VIEW_FIELD	1443	VIEW_PREVENT_UPDATE
—<	<-----	—<	<-----
1444	PS_NO_RECURSION	1451	ROW_IS_REFERENCED_2
1445	SP_CANT_SET_AUTOCOMMIT	1452	NO_REFERENCED_ROW_2
1446	MALFORMED_DEFINER	1453	SP_BAD_VAR_SHADOW
1447	VIEW_FRM_NO_USER	1454	TRG_NO_DEFINER
1448	VIEW_OTHER_USER	1455	OLD_FILE_FORMAT
1449	NO_SUCH_USER	1456	SP_RECURSION_LIMIT
1450	FORBID_SCHEMA_CHANGE	1457	SP_PROC_TABLE_CORRUPT

System Error Notifications

Error Notification Conventions

The following tables list the System error notifications. The symbols %1 and %2 represent a variable field and different error messages will be generated according to the variable information.

General System Error Notifications

Table 38: General System Error Notifications

ID	Notification Name	Description
6300	AmsInitFailed	Error adding AMS registrar.
6301	StateRefresh	State refresh interrupted
6302	ActivateNotAllowed	Activate transition denied because initialization not finished.
6303	RoleTransition	Role is %1.
6304	StandbyNotAllowed	Standby transition denied because initialization not finished.
6305	UnassignedNotAllowed	Unassigned transition denied because initialization not finished.
6306	DbInitFailed	Error initializing database connection.

ID	Notification Name	Description
6307	**LoadSystemModelFailed**	Error loading system model from database.
6308	**InvalidParameter**	Invalid parameter
6309	**HaDisposition**	%1
6310	**ModuleRegDeniedNot Provisioned**	Module %1 not provisioned in system model. Run request denied.
6311	**ModuleDeregDeniedNot Provisioned**	Module %1 not provisioned in system model. Deregistration denied.
6312	**MemoryAllocationError**	Error allocating memory.
6313	**OperationUndefined**	Operation [%1] undefined in SystemManager.
6314	**ShelfProvisioningMissing**	No shelf information found in database.
6315	**InvalidLeftSubnet**	Invalid left backplane subnet specified.
6316	**InvalidRightSubnet**	Invalid right backplane subnet specified.
6317	**BackplaneSubnetsNot Specified**	No backplane subnet specified.
6318	**ChassisMgrInitFailed**	ChassisManager initialization failed
6319	**ScStartFailed**	Error starting SystemController on slot %1.
6320	**ModuleNotFound**	%1 module not found in the system model.
6325	**SrpCreateTransactionFailed**	srAmsStartTrn for MO [%1] returned error [%2].
6326	**SrpCreateCgFailed**	SRP error [%1] creating cluster group [%2].
6327	**SrpInitializeMoFailed**	SRP error [%1] from AMSInitialize on MO [%2].
6328	**SrpAmsSetStrAttributeFailed**	SRP error [%1] from AMSSetStrAttribute on MO [%2].
6329	**SrpAmsObjectDependencies**	SRP error [%1] from AmsSetObjectDependencies on MO [%2].
6330	**SrpAmsGetObjectDependencies**	SRP error [%1] from AmsGetObjectDependencies on MO [%2].
6331	**SrpAmsGetObjectHandle**	SRP error [%1] from AmsGetObjectHandle on MO [%2].
6332	**NoMoDeps**	No Module dependencies found in database.

ID	Notification Name	Description
6333	DpoSubscribeError	Error [%1] subscribing to DataProviderObserver.
6334	DpoUnsubscribeError	Error [%1] unsubscribing from DataProviderObserver.
6335	DpoUpdateInvalidAttrib	Update notification for entity [%1] contains invalid attribute [%2].
6338	DpoStartError	Error [%1] starting DataProviderObserver.
6339	DbLoadEntityNotFound	No provisioning information found in database for entity [%1].
6340	DbLoadEntity	Error [%1] loading entity [%2] provisioning information from database.
6341	DbSetRef	Error updating system model references.
6342	DbNoSession	No session available for request.
6343	DpoNoCriteria	Dpo notification contains no criteria set.
6344	DpoUnknownOperator	Dpo notification contains criteria with unknown operator.
6345	DpoUnsupportedEntity	Dpo notification received for unsupported entity [%1].
6346	DpoUnsupportedRequestType	Dpo notification received for entity [%1] of unsupported type [%2].
6347	DpoUnsupportedReqCriteria	Dpo notification for request type [%1] entity [%2] contains unsupported criteria operator [%3].
6348	DpoUnsupportedReqAttribute	Dpo notification for request type [%1] entity [%2] contains unsupported attribute [%3].
6349	DpoInsufficientCriteria	Dpo notification for request type [%1] entity [%2] contains insufficient criteria.
6350	DpoCriteriaValueInvalid	Dpo notification for request type [%1] entity [%2] contains invalid criteria value [%3=%4].
6351	RequestFailed	An error occurred trying to process the request.
6352	RequestTypeNotSupported	The request type is not supported.
6353	OperationNotSupported	The operation is not supported.
6354	AlreadyUnlocked	Already unlocked.
6355	UnlockedFailedMOLocked	Already locked.

ID	Notification Name	Description
6356	SrpAmsEndTransaction	SRP error [%1] from srAmsEndTrn on MO [%2].
6357	SrpAmsSetIntAttribute Failed	error [%1] from AMSSetIntAttribute on MO [%2].
6358	AlreadyLocked	Already locked
6359	LockingActiveNotAllowed	Not allowed to perform lock operation on active.
6360	SrpAmsCreateConfigured Object	srAmsCreateConfiguredObject for object [%1] returned error [%2].
6361	SrpAmsSetIntAttribute Failed_Network	Ignoring SRP return code [%1] from AMSSetIntAttribute on MO [%2].
6362	UnhandledEvent	Unable to process event [%1] during state [%2].
6363	LockUnprovisionedSlot	Not allowed to perform lock operation on unprovisioned slot.
6364	InvalidDiskUsageThresh	Invalid disk usage threshold specified.
6365	UnsupportedUpdateAttribute	Not allowed to modify the given attribute.
6366	PeerSlotUnknown	Unable to determine peer slot for slot %1.
6367	SwitchoverUnprovisioned Slot	Switchover operation not permitted on unprovisioned slot.
6368	SwitchoverNotActiveSlot	Switchover operation only permitted on slot with an HaRole of Active.
6369	SwitchoverUnprotectedSlot	Switchover operation not permitted on unprotected slot.
6370	SystemModelError	Error locating object %1 in system model.
6371	ModuleOpStateDpController	Module %1 on slot %2 operational state is %3.
6372	ModuleOpStateOampEventMgr	Module %1 on slot %2 operational state is %3.
6373	ModuleOpStateOampManager	Module %1 on slot %2 operational state is %3.
6374	ModuleOpStateOamp PerformanceManager	Module %1 on slot %2 operational state is %3.
6375	ModuleOpState HlrServer	Module %1 on slot %2 operational state is %3.
6376	ModuleOpStateHlrProvManager	Module %1 on slot %2 operational state is %3.
6377	ModuleOpStateHlrWgs	Module %1 on slot %2 operational state is %3.

ID	Notification Name	Description
6378	ModuleOpStateAucServer	Module %1 on slot %2 operational state is %3.
6379	ModuleOpStateSS7Manager	Module %1 on slot %2 operational state is %3.
6380	ModuleOpStateSipServer	Module %1 on slot %2 operational state is %3.
6381	ModuleOpStateSipGateway	Module %1 on slot %2 operational state is %3.
6382	ModuleOpStateSip ProvManager	Module %1 on slot %2 operational state is %3.
6383	ModuleOpStateNodeManager	Module %1 on slot %2 operational state is %3
6384	ModuleOpStateSipGsmGateway	Module %1 on slot %2 operational state is %3
6385	ModuleOpStateSipIpManager	Module %1 on slot %2 operational state is %3
6386	ModuleRestarted	Module %1 on slot %2 was restarted.
6387	ShelfManagerIpNotSpecified	No shelf manager IP specified.
6388	ModuleStateSubscriberFailed	Module State Subscriber init error
6389	IdentityAlreadyBind	Identity %1 is already bind to slot %2.
6390	ModuleAlreadyDeployed	Module %1 required by service %2 is already deployed on slot %3.
6391	NoSlotIdentity	Slot %1 has no identity.
6392	ServiceAlreadyBind	Service %1 is already bind to slot %2.
6393	CoreServiceFound	Core service %1 must be removed before removing identity %2.
6394	ClusterGroupNotFound	ClusterGroup %1 not found in provisioning.
6395	ActiveStandbyAllocFailed	Active standby module already allocated.
6396	SysModelEntityNotFound	Cannot retrieved the specified entity form in-memory system model.
6397	ServiceNotBind	Service %1 is not bind to slot %2
6398	SrpAmsGetStrAttributeFailed	SRP error [%1] from AMSGetStrAttribute on MO [%2].
6399	SrpDeleteMoFailed	SRP error [%1] while deleting MO [%2].
6400	UserServiceBindingFound	User service binding to slot [%1] found.
6401	InvalidOption	Service [%1] doesn't support option [%2].

ID	Notification Name	Description
6402	**ServiceInstanceOptionExist**	Option [%1] already bind to service[%2] on slot[%3].
6403	**StartServiceFailed**	Failed to start service [%1] on shelf[%2], slot[%3].
6404	**StopServiceFailed**	Failed to stop service [%1] on shelf[%2], slot[%3].
6405	**SwitchoverNotActiveService**	Switchover operation only permitted on service with an HaRole of Active.
6406	**SwitchoverUnprotected Service**	Switchover operation not permitted on unprotected service.
6407	**PeerServiceUnknown**	Unable to determine peer service for service %1 on slot %2.
6408	**NonDynamicOption**	Cannot add or remove non-dynamic option %1 on started service %2, stop service first.
6409	**MissingServiceScript**	Cannot find service script %1 for service %2.
6410	**LoadSharingFailed**	Failed to configured ModuleType[%1] in load-sharing mode.
6411	**SetOampVipFailed**	Failed to configure the Oamp VIP.
6412	**SetSipVipFailed**	Failed to configure the SIP VIP.
6413	**SetHssVipFailed**	Failed to configure the HSS VIP.
6414	**ClearOampVipFailed**	Failed to clear the Oamp VIP.
6415	**ClearSipVipFailed**	Failed to clear the SIP VIP.
6416	**ClearHssVipFailed**	Failed to clear the HSS VIP.
6417	**AsynchronousOperation**	This operation is handled asynchronously.
6418	**ExceedServiceMaxInstance**	Service %1 maximum number of instance has been reached.
6419	**SystemConfigurationFailed**	The system configuration [%1] failed on slot %2.
6420	**RemovingActiveSystem Controller**	Cannot remove active system controller identity, operation not permitted.
6421	**CannotRemoveRunningService**	Service [%1] on slot [%2] must be stopped before removing it.

ID	Notification Name	Description
6423	**CannotRemoveCoreService**	Cannot remove core service [%1] on slot[%2] of shelf [%3] while at least one user service is still running.
6424	**RunTimeConfigNotAllowed**	Attribute update while the ServiceInstance is started is not permitted.
6425	**SecurityReplicationFailed**	Failed to replicate security configuration on host[%1].
6426	**RemoveCoreServiceNotAllowed**	Removing a core service is not allowed, remove identity instead
6427	**IoctlError**	Ioctl error while reading network configuration [%1] of interface [%2].
6428	**InvalidNetmask**	Invalid Netmask for virtual interface [%1]. Netmask should be [%2].
6429	**NetworkConfigFailed**	Configuration of %1 on interface [%2] with value [%3] failed.
6430	**NoGeoRedundantSite**	No geo-redundant site is configured.
6431	**NotInitialized**	Component [%1] is not initialized.
6432	**VipBindingAlreadyExist**	VipBinding already exist
6433	**VipBindToAnotherService**	Vip [%1] already exist on slot[%2] for service[%3].
6434	**VipBindToAnotherSlot**	Error, Vip [%1] already exist on other slot[%2].
6435	**VipReservedByAccessIp**	Error, Vip [%1] is already reserved for slot[%2] public access IP.
6436	**VipReservedByPublic OampVip**	Error, Vip [%1] is already reserved for public OAMP VIP.
6437	**InvalidVipValue**	Error, Vip [%1] is not compatible with network %2/%3.
6438	**StoppingActiveSystem ControllerNotAllowed**	Stopping active System Controller on slot[%2] of shelf [%3] from user interface is not allowed.
6439	**VipAlreadyExist**	VipType %1 is already bind with IpAddress %2.
6440	**VipReservedForShelf PrivateNetwork**	Error, Cannot bind Vip [%1] that lie in shelf private network [%2:%3].

ID	Notification Name	Description
6441	SetVipFailed	Failed to bind VIP [%1] on slot[%2]. Reason: %3.
6442	OperationNotAllowedWhile ServiceIsStartingOrStopping	Cannot perform operation [%1] while service is in [%2] state.
6443	InvalidIpAddressFormat	String [%1] doesn't comply to IP address format (no heading or trailing space are allowed).
6444	InvalidNetmaskFormat	String [%1] doesn't comply to netmask address format (no heading or trailing space are allowed)
6445	CannotModifySysModelWhile DbIsSynchronizing	Cannot add/remove identity or service while DB is synchronizing
6446	NotActiveSystemController	Operation can only performed on active system controller
6449	SrpAmsAllocRemoteAdapter Failed	SRP error [%1] while allocating remote adapter for MO [%2].
6450	SubscribersSetAlreadyExist	SubscribersSet [%1] already exist.
6451	SubsSetClusterNotRemoved	SubsSetCluster on slot [%1] are still bind to SubscribersSet [%2].
6452	SubsSetAlreadyAssigned ToSlot	Slot[%1] is already bind to SubscribersSet [%2].
6453	SrpDeleteCgFailed	SRP error [%1] deleting cluster group [%2].
6454	InvalidSystemController SubscribersSet	All SystemController blade must be bind to same SubscribersSet.
6455	CannotAddFwServiceOn SystemController	Cannot add service[%1] of type Framework on a SystemController slot [%2].
6456	CannotBindSubsSetOnSlot WithNoidentity	Cannot bind slot [%1] to SubscribersSet [%2] because there is no identity bind to this slot.
6457	CannotBindSubsSetToMore ThanTwoSlots	Cannot bind SubscribersSet to more than one slot.
6459	SubsSetRemovalAllowedOnly WhenDatabaseStopped	Cannot unbind SubsSet while database service is not stopped.
6460	RemoveSubsSetBeforeIdentity	Cannot remove identity from slot [%1] because SubscribersSet [%2] is still bind to this slot.

ID	Notification Name	Description
6461	RemovingBackendService NotAllowed	Removing a backend service is not allowed, unbind SubscribersSet instead.
6462	AddingBackendService NotAllowed	Adding a backend service is not allowed, bind SubscribersSet instead.
6463	OnlyOneFragmentSupported	Only one fragment must exist in single fragment mode.
6464	GenericError	Error: %1.
6465	GenericInfo	Info: %1.
6466	BackgroundMonitorBusy	SystemManager is already busy processing task: %1.
6467	ServiceScriptBusy	The service [%1] script is currently busy.
6468	NodeUnreachable	Cannot reach node [%1].
6469	RemoteAdapterNotFound	Cannot found remote adapter form orl [%1].
6470	SelfReliantError	Error [%1] while performing operation [%2].
6471	ShellCommandTimeout	Timeout while sending command to shell.
6472	DatabaseInstallation Failed	Failed to installed DB group %1 on slot %2 of shelf %3, [reason: %4].
6473	SubsSetNotDisabled	SubscribersSet must be disabled to be modified.
6474	InvalidSubsSetId	SubsSetId must be higher than 0 and lower than 256.
6475	OperationNotSupportedIn SingleFragmentMode	Operation is not supported in single fragment configuration.
6476	ClearReservedVipFailed	Failed to clear reserved VIP [%1].
6477	NotReadyForManualSWO	Blade is not ready for manual switchover until [%1].
6478	LockingNotAllowed	Locking is not allowed.
6479	SCSubscribersSetAlready Exist	System Controller SubscribersSet already exist.
6480	InvalidSubsSetIdentity	SubscribersSet identity is not the same as slot identity.
6481	CannotRemoveChildService	Cannot remove child service.

ID	Notification Name	Description
6482	ChangingServiceGroup NotAllowed	Changing service group only allowed on Backend service.
6483	ProxyApplicationNotExist	ProxyApplication does not exist.
6484	ProxyApplicationAlready Exist	Decoupled application already exist.
6485	UnknownModuleType	Unknown ModuleType.
6486	CannotRemoveInternal Component Instance	Removing internal component instance not allowed.
6487	VipNotFound	Cannot find Vip.
6488	InvalidUpgradeState	Invalid upgrade state.
6489	MissingUpgradedNode	Node [%1] is not upgraded.
6490	DatabaseRoutingSwitchFailed	Failed to switch DatabaseRouting after upgrade.
6491	NoMasterDatabaseFor ServiceGroup	No master found for database service group [%1].
6492	NoDatabaseFoundOnNode	No database found on node.
6493	GeoClusterNotFoundFor SpecificUpgradeState	Cannot find database for GeoClusterId [%1] in upgrade state [%2].
6494	SubsSetNotFoundForSpecific UpgradeState	Cannot find database for SubscribersSet [%1] in upgrade state [%2].

DPM Error Notifications

Table 39: DPM Error Notifications

ID	Notification Name	Description
1	RequestHasNotBeenProcessed	Request has not been sent to processing yet.
2	ErrorProcessingRequest	N/A
3	ErrorInitializing RelationalDataSource	N/A
4	ErrorPendingRequestIn TransactionMode	N/A
5	ErrorWrongRequestId	N/A

ID	Notification Name	Description
6	ErrorGettingRelational DataProvider	N/A
7	ErrorTransactionIn TransactionNotSupported	N/A
8	ErrorCommandSentOutOfSync	N/A
9	ErrorServerIsGone	N/A
10	ErrorConnection	N/A
11	ErrorConnectionUnknownHost	N/A
12	ErrorServerConnectionIs LostDuringQuery	N/A
13	ErrorServerQueryError	N/A
14	MessageHasNotBeenQueued	N/A
15	ErrorInitiatingDataProvider	N/A
16	ErrorCommitBeforeStart Transaction	N/A
17	ErrorAllocatingDataSource Accessor	N/A
18	WrongTransactionUsage	N/A
19	OutOfMemory	N/A
20	ErrorClientVersion	N/A
21	ErrorDatabaseIsNotAlive	N/A
22	WarningNoConnectionActive	N/A
23	ErrorProcessingController Command	N/A
24	ErrorAllocatingMemory	N/A
25	ErrorGeneralRequestError	N/A
26	ErrorRequestCreation MemoryError	N/A
27	ExceptionCaugth	N/A
28	ErrorParsingRequest	N/A

ID	Notification Name	Description
29	ErrorDataProviderNot Initialized	N/A
30	ErrorParsingXml	N/A
31	ErrorProcessingParameters	N/A
32	ErrorCommandOutOfSync Rejected	N/A
33	ErrorNotFound	N/A
34	ErrorRequestStateError	N/A
62	ErrorSessionNotAvailable	N/A
63	ErrorRdbWrongDbLocation	N/A
64	ErrorRdbInvalidSubsSetId	N/A
65	ErrorRdbSpArpFailed	N/A
66	ErrorRdbDataLocationFailed	N/A
67	ErrorRdbResultProxyTooSmall	N/A
68	ErrorRdbResultBufferInvalid	N/A
69	ErrorRdbResultBufferToo Small	N/A
70	ErrorRdbInvalidResult	N/A
71	ErrorRdbPoolNotExist	N/A
72	ErrorRdbInvalidType	N/A
73	ErrorNoConnectionAvailable	N/A
74	ErrorRdbUseOtherRdb	N/A
75	ErrorRdbReqResultTimeout	N/A
76	ErrorRdbReqNull	N/A
77	ErrorRdbUnknownConstraint	N/A
78	RdbRequestBroadcast	N/A
79	RdbDppNotSupported	N/A
80	ErrorRdbNoProviderAvailable	N/A

ID	Notification Name	Description
81	ErrorGetRequestConstraint	N/A
82	ErrorNoActiveFragment	N/A
83	ErrorInvalidConstraint	N/A
84	FailedToComplyConstraint	N/A
85	ErrorInvalidDistribution Type	N/A
86	ErrorInstallingPhysical DatabaseSchema	ErrorInstallingPhysical DatabaseSchema
87	NoResultFromDpp	N/A
88	NotAllResultFromDpp	N/A
89	NoRowAffected	N/A
90	TransactionNested	N/A

DPM Request Handle Error Notifications

Table 40: DPM Request Handle Error Notifications

ID	Notification Name	Description
3001	ErrorXmlTag	N/A
3002	ErrorXmlCaughtByParser	N/A
3003	ErrorXmlMissingTagNbReq	N/A
3004	ErrorXmlMissingTag RequestName	N/A
3005	ErrorXmlRequestType	N/A
3006	ErrorTagEntity	N/A
3007	ErrorTagAttr	N/A
3008	ErrorTagOp	N/A
3009	ErrorTagValue	N/A
3010	ErrorAllocatingResultSet	N/A
3011	ErrorAllocatingResult SetRow	N/A

ID	Notification Name	Description
3012	ErrorAllocatingResultSet RowValue	N/A
3013	ErrorTagOperation	N/A
3014	ErrorTagFunction	N/A
3015	ErrorXmlRequestTemplate MissingTagId	Error parsing request template. Tag id not specified.
3016	ErrorAllocatingRequest	Error allocating new request
3017	ErrorXmlTpiMissing Attribute	Error parsing tpi. Attribute not specified
3018	ErrorXmlTpiMissing AttributeValue	Error parsing tpi. Attribute value not specified
3019	ErrorXmlProvTemplate MissingTagId	Error parsing template. Tag id not specified
3020	ErrorAllocatingProvTemplate	Error allocating template
3021	ErrorXmlProvTemplate MissingAttribute	Error parsing template. Attribute not specified
3022	ErrorXmlProvTemplate MissingTrId	Error parsing template. Template request id not specified

Framework Error Notifications

Table 41: Framework Error Notifications

(The symbols %1, %2, and %3 represent a variable field and different error messages will be generated according to the variable information).

ID	Notification Name	Description
37	LackingDatabaseThread Resource	Lacking database thread resource.
42	DatabaseNotRunning	The database is no longer running. Restarting.
43	DatabaseReplicationStatus NotRunning	The database replication mechanism is no longer running. Restarting.
44	ErrorBackupDatabase StructureDoesNotMatch	Error restoring the backup database structure does not match.
45	ErrorSessionModeAlreadySet	The session mode is already set for a given module.

ID	Notification Name	Description
46	ErrorAlreadyLoadSharing Module	The system is already load sharing this module.
47	ErrorModuleLoadSharing NotEnabled	Load sharing for this module is not enabled.
48	ErrorNoLoadShareCluster Found	Can't find any load sharing cluster for that given module type.
49	ErrorNoMasterModuleFound	Can't find any active master module for that module type.
50	ErrorAttributeNotFound	Can't find the specified attribute.
51	ScheduledDbBackupCompleted	Scheduled Database Backup completed.
52	ErrorStopAllServices	Error stop all services except CoreSystemController active.
54	TryLockFailed	Trylock failed.
55	ErrorStandbyActivation	Dpc error standby activation (%1).
56	TemplateInvokingfileNoTpi	The Template Invoking file has no template instructions.
57	TemplateInvokingfileTpi NoAttribute	The Template Invoking file instruction has no attribute.
58	TemplateInvokingfileTpi NoAttributeValue	The Template Invoking file instruction has no attribute value.
59	TemplateInvokingfileError CreatingTpi	Error creating the Template Invoking file instruction.
60	ProvTemplateNoTreq	Template has no template requests.
61	MaximumTemplateInstance Reached	Error maximum number of template instances reached.
100	ErrorStopAuditFirst	Audit component should be stop first.
101	ErrorOperationOnAudit	Audit doesn't support this operation.
102	ServiceGroupNotActive	Error service group is not active.
2001	MessageWasNotQueued	N/A
2002	MessageSentSizeMismatch	N/A
2004	NotABooleanValue	%1 not a boolean value (0 false, 1 true).
2005	StringSize	%1 string size limit %2.

ID	Notification Name	Description
2006	DigitOnlyAccepted	%1 digit only are accepted.
2007	NotInRange	%1 value not in range: %2-%3.
2008	NumericSize	%1 too many digits max.: %2
2009	CharacterOnlyAccepted	%1 character only are accepted.
2010	InvalidEnumValue	%1 invalid enum value, single in-list value accepted.
2011	AsynchronousEventScheduled	Asynchronous event currently executing.
2012	DatabaseNotInitialized	Cannot log alarm database not initialize.
2013	UndefinedAlarmOperation	Undefined alarm operation (alarm: %1).
2014	MissingDatabaseSession	Missing database session.
2015	InvalidSetValue	%1 invalid set value (i.e., or values).
2016	ExceptionCaught	Exception caught by the framework: %1.
2017	ProtocolError	Protocol exchange error.
2018	ErrorMissingMandatory Parameter	Parameter %1 must be provided.
2020	GenericError	Error: %1
2021	GenericInfo	Info: %1
2022	UndefinedOperation	Undefined operation %1.
2023	InvalidTimeFormat	Invalid time format
2200	GeoBackupFailedWrongState	Geo backup request failed wrong state.
2201	GeoBackupFailedDuringBackup	Geo backup request failed during backup execution.
2202	ErrorProcessingGeoRestore Request	Error Processing Geographic Restore Request.
2203	ErrorObtainingGeoRestore Checkpoint	Error obtaining geographic restore checkpoint position.
2204	ErrorRestoringGeoRestore Checkpoint	Error restoring geographic restore checkpoint position.
2206	ErrorCannotStartMasterTo MasterReplication	Error cannot start master-to-master replication.

ID	Notification Name	Description
2209	ErrorWrongStateTransition Detected	Error wrong state transition detected.
2212	PublishFailed	Publish failed with error [%1].
2213	GeoRedundancyEventInfo	Geo-Redundancy INFO --> EVENT=%1 STATE=%2 CLUSTER=%3.
2214	GeoRedundancyEventWarning	Geo-Redundancy WARNING --> EVENT=%1 STATE=%2 CLUSTER=%3.
2215	GeoRedundancyEventError	Geo-Redundancy ERROR --> EVENT=%1 STATE=%2 CLUSTER=%3.
4106	AlreadyStarted	Database Extraction Tool is already started. No config change is allowed.
4107	NotStarted	Database Extraction Tool is not started yet.
4108	InternalFailed	Database Extraction Tool experienced an internal failure.
4109	StillRunning	Database Extraction Tool is still running.
4110	KeyNotSupported	Database Extraction Tool does not support service key provided.
4111	MixServiceNotSupported	Database Extraction Tool does not support mix services (pool and non-pool).
4112	InvalidHostIp	Database Extraction Tool detects invalid remote host IP.
4113	MissingRangeValue	Database Extraction Tool requires range value.
4114	MissingHostAuth	Database Extraction Tool requires remote host authentication data (user and password).
4118	ServiceListEmpty	Database Extraction Tool detects empty service list table.

Critical Resource Monitoring Error

Table 42: Critical Resource Monitoring Error

ID	Notification Name	Description
319	NtpError	NTP daemon state (%1) unknown.
326	StructureNotFound	Structure %1 not found %2.

ID	Notification Name	Description
327	StructureAlreadyDefined	Structure %1 already defined %2.
328	XmlParsingError	Error parsing XML.
329	XmlParsingException	Exception while parsing XML.
330	XmlErrorParsingStructure	Error parsing XML structure %1.
331	CantLoadStaticSchema	Can't dynamically load static schema.

DPC (Data Provider Controller) Error Notifications

Table 43: DPC (Data Provider Controller) Error Notifications

ID	Notification Name	Description
4000	ErrorSettingCommunication	Error setting communication.
4001	ErrorStartingDatabase	Error starting the database.
4002	ErrorControllerNot Constructed	Error controller not instantiated.
4003	ErrorControllerNot Initialized	Error controller not initialized.
4004	ErrorDatabaseStopped	Error database stopped.
4005	ErrorStanbyCantConnect NoIpAddress	Error standby can not connect no ip address.
4006	ErrorInitializingRelational DataSource	Error initializing resource manager.
4007	ErrorDatabaseIsNotAlive	Error database is not alive.
4008	ErrorDatabaseIsStillAlive	Error database is still alive.
4009	ErrorSlaveIsNotActive	Error slave not ready.
4010	ErrorGettingSlaveHostAddress	Error getting slave host address.
4011	ErrorProducingMasterBackup	Error producing master backup.
4012	ErrorSlaveNotInitialized	Error slave database not initiated.
4013	ErrorRequestNotProcessed	Error request not processed.
4014	ErrorProcessingBackup Request	Error processing backup request.
4015	ErrorFileDoesNotExist	Error file does not exist.

ID	Notification Name	Description
4016	ErrorRestoreMustBe AppliedAgainst-ActiveWithoutStandby	Error restore must be applied against active with no standby.
4017	ErrorRestoringDatabase	Error restoring database invalid parameters.
4018	ErrorBackupingDatabase	Error backuping database.
4019	ErrorNicNotAlive	Error network IP address not active.
4020	ErrorProducingTarFile	Error producing tar.
4021	ErrorTransferring BackupFiles	Error transferring backup file.
4022	ErrorUntarringFile	Error untarring file.
4023	ErrorTransferring RestoredFiles	Error transferring restored file.
4024	ErrorExtractingData FromBackupFile	Error extracting data from backup file.
4025	ErrorChangingOwnershipOf RestoredFile	Error changing ownership of restored file.
4026	InvalidOperator	Invalid operator used after: %1.
4027	ModuleStateChange	Internal module state change %1 %2.
4028	ActiveObjectQueueStopped	ActiveObject queue is stopped.
4029	ErrorInitiatingShelf Upgrade	Initiating upgrade sequence. Check if upgrade is not already ongoing.
4030	ErrorStartCollection	Starting collection. Shelf upgrade must be initiated first.
4032	ErrorSynchronizing WithGeographicLocation	Synchronizing with geographic database site %1.
4036	GeoRedundancyDisabled	Error, geo-redundancy is disabled.
4039	GeoConnectionClosed	Error, trying to send a message to geo-redundancy peer while the connection is closed.
4100	AlreadyStarted	DRM is already started. No config change is allowed.
4101	NotStarted	DRM is not started yet.
4102	InternalFailed	DRM experienced an internal failure.
4103	StillRunning	DRM is still running.

ID	Notification Name	Description
4105	ScanMethodNot SupportedYet	Scan method not supported yet.

OAM&P Error Notifications

Table 44: OAM&P Error Notifications

ID	Notification Name	Description
7001	DeliveryError	delivering the message to module owner
7002	DeliveryTimeout	delivery timeout
7003	UnknownModule	error module currently not available
7004	InvalidRequest	invalid request
7005	DbHandlerError	handling request
7006	DbProcessingError	processing database request
7007	InitiatingException	error initiating OampManager
7008	ErrorAllocatingDatabase Session	error allocating database session
7013	GeneralFailure	Oamp general failure
7014	LoginFail	Login failed
7015	UserAucFail	User authentication failure
7016	AccessViolation	Access violation
7017	GetOSDataFail	Access violation
7018	InvalidUser	Invalid user provided
7019	InvalidGroup	Invalid group provided
7020	Note: xception	Not an exception Oamp operation
7021	InvalidParamValue	Invalid parameter value
7022	InvalidPasswd	Invalid password provided
7023	GroupNotEmpty	Group still has users
7024	UserExist	Security user already exists
7025	GroupExist	Security group already exists

ID	Notification Name	Description
7026	RequestFailed	Request is failed
7027	GenericError	Error: %1
7028	InvalidRequestTemplate	Error occurred while translating RequestTemplate into XML DB Requests.
7029	RequestTemplateExecution Error	Error occurred while processing RequestTemplate, on request %1 with error code %2.
7030	RequestTemplateValidation Error	Error occurred while validating RequestTemplate.
7031	XdsError	Error: %1
7032	XdsInfo	Info: %1
7033	SubscriptionIsReferenced	Subscription cannot be deleted because it still contains at least one subscriber profile.
7034	CommitOrRollbackBefore StartTransaction	Commit or Rollback received before StartTransaction.
7035	SubscriberManagerOutOf Resources	Subscriber Manager is busy and has no more resources to process request.
7036	TransactionFailure	Transaction could not be processed properly
7037	ManualTransactionRequest NotAllowed	StartTransaction, Commit or Rollback requests not allowed in transaction object.
7038	FailedToAccessLicense	Failed to access license information, provisioning will not be allowed (%1).
7039	ConnectionHeartbeat	Connection heartbeat with XDS is successful.
7040	ServiceExist	Security service already exists.
7041	UserExistInOs	Security user exists in OS. Don't allow deletion.
7042	GroupExistInOs	Security group exists in OS. Don't allow deletion.
7043	UserCantBeChanged	Security user property can't be changed on run-time. It should be deleted first.
7044	GroupCantBeChanged	Security group property can't be changed on run-time. It should be deleted first.
7045	InvalidService	Invalid service provided.
7046	RequestTooLong	Request has exceeded size limit of %1 bytes.

ID	Notification Name	Description
7047	**DasError**	Error: %1
7048	**DasInfo**	Info: %1
7049	**RasError**	Error: %1
7050	**RasInfo**	Info: %1
7051	**GeoRedundancyDownSubs DelNotAllowed**	Deletion of a subscriber not allowed while the Geo-Redundancy connection is down.
7054	**SprMaxNumberSubsLicense Violation**	Rejection: The maximum number of SPR subscribers authorized by the license is reached!
7055	**SprPoolHasSubscriber**	Rejection: The pool subscriber has profile subscriber connected.!
7056	**SprProfileIsMemberOfPool**	Rejection: The profile is a member of a pool!

Chapter 4

Database Operations

Topics:

This chapter describes the entities for the different database operations that can be performed with the SDM Database. The database operations can be performed from the WebCI, more precisely, from the Database application folder, which provides access to the Backup and Restore operations.

Database Entities

Geo-Database State

Name
GeoDatabaseState

Description

This is used to get information on the state of the database in a geo-redundancy deployment.

CLI Navigation
Database[]>GeoDatabaseState

CLI Inherited Attributes

None.

CLI Command Syntax
Database[]> display GeoDatabaseState[]

Operations Permitted
Display.

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Table 9: Predefined access permissions to services per user group* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 45: Geo-Database State Mandatory Attributes

Attribute	Value Range	Default	Description
DbGeoState	**Starting** **Initialized** **PendingReplica** **Replica** **PendingReference** **Negotiating** **Reference** **ReferenceProtected** **UnassignedEnabled**	N/A	Read only. It indicates the state of the database during the synchronization and replication process for a system in a geo-redundancy deployment.

Attribute	Value Range	Default	Description
	UnassignedDisabled **Stopped**		

CLI Example

```
1 :Database[]> GeoDatabaseState[]> display
```

Database Operations

This section describes the operations that can be performed with the SDM Database.

Database Backup

The SDM system allows for a full consistent snapshot of the database or segments of it to be taken while it is active. A backup of all the subscriber data and system configuration data on the active System Controller can be executed manually, as well as an individual backup of only subscriber data or only alarms or only OamConfiguration or only HlrConfiguration. Moreover, an automatic backup can be set and activated to perform backups of the subscriber profiles data automatically.

Manual Backup from CLI

The operator can manually perform a backup of all the database or only one of the following segments of it on the active System Controller:

- Subscriber Profiles
- Alarms
- OamConfiguration
- HlrConfiguration
- HssConfiguration

When executing the Backup operation, a directory must be specified of where the backup is to be stored on the active System Controller and the segment of the database to be backed up must be specified.

Caution: The backup operation impacts the performance of the system. Hence, the backup operation must be done only during low traffic periods.

A backup can be done for all the database files or individually of only one database file:

Table 46: Database Files and Backup Extensions

Database file	Operation	Backup file extension
All databases	Backup()	all.tar
Subscribers	Backup()	bluedb.tar

Database file	Operation	Backup file extension
Alarms	Backup()	bluealm.tar
OamConfiguration	Backup()	blueoam.tar
HlrConfiguration	Backup()	bluehlr.tar
HssConfiguration	Backup()	bluehss.tar

Caution: The size of the backup file .tar can be big and therefore, it is very important to transfer the database backup file onto a backup server.

For example, to initiate a backup, type:

```
:Database[]> Backup() ToDirectory = /export/backup ;Database=Alarms
```

Where Database can take the following values:

```
0 All Databases
1 Subscribers
3 Alarms
4 OamConfiguration
5 HlrConfiguration
6 HssConfiguration
```

The backup operation will store the entire backup data along with the related database structure information in a tarball in the directory specified.

An example of a backup filename is: `dbback_050303_142434_all.tar` (in the format: dbback_yymmdd_hhmmss_all.tar), where

yy = 2 digit year

mm = 2 digit month

dd = 2 digit day

hh = 2 digit hour

mm = 2 digit minute

ss = 2 digit second

Automatic Backup from CLI

A backup of all the subscriber profiles can be performed automatically on the active System Controller. No automatic backups are executed by default, this function must be activated in order to start automatic backups. Automatic backups are executed at the time specified by the operator when setting the DatabaseBackupSchedule through the CLI or WebCI. In an automatic backup, a maximum of 7 files can be backed up. This number must be adjusted based on the size of the backup files.

To perform an automatic backup, a backup schedule must be defined. By default, the automatic backup only backs up all the subscriber profiles data. However, when setting the schedule of the automatic backup, the Network Operator can optionally set the IncludeConfiguration parameter to '1'. This will set the automatic backup to back up all the configuration data in addition to all the subscriber profiles

data. An automatic backup of Subscriber Profiles and optionally of all configuration data will be performed every time it has been scheduled to do so.

Refer to section "Creating a Backup of the system" and "Restoring the system from a backup" of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for instructions that show how to set a backup schedule, activate the automatic backup, deactivate it and modify it.

Here are more details on the entity to configure to set the Automatic backup through CLI and WebCI.

Database Backup Schedule

Name
`DatabaseBackupSchedule`

Description

Entity that allows the operator to set the automatic backup, its schedule, backup directory and file rotation in storage.

CLI Navigation
`Database[]>DatabaseBackupSchedule`

CLI Inherited Attributes

None.

CLI Command Syntax
```
:Database[]> add
DatabaseBackupSchedule[Hour=time;Minute=time;BackupDirectory=text;FileRotation=1
to 7; IncludeConfiguration=0,1]
```

Operations Permitted
`Add, modify, display, delete.`

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Table 9: Predefined access permissions to services per user group* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 47: Database Backup Schedule Mandatory Attributes

Attribute	Value Range	Default	Description
`Hour`	Time in hours	N/A	Hour at which the subscriber profiles data will automatically be backed up.
`Minute`	Time in minutes	N/A	Minutes at which the subscriber profiles data

Attribute	Value Range	Default	Description
			will automatically be backed up.
BackupDirectory	text	N/A	Directory where you wish to store the file with the subscriber profiles data backed up.
FileRotation	1 to 7	N/A	Number of backup files that can be stored in the directory. It is recommended that a maximum of 7 files be stored at the same time. This number must be adjusted based on the size of the backup files.
IncludeConfiguration	Bool 0 or 1	0	Parameter that indicates whether or not all the configuration data must be included in the automatic backup. 0: The automatic backup only backs up all the subscriber profiles. 1: The automatic backup backs up all the subscriber profiles and all the configuration data.

CLI Example

```
1 :Database[]> add DatabaseBackupSchedule[Hour=3; Minute=45;
BackupDirectory=/export/backup;FileRotation=7;IncludeConfiguration=1]
```

Once the DatabaseBackupSchedule has been set, the operator must activate it if he wants a backup of the subscriber profiles data to be performed automatically following the schedule set. The operator can also deactivate the automatic backup feature. To do so, two operations exist as follows:

Activate()

This operation is used to activate the automatic backup with the DatabaseBackupSchedule already provisioned.

Command syntax:

```
Database[]> DatabaseBackupSchedule[]> Activate()
```

Deactivate()

This operation is used to deactivate an automatic backup.

Command syntax:

```
Database[]> DatabaseBackupSchedule[]> Disable()
```

Restore from CLI

Requirements: Lockout and deactivate the standby System Controller.

Danger: When restoring the database, this operation will cause the system to be down and thus not available until the database has been restored on the active blade.

Danger: When restoring the database on Geo-Redundant system, this operation can lead to loss of subscriber provisioning activity on system where the Geo-Redundancy was disabled for more than 4 hours. Please refer to *Geo-Cluster Configuration* for more information on Geo-Redundancy management.

The Restore operation will restore database information onto the active System Controller. To execute this operation, the directory and the filename of the backup database must be provided.

For example, to restore a database, type:

```
:Database[]> Restore() FromDirectory = /blue/var/dbbackclnt; FileName =
dbback_050302_142434_all.tar
```

To List the files in the /export/backup directory, type:

```
Database[]> GetFileList() FromDirectory = /export/backup
```

Database Application Folder

This section describes the operations that can be performed with the SDM Database from the WebCI. The Database application folder provides access to the Backup and Restore operations.

Manual Backup from WebCI

The Backup view is used to create either a full database backup of all the subscriber's data and configuration files on the active System Controller (SC), or individually of only the subscriber's data, only alarms, only OamConfiguration, only HlrConfiguration and only HssConfiguration. Finally, the directory to store the backup file can be specified.

Caution: The backup operation impacts the performance of the system. Hence, the backup operation must be done only during low traffic periods.

DANGER

Danger: When restoring the database on Geo-Redundant system, this operation can lead to loss of subscriber provisioning activity on system where the Geo-Redundancy was disabled for more than 4 hours. Please refer to *Geo-Cluster Configuration* for more information on Geo-Redundancy management.

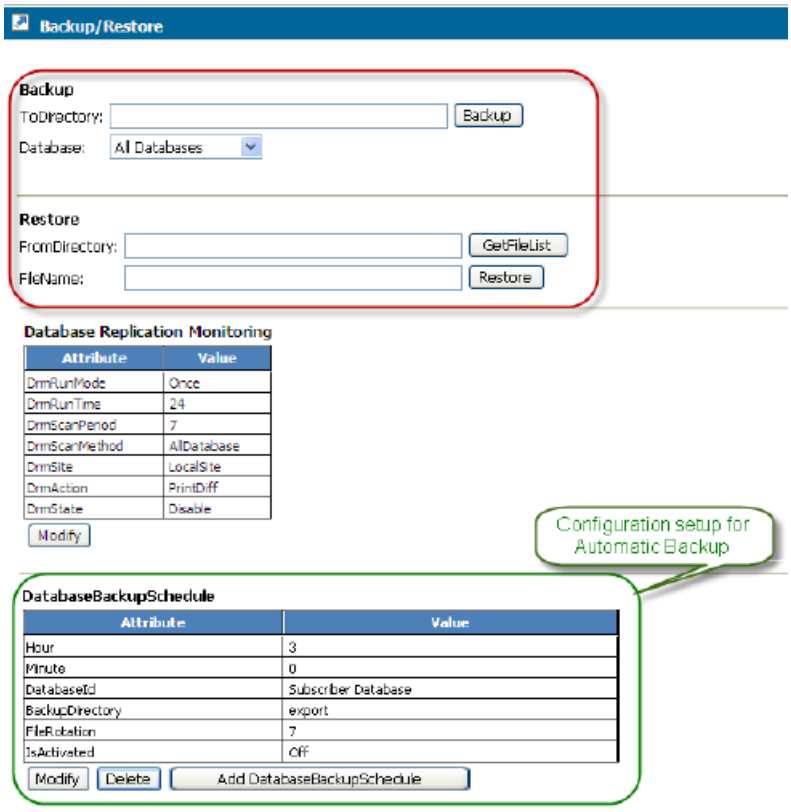


Figure 10: Backup/Restore Window

Automatic Backup from WebCI

The Automatic Backup creates a consistent snapshot of the subscriber's profile data while the system is active. It will backup all the subscriber's profile data onto the active System Controller (SC).

An automatic backup can be set and activated through the WebCI, with the DatabaseBackupSchedule table in the Database Configuration window (see *Figure 10: Backup/Restore Window*). By default, the automatic backup only backs up all the subscriber profiles data. However, when setting the schedule of the automatic backup, the Network Operator can optionally set the IncludeConfiguration parameter to '1'. This will set the automatic backup to back up all the configuration data in addition to all the subscriber profiles data.

An automatic backup of Subscriber Profiles and optionally of all configuration data will be performed every time it has been scheduled to do so.

To have more details on the step-by-step procedures to set, activate, modify or deactivate an automatic backup, please refer to the "Creating a Backup of the system" and "Restoring the system from a backup" sections of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide*.

Automatic backups are executed and stored on the active blade. The automatic database backup can be set up to launch following these configurable parameters:

- Hour: hour at which the backup of subscriber profiles data will be performed.
- Minute: minutes at which the backup of subscriber profiles data will be performed.
- BackupDirectory: directory in which the backup file will be stored.
- FileRotation: number of backup files that can be stored in the directory. It is recommended that a maximum of 7 files be stored at the same time.
- IsActivated: attribute that determines if the automatic backup is activated or not. When IsActivated=On, the automatic backup is activated and when IsActivated=Off, the automatic backup is not activated.
- IncludeConfiguration: indicates whether or not the configuration data must be included in the automatic backup.

Restore from WebCI

The Restore view is used to restore database information onto the active System Controller (SC). Refer to *Figure 10: Backup/Restore Window*. A listing of the backup files can be obtained by specifying the directory name in the FromDirectory field. To restore the database, specify the file name in the FileName field.

Danger: When restoring the database on Geo-Redundant system, this operation can lead to loss of subscriber provisioning activity on system where the Geo-Redundancy was disabled for more than 4 hours. Please refer to *Geo-Cluster Configuration* for more information on Geo-Redundancy management.

Chapter 5

OAM&P

Topics:

This chapter describes how to troubleshoot problems with the OAM&P.

SNMP

The Tekelec SDM supports SNMP (Simple Network Management Protocol) to provide real time notifications to the Network Manager system. The SDM MIB (Management Information Base) is separated into two MIBs: SMI Root and System MIB.

SMI Root MIB

This MIB defines the Tekelec SMI (Structure of Management Information) root in ASN.1 format. The Tekelec root SMI specifies the top level object definition for all the Tekelec MIB modules. The Tekelec System MIB is defined under this object definition. The SMI root structure is shown below:

```
+--iso(1)
     |
    +--org(3)
         |
        +--dod(6)
             |
            +--internet(1)
                 |
                +--private(4)
                     |
                    +--enterprises(1)
                         |
                        +--blueslice(17094)
```

For the SMI Root MIB script, refer to the Machine Readable File provided.

System MIB

The System MIB provides Tekelec system level information in ASN.1 format. The trap definitions and their parameters are defined.

The bsAlarmNotificationGroup object regroups seven generic traps to raise four alarm notifications, one acknowldegement, one cleared, and one synchro.

- The bsAlarmNotificationParamGroup object contains all the parameters that define an alarm.
- The bsHeartbeatNotificationGroup contains the heartbeat notification trap.
- The bsNmAlarmSynchro object is used as a mechanism to synchronize the Network
- Manager alarms with alarms in the Tekelec managed object.

The System MIB tree is shown below.

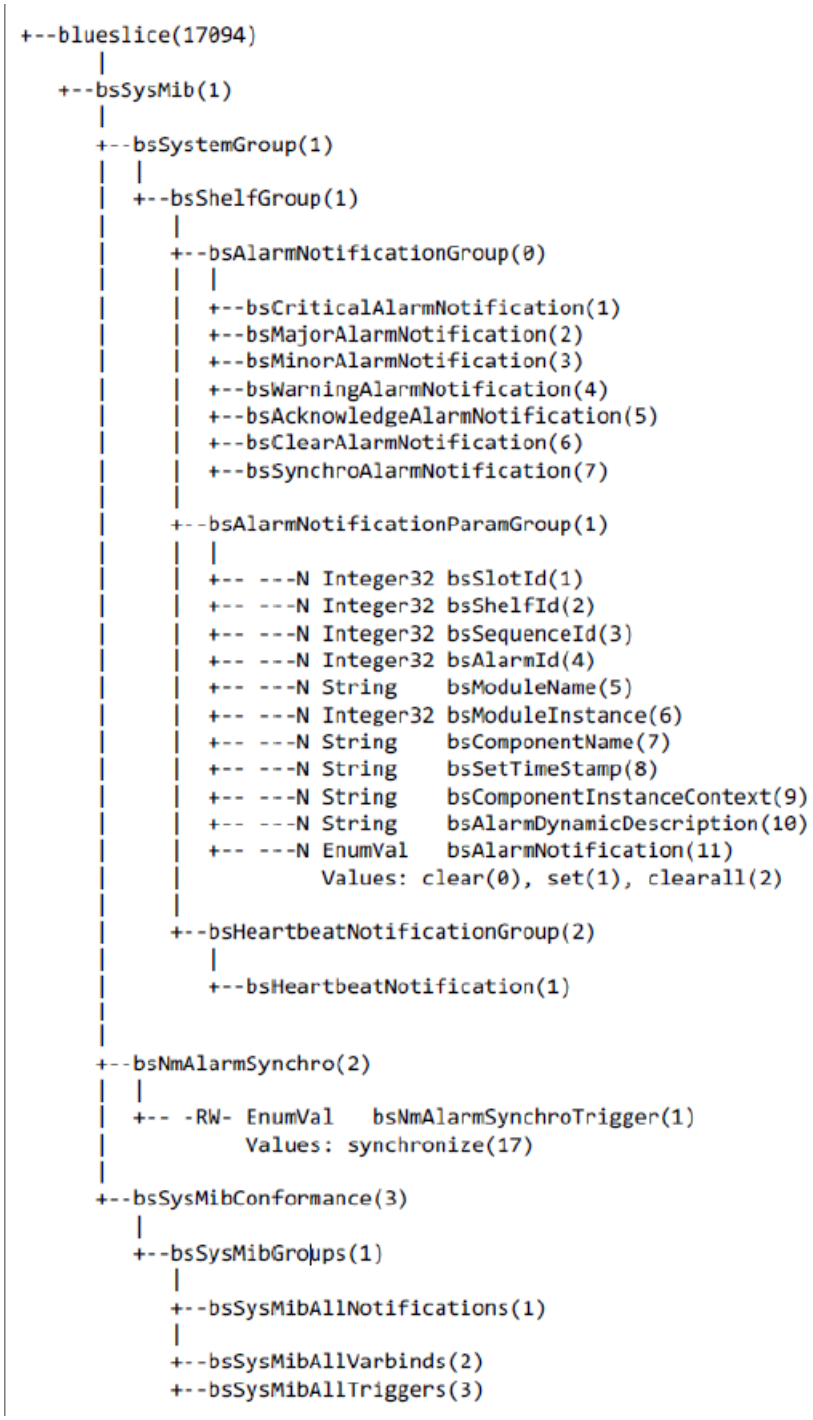


Figure 11: System MIB Structure

SNMP Object Description

SNMP Managed objects descriptions are provided as follows:

bsShelfGroup

Table 48: SNMP Object Description

Object Identifier	Description	OID
bsAlarmNotificationGroup	Generic traps container	1.3.6.1.4.1.17094.1.1.1.0
bsAlarmNotificationParamGroup	Regroups all the varbinds	1.3.6.1.4.1.17094.1.1.1.1

bsAlarmNotificationGroup

Table 49: bsAlarmNotificationGroup

Managed Object	Description	OID	Related Objects
bsCriticalAlarm Notification	Mapped to a raised critical alarm.	1.3.6.1.4.1.17094.1.1.1.0.1	bsSlotId bsShelfId bsSequenceId bsAlarmId bsModuleName bsModuleInstance bsCompnentName bsSetTimeStamp bsComponentName bsSetTimeStamp bsComponentInstanceContext bsAlarmDynamicDescription bsAlarmNotification
bsMajorAlarm Notification	Mapped to a raised major alarm.	1.3.6.1.4.1.17094.1.1.1.0.2	
bsMinorAlarm Notification	Mapped to a raised minor alarm.	1.3.6.1.4.1.17094.1.1.1.0.3	
bsWarningAlarm Notification	Mapped to a raised warning alarm.	1.3.6.1.4.1.17094.1.1.1.0.4	
bsAcknowledge AlarmNotification	Mapped to an acknowledged alarm.	1.3.6.1.4.1.17094.1.1.1.0.5	bsSequenceId*
bsClearAlarm-Notification	Mapped to a cleared alarm.	1.3.6.1.4.1.17094.1.1.1.0.6	
bsSynchroAlarm-Notification	Mapped to a reconnect.	1.3.6.1.4.1.17094.1.1.1.0.7	Not applicable.

Note: Network Manager can use the bsSequenceId as a key to find the corresponding active alarms.

bsAlarmNotificationParamGroup

Table 50: bsAlarmNotificationParamGroup

Managed Object	SNMP Type	OID
bsSlotId	Integer32	1.3.6.1.4.1.17094.1.1.1.1.1.0
bsShelfId	Integer32	1.3.6.1.4.1.17094.1.1.1.1.2.0
bsSequenceId	Integer32	1.3.6.1.4.1.17094.1.1.1.1.3.1
bsAlarmId	Integer32	1.3.6.1.4.1.17094.1.1.1.1.4.0
bsModuleName	Octet String	1.3.6.1.4.1.17094.1.1.1.1.5.0
bsModuleInstance	Integer32	1.3.6.1.4.1.17094.1.1.1.1.6.0
bsComponentName	Octet String	1.3.6.1.4.1.17094.1.1.1.1.7.0
bsSetTimeStamp	Octet String	1.3.6.1.4.1.17094.1.1.1.1.8.0
bsComponentInstanceContext	Octet String	1.3.6.1.4.1.17094.1.1.1.1.9.0
bsAlarmDynamicDescription	Octet String	1.3.6.1.4.1.17094.1.1.1.1.10.0
bsAlarmNotification	Integer (0,1)	1.3.6.1.4.1.17094.1.1.1.1.11.0

bsHeartbeatNotification

Table 51: bsHeartbeatNotification

Object Identifier	Description	OID
bsHeartbeatNotification	Contains the OID for the Heartbeat Notification	1.3.6.1.4.1.17094.1.1.1.2.1

bsNmAlarmSynchro

Table 52: bsNmAlarmSynchro

Object Identifier	Description	OID
bsNmAlarmSynchro	Contains the OID for the NM Alarm Synchronization	1.3.6.1.4.1.17094.1.2

bsNmAlarmSynchroTrigger

Table 53: bsNmAlarmSynchroTrigger

Object Identifier	SNMP Type	OID
bsNmAlarmSynchroTrigger	Integer	1.3.6.1.4.1.17094.1.2.0

For the System MIB script, refer to the Machine Readable File provided

License Manager

The Oamp folder contains the License Manager feature which provides for the management of active subscribers in the SDM. It provides tracking control on the maximum number of active and total subscribers registered on the system.

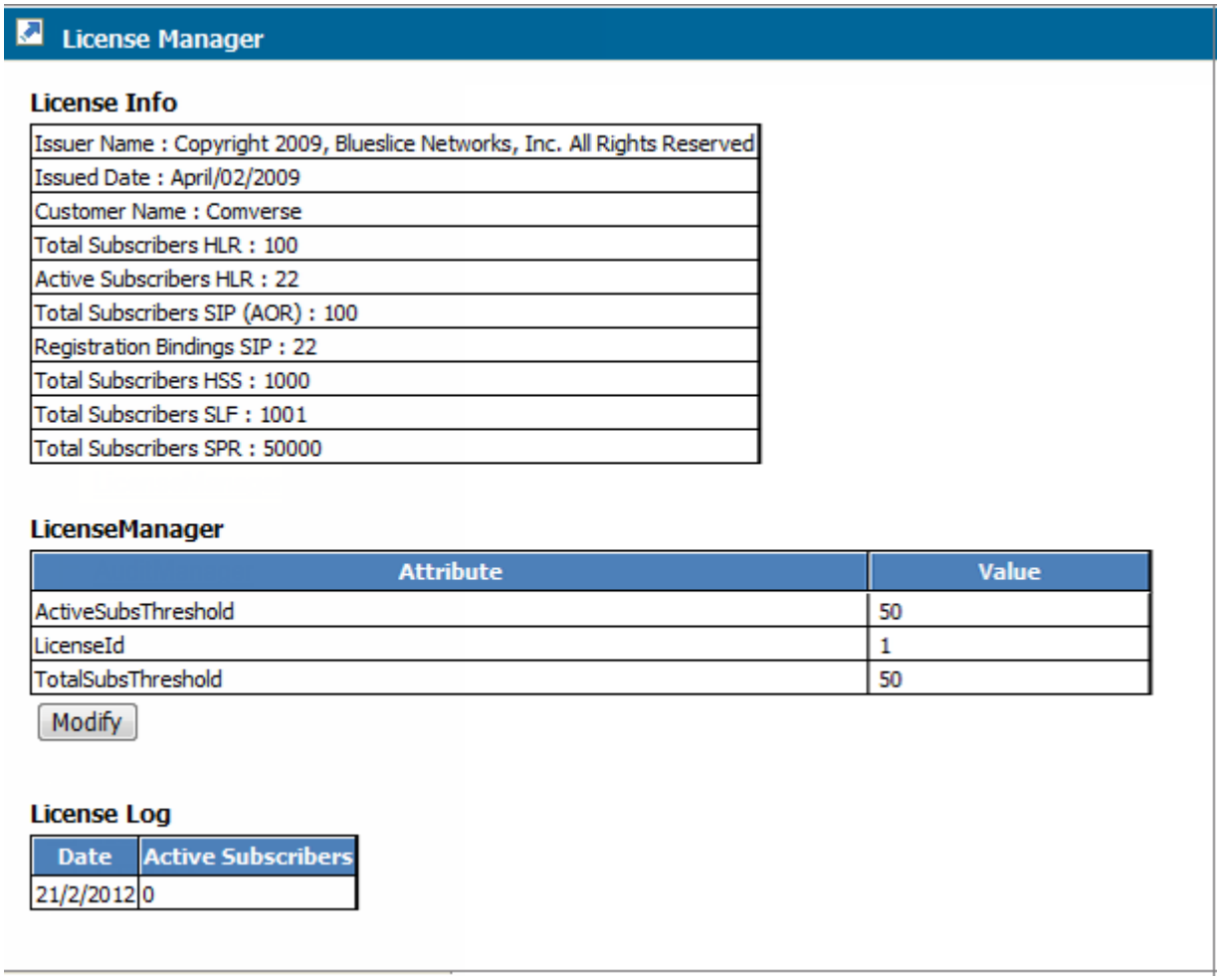


Figure 12: License Manager

The License Info table provides information on the Issuer name and date, customer name, and number of active subscribers and total subscribers permitted with the license. The License Manager table displays the License Id, Active Subscriber threshold value, and Total Subscriber threshold.

Threshold values are expressed as a percentage (default = 50%). The Total-Subscriber-Threshold alarm is evaluated in the following conditions:

1. At system start up
2. When the license is updated
3. When a new subscriber is provisioned
4. When a subscriber is deleted.

When the number of subscribers reaches the threshold, it will trigger a warning alarm. When the number of subscribers exceed the maximum, it will trigger a critical alarm. The threshold values may also be modified from this table. The License Log table provides the date and total number of subscribers that were active during that month.

The License Manager generates a license log at the beginning of each month and updates the timestamp and the number of active HLR subscribers on a daily basis. At the end of each calendar month, there is a license log that indicates the total number of subscribers that were active during that month. The 12 most recent logs are kept in history.

License Manager Operations

This section describes the operations that can be used to display the License and log information from the CLI.

DisplayLicense()

This operation will retrieve and display the License information.

Command syntax:

```
:Oamp[]:OampManager[]:LicenseManager[LicenseId = 6]> DisplayLicense()
```

DisplayLicenseLog()

This operation will retrieve and display the License log information. The License Manager generates a license log at the beginning of each month and updates the timestamp and the number of active HLR subscribers on a daily basis. At the end of each calendar month, there is a license log that indicates the total number of subscribers that were active during that month. The 12 most recent logs are kept in history.

Command syntax:

```
:Oamp[]:OampManager[]:LicenseManager[LicenseId = 6]> DisplayLicenseLog()
```

Oamp Manager

Template Management

The Oamp folder contains the Oamp Manager sub-folder which provides information on the disk space allocated in the database for the template requests and which also allows to define the maximum total size (in bytes) the template requests can reach.

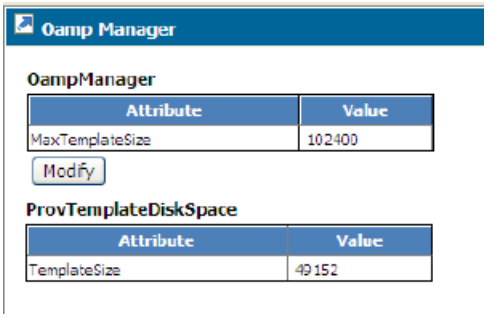


Figure 13: Oamp Manager

This section describes the OampManager and ProvTemplateDiskSpace entities and their parameters:

Oamp Manager

Name
`OampManager`

Description

This entity can be used by the operator to set the template requests size restriction by defining the maximum total size (in bytes) the template requests can reach.

CLI Navigation
`Oamp[]> OampManager`

CLI Inherited Attributes

None

CLI Command Syntax
`Oamp[]> display OampManager [MaxTemplateSize= int]`

Operations Permitted

`Display, Modify.`

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Table 9: Predefined access permissions to services per user group* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 54: Oamp Manager Mandatory Attributes

Attribute	Value Range	Default	Description
MaxTemplateSize	Suggested value range: **48 KB<MaxTemplateSize<2Gbytes**	N/A	This parameter allows the operator to set a size restriction (in bytes) for all the template requests. If this parameter is provisioned with a value of zero, it is turned off and there is no size control restriction for the provisioning template requests.

CLI Example
Oamp[]> display OampManager[]

Prov Template Disk Space

Name
ProvTemplateDiskSpace

Description

This entity can be used by the operator to view the disk space allocated in the database for the template requests.

CLI Navigation
Oamp[]> ProvTemplateDiskSpace

CLI Inherited Attributes

None

CLI Command Syntax
Oamp[]> display ProvTemplateDiskSpace [TemplateSize= int]

Operations Permitted

Display.

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Table 9: Predefined access permissions to services per user group* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 55: Prov Template Disk Space Mandatory Attributes

Attribute	Value Range	Default	Description
TemplateSize	**Int** (bytes)	N/A	This parameter indicates the size in bytes that has been allocated for the template requests. The disk space allocation is done in blocks of bytes, with an initial allocation of a 48 KB block and with an allocation of a 32 KB block each time more space is needed. This means that this parameter doesn't give the exact size in bytes occupied by the template requests, but the disk space occupied by the blocks (in bytes) that have been allocated for the template requests, depending on their total size.

CLI Example

```
Oamp[]>display ProvTemplateDiskSpace []
```

Audit Log File Management

Prior to enabling the audit log files to be generated, the different management options must first be configured in the AuditManager entity. This section provides a description of this AuditManager entity.

For more details on how to provision this entity, refer to the "Configuring Audit log files management options" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide*.

Audit Manager

Name

AuditManager

Description

This entity can be used by the operator to configure (prior to enabling the Audit log files (StartAudit()):

- The Audit log message format (CSV or XML)
- The number of days that the old audit log files must be kept in the /export/audit directory.
- The debug information request in order to request the following debug information to be included in each audit line: slot, module, file and line. By default, this debug information is not included.

CLI Navigation

```
Oamp[]> AuditManager
```

CLI Inherited Attributes

None

Command Syntax in the CLI

```
Oamp[]> display AuditManager []
```

Operations Permitted

```
Display, Modify.
```

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Table 9: Predefined access permissions to services per user group* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 56: Audit Manager Optional Attributes

Attribute	Value Range	Default	Description
AuditFormat	**0** (CSV) **1** (XML)	**0** (CSV)	This parameter allows the operator to set the format in which the system writes and stores the audit log files in.
AuditHistory	**integer**	**7**	The number of days that the old audit log files must be kept in the /export/audit directory.
AuditDebug	**0 or 1**	**0**	This parameter allows the Network Operator to request the following debug information to be included in each audit line: slot, module, file and line.

Attribute	Value Range	Default	Description
			0: the debug information is not requested to be included in the audit files. 1: the debug information is requested to be included in the audit files.

CLI Example

```
Oamp[]> display AuditManager[]
```

Audit Information

Name

AuditInfo

Description

This entity can be used by the operator to enable/disable for logs to be generated on a per audit component basis.

CLI Navigation

```
Oamp[]> AuditManager> AuditInfo
```

CLI Inherited Attributes

None

Command Syntax in the CLI

```
Oamp[]> AuditManager []> display AuditInfo []
```

Operations Permitted

Display, Modify.

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Table 9: Predefined access permissions to services per user group* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 57: Audit Info Mandatory Attributes

Attribute	Value Range	Default	Description
AuditId	**40000** (AaaIp)	N/A	Identification of the Audit Component. In the current release, the only audit component supported is the AaaIp component.

Table 58: Audit Info Optional Attributes

Attribute	Value Range	Default	Description
AuditHistory	**integer**	**7**	The number of days that the old audit log files must be kept in the /export/audit directory.
AuditStatus	**1** (Enable) **2** (Disable)	**2** (Disable)	This parameter allows the Network Operator to enable/disable the generation of logs for a specific audit component. 1: the generation of logs for the AuditId specified is enabled and when starting the Audit (StartAudit()), logs will be generated for this audit component. 2: the generation of logs for the AuditId specified is disabled. Even if the StartAudit() operation is performed, no logs will be generated for this audit component.

CLI Example

```
Oamp[]> AuditManager[]>display AuditInfo []
```

Audit Operations

This section describes the operations that can be used to start/stop the audit logging mechanism from the CLI.

StartAudit()

This operation will start the audit logging mechanism.

Requirements: Prior to executing this operation for a specific audit component, the audit logging options must have already been configured and the AuditInfo's AuditStatus attribute must be set to 'Enable' for that audit component. For instructions on the steps that need to be followed prior to executing this operation, refer to the "Configuring and Enabling/Disabling Audit Logging" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide*.

Command syntax:

```
Oamp[]:AuditManager[]:AuditInfo[AuditId = 40000]>StartAudit()
```

StopAudit()

This operation will stop the audit logging mechanism.

Requirements: Prior to executing this operation, you must disable the audit logging set per IP address pool. To achieve this, you must set the AAAAddressAllocationPolicy's AuditLoggingEnabled parameter to 'Disable'. Refer to the "Configuring Address Allocation Policies and IP address pools" section of the *SDM System Configuration – User Guide* for instructions on how to modify the AAAAddressAllocationPolicy entity.

Command syntax:

```
Oamp[]:AuditManager[]:AuditInfo[AuditId = 40000]> StopAudit()
```

Accessing Logs and Traces

Logs

Log messages are generated whenever an action or event occurs on the system. Logs provide operators with an additional level of information and allow them to verify correct operation of the SDM. Log files can be viewed by all users by accessing the system through the SSH client.

System log messages are displayed in real time and reflect system activity as it occurs. The log files are generated for the current day and stored in a directory. Log files are rotated every night at 0:00 hours and are kept for a period of seven days.

The operator can:

- Save log files (i.e., historical log files)
- View logs
  - Current log file (current.xml)
  - Previous log files (/blue/var/log – days of week)

Traces

All of the events with Trace and Trace Error levels are called traces.

If requested by the Customer Care Center during troubleshooting, the operator can:

View traces through the CLI by accessing the /blue/var/trace directory. For more details on how to access traces, please refer to the 'Accessing traces' section in the *SDM Monitoring, Maintaining, Troubleshooting-User Guide.*

It is very important to note that traces are managed by Tekelec and so the Customer Care Center must always be contacted first before troubleshooting with traces. The Customer Care Center will then be able to guide you and provide you with the correct analysis using the traces.

The system offers the Customer Care Center the ability to manage traces by performing the following through the CLI:

Accessing Traces from the blade where the application concerned is running by accessing the `/blue/var/trace` directory. The trace file name includes the time of the last trace in the file. The traces are stored in a set of files per process with a rotation schedule. The rotation is based on the maximum number of trace files, which are 100. The oldest trace file will be replaced with the newest file. Each trace file can contain up to 50000 trace lines.

The Traces are stored in a text format. Additional information about the component is also included in the traces. A trace includes the following information:

```
Time:
    This is the local time in format "Tue Nov 11 2008 09:44:49:530489
(microseconds)".
Level:
    This is the event level or also called severity.
File:
    This is the originating source file name.
Line:
    This is the originating line number in the source file.
Slot Identification:
    This is the chassis slot identification
Thread:
    The thread identification within the process
Module:
    the Module name (extracted from the Module Identity)
Component:
    This is an optional trace parameter used for filtering.
Description:
    This is the text that is given with the trace.
```

Example:

```
[Fri Dec 19 2008 16:36:31:106534][Slot:5][bHlrSS7Main.cc(130)][HlrServer(HLR_INF
O)][Tid:4115138240][DEBUG]
          ->HlrSS7 main : Instantiating HlrSS7Mng
```

Activate/Deactivate traces for each module (i.e., process) of the system. This allows the Tekelec technicians to display or not a module's traces by executing the StartTrace(), StopTrace() operations through CLI. When the trace is activated for a module, all the log events (i.e. from Info level and up) are also stored in the trace file of that module. This helps to correlate events that occurred in time line by ordering all the events in one file.

Filter on components for a given module (i.e., process). With this filtering option, only specific traces can be displayed rather than the set of traces available for that process. By default, when activating the traces for a given module, all traces are produced. In order to reduce the number of traces produced, the Customer Care Center can add filter specific components so that only traces about these components will be produced. Filtered Traces are activated per module (for the entire process) and by component. A list of filter specific components is predefined in the system for each module type. The following two operations can be executed by the Tekelec technicians in order to perform such filtering:

- AddFilterComponent ()
- RemoveFilterComponent()

Accessing Stored Log Files

The stored log files can be viewed by accessing the specific System Controller (SC) card.

The current day logs are stored in an XML file named current.xml located in the directory: `/blue/var/log.`

Log files are rotated every night at 0:00 hours and are stored for a period of 7 days. Previous logs are stored in files named with the days of the week in the directory: `/blue/var/log`. (e.g., `monday_20060320_000001, tuesday_20060321_000003,` ...) The file contents can be displayed by invoking the vi editor. Alternatively, typing: more filename will display the file contents one page at a time.

Audit Log Files

The Logging of IP address allocation feature generates logs for the allocation and de-allocation of IP addresses done by the AAA, for selected address pools.

These logs are written into audit files which can be found on each of the System Controller blades (active and standby) under the following directory: `/export/audit`.

Each log message consists of the following pieces of information:

- Timestamp: the time at which the allocation/deallocation was performed
- Pool Name: the address pool name associated with the IP address
- MSISDN: the MSISDN to which the IP address is assigned
- IP Address: the address which was allocated or deallocated

Event: a two-letter code describing the action which was performed. Hereunder is the list of event codes that can be generated.

Note: There are several OAMP operations that may cause the de-allocation of an IP address as a side-effect, these are enumerated as D1, D2,D3,D4 and D5.

Table 59: Audit Log Event Files

EVENT CODE	EVENT DESCRIPTION
AD	Allocation of a dynamic IP address as a result of an access-request message.
AS	Allocation of a static IP address as a result of an access-request message.
DS	Deallocation of an IP address as a result of an accounting-request (stop) message.
DT	Deallocation of an IP address by the AAA due to a timeout.
D1	Deallocation of an IP address as a result of a ClearAddresses operation.
D2	Deallocation of an IP address as a result of the deletion of an Address Pool Range.
D3	Deallocation of an IP address as a result of the update of an Address Pool Range.
D4	Deallocation of an IP address as a result of a DisconnectNAS operation.
D5	Deallocation of an IP address as a result of a DisconnectUser operation.

The audit files are classified into two categories:

- The current audit file. Format: <Audit Component>.<Extension>
- The previous audit file. Format: <Audit Component>-<Timestamp>.<Extension>

The Audit Component represents the information which is audited, ex: AaaIp. The timestamp represents the time when the audit file is created and has the format yyyymmddhhmmss. The file extension represents the audit data format, which can be: csv (comma-separated values) or xml (Extensible Markup Language).

Examples of previous audit file names:

- *AaaIp-20091113150033.csv*
- *AaaIp-20091113150033.xml*

Examples of current audit file names:

- AaaIp.csv
- AaaIp.xml

Audit file content examples :

- CSV format :
  - *20091113150444,pool-poc,123456789,127.0.0.1,AD*
  - 20091113150445,pool-poc,123456789,127.0.0.1,AD
  - 20091113150446,pool-poc,123456789,127.0.0.1,AD
  - 20091113150447,pool-poc,123456789,127.0.0.1,AD
  - 20091113150448,pool-poc,123456789,127.0.0.1,AD

XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type='text/xsl' href='logs.xslt'?>
<audits xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="logfile.xsd">
```

```
 <audit><tm value='20091116084855' /><pool value='pool-poc' /><msisdn
value='123456789' /><ip value='127.0.0.1' /><event value='AD' /></audit>
 <audit><tm value='20091116084856' /><pool value='pool-poc' /><msisdn
value='123456789' /><ip value='127.0.0.1' /><event value='AD' /></audit>
 <audit><tm value='20091116084857' /><pool value='pool-poc' /><msisdn
value='123456789' /><ip value='127.0.0.1' /><event value='AD' /></audit>
 <audit><tm value='20091116084858' /><pool value='pool-poc' /><msisdn
value='123456789' /><ip value='127.0.0.1' /><event value='AD' /></audit>
 <audit><tm value='20091116084859' /><pool value='pool-poc' /><msisdn
value='123456789' /><ip value='127.0.0.1' /><event value='AD' /></audit>
</audits>
```

The audit files are also rotated when the following triggers are met:

- The daily time has reached midnight.
- The audit file contains more than 100 000 lines.

The old audit file cleanup will be done on a daily basis at midnight based on the configurable number of history days set by the Network Operator through a Tekelec Interface. In the case of multiple audits, the cleanup is done per audit component.

The following has been implemented in the database in order to allow the Network Operator to manage the audit files (prior to starting them) through the Tekelec Interfaces:

The new AuditManager entity has been implemented to allow the Network Operator to configure:

- The Audit log message format (CSV or XML)
- The number of days that the old audit log files must be kept in the /export/audit directory.
- The debug information request in order to request the following debug information to be included in each audit line: slot, module, file and line. By default, this debug information is not included.

For more details on how to configure and enable/disable the audit loggings per audit component, refer to the “Configuring and Enabling/Disabling Audit loggings” section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide.*

The newly implemented StartAudit() and StopAudit() operations allow the Network Operator to start/stop an audit component dynamically (with no system restart). When an audit component is started, a new current audit file is created under /export/audit (on both SC). And when an audit component is stopped, the current audit file will be renamed to old audit file, so that the external tools can connect and get all the audit files during audit period. The operator must be careful when activating the audit logging feature because the performance impact will be on the blades where applications are running and also on both SCs.

In addition to being able to turn on or off the generation of audit files on a global level, the AuditLoggingEnabled flag has been implemented in the AAAAddressAllocationPolicy entity in order to allow the Network Operator to enable/disable this feature on a per-pool basis. In other words, this flag determines whether or not the logs will be generated for the IP addresses associated with the pool.

LTE-HSS Log File

An LTE-HSS message notification is added to a log file when certain types of diameter messages are received by the LTE-HSS. The log event is stored as a line which is added to the log. The log file is in

CSV (comma-separated values) format. Each log file event contains the following mandatory information:

- The local timestamp
- The request type code
- The MME/SGSN hostname
- The diameter result code number
- The IMSI

Depending on the diameter message additional optional information is included:

Diameter Message Type	Optional Information
Location Update Request	• Visited PLMN ID • MSISDN • IMEI
Authentication Information Request	• Visited PLMN ID • Requested Authentication
Notify Request	Alert reason
Cancel Location Request	Cancellation type: • MME_UPDATE_PROCEDURE=0 • SGSN_UPDATE_PROCEDURE=1 • SUBSCRIPTION_WITHDRAWAL=2 • INITIAL_ATTACH_PROCEDURE=4

Empty parameters are represented by a null character between two commas. (,,).

LTE-HSS log files are stored on the front end blade of the LTE-HSS under the following directory: `/blue/var/log/csv`. They are classified into two categories:

- The current LTE-HSS log file. Format: <filename>.<extension>
- The previous LTE-HSS log file. Format: <filename>.<timestamp>.<extension>

The filename is lteHSSCaleaLogs. The timestamp represents the time that the file was created and is in the format yyyymmdd_HHhMMmSSs. The file extension represents the data format. It is CSV (comma-separated values).

Example of the current log file name:

- lteHSSCaleaLogs.csv

Example of a previous log file name:

- lteHSSCaleaLogs.20120926_23h30m12s.csv

Each LTE-HSS log file displays information in the following order:

- The local timestamp
- The request type code
- The MME/SGSN hostname
- The diameter result code number
- The IMSI

- The visited PLMN ID or Alert reason or Cancellation type
- The MSISDN or Requested Authentication
- The IMEI

Example of CSV format log file:

```
2013-04-17 13:17:20,316,mmeA.lte.blueslice.com,2001,320910421000100,05F613,
15141111111,
2013-04-18 16:20:34,316,mmeA.lte.blueslice.com,2001,320910421000100,05F613,
15141111111,
2013-04-18 17:21:55,318,mmeA.lte.blueslice.com,2001,320910421000100,05F613,
EUTRAN
2013-04-18 17:22:29,316,mmeA.lte.blueslice.com,2001,320910421000100,05F613,
15141111111,
2013-04-18 17:22:32,317,mmeA.lte.blueslice.com,,320910421000100,0
2013-04-18 17:24:00,321,mmeA.lte.blueslice.com,2001,320910421000100
```

The log files are rotated when the following triggers are met:

- The time is 0130
- The number of lines has reached 500,000

The old lteHSSCaleaLog file cleanup is done at 0130 each day or when the maximum number of lines has been reached. Log files are stored in `/blue/var/log/csv` for seven days. After 7 days of storage the log files are erased.

VLR Message Notifications Log File

A VLR message notification is added to a log file when a MAP message is received from the VLR. The notification is in the form of a line which is added to the log. The log file is in CSV (comma-separated values) format. Each log file notification contains the following information:

- The “displayed” MSISDN of the subscriber
- The registered IMSI of the subscriber
- The global title (e.164) address of the node that sent the message (VLR or SGSN)
- The type of message received (UL, UL_GPRS, SAI, ReadySM, PurgeMS or CL)
- The local timestamp (format: YYYY-MM-DD HH:MM:SS)
- The MSC e164 address
- The Alert Reason
- The Result. This indicates if the message was executed successfully or not. In the event of a failure, the error code is included:
  - 0 = Success
  - Error code given for other items
- The SourceSSN. This indicates the subsystem number associated with the source node, if it can be determined from the message type. It is one of the following values:
  - 0 = unknown (set if message is not UL or UL-GPRS)
  - 7 = VLR (only set if message type is UL)
  - 149 = SGSN (only set if message type is UL-GPRS)

Empty parameters are represented by a null character between two commas. (,,).

VLR message notification log files are stored on the blade running the Hlr service under the following directory: `/blue/var/log/csv`. They are classified into two categories:

- The current VLR message notification file. Format: <filename>.<extension>
- The previous VLR message notification file. Format: <filename>.<timestamp>.<extension>

The filename is VlrMessageNotification. The timestamp represents the time that the file was created and is in the format yyyymmdd_HHhMMmSSs. The file extension represents the data format. It is CSV (comma-separated values).

Example of the current log file name:

- VlrMessageNotification.csv

Example of a previous log file name:

- VlrMessageNotification.20120926_23h30m12s.csv

Example of CSV format log file:

```
15634210100,310910421000100,15634110002,UL,2012-09-12
15:43:00,15634110002,,0,715634210100,310910421000100,15634110002,ReadySM,2012-09-12
 15:43:07,,1,0,015634210100,310910421000100,15634110002,PurgeMS,2012-09-12
15:43:14,,,0,015634210100,310910421000100,15634110002,UL_GPRS,2012-09-12
15:47:04,,,0,14915634210100,310910421000100,15634110002,SAI,2012-09-12
15:47:38,,,0,0310910421000218,,UL_GPRS,2012-09-12
17:31:09,,,1,149310910421000219,,SAI,2012-09-12 17:31:09,,,1,
310910421000100,,CL,2012-09-13 10:55:00,,,0,0
310910421000100,15634110003,CL,2012-09-13 12:53:39,,,0,0
15634210100,310910421000100,15634110002,UL,2012-09-13 12:53:39,15634110004,,0,7
,310910421000100,,CL,2012-09-13 10:55:00,,,0,0
```

The default is to have no header. An optional header can be added.

The log files are rotated when the following triggers are met:

- The time is midnight
- The number of lines has reached 500,000

The old VlrMessageNotification log file cleanup is done at midnight each day or when the maximum number of lines has been reached. Log files are stored in `/blue/var/log/csv` for seven days. After 7 days of storage the log files are erased.

SPR provisioning logs

The SPR Provisioning Log feature records all provisioning requests and retrieval attempts processed by the SPR. Processed information includes subscriber, pool, quota, state, and other related data. Both functions, the logging of provisioning events and the logging of retrieval events, can be enabled independently.

The provisioning requests can be received from either of these interfaces: CLI, WebCI, XML-TCP (Direct XML), XML-SOAP, or XML-REST (MSR API).

Request types include create, modify, delete, and retrieve, where the command name for these requests depends on the provisioning interface used.

Each log event creates a new line in the log file and contains the following mandatory information:

- Date and time of transaction in system time format
- Source that initiated the transaction
  - IP address (XML-REST)
  - User name (other provisioning interfaces)
- Action requested (create/modify/delete/retrieve)
- Key of the affected subscriber (MSISDN, IMSI, or NAI)
- Command parameters(all values to be inserted, modified, deleted, or retrieved)
- Result code (success, failure, or other error codes as needed)

The log captures command parameters in the XML format in which they were received. For XML-REST, the log also captures the URL. The log represents an empty parameter by a null character between two commas (,,).

SPR log files are stored on the server associated with the provisioning interface. The maximum file size is 10MB. The files can be retrieved in CSV (comma-separated values) format from this directory: `/blue/var/log/csv`. The files can also be retrieved by SCP/SFTP protocol to an external server.

The current log file uses the <filename>.<extension> format, for example, `provlog.csv`. The previous files use the <filename>.<timestamp>.<extension> format, for example, `provlog.20131024_15h54m30s.csv`. The rotation queue size is configurable and can contain a maximum of 10 files. Rotation occurs when the number of log files exceeds the configured number.

The following SPR provisioning log entry is the result of an XML-REST request by IP address 10.15.34.64 to create (INSERT) a pool profile with pool Id 10000. The request includes pool parameters and their respective value. The zero after the comma at the end of the line indicates the result code, where zero indicates success.

```
2013-12-17 09:48:37,10.15.34.64,INSERT,10000,<?xml version="1.0"
encoding="UTF-8"?><pool><field name="BillingDay">1</field><field
name="Entitlement">Daypass</field><field name="Entitlement">Weekpass</field><field
 name="Tier">12</field><field name="Custom15">allo</field><field
name="PoolID">10000</field></pool>,0
```

For a request created in CLI, WebCI, or XML (TCP or SOAP), the IP address is replaced with the user name. The following log entry uses the user name "admin" instead of an IP address:

```
2013-12-17 09:49:48,admin,INSERT,20000,<?xml version="1.0"
encoding="UTF-8"?><pool><field name="PoolID">20000</field><field
name="BillingDay">0</field></pool>,0
```

This is an example of a REST request of a subscriber profile which includes a number of custom fields:

```
2014-02-24 17:23:21,10.15.60.145,INSERT,1,<?xml version="1.0"
encoding="UTF-8"?><subscriber><field name="MSISDN">1</field>
<field name="AccountId">1</field><field name="BillingDay">2</field>
<field name="Entitlement">Daypass</field><field name="Entitlement">Weekpass
</field><field name="Tier">12</field><field name="Custom11">
allo</field><field name="Custom12">allo1</field>
<field name="Custom13">allo2</field></subscriber>,0
```

This is an example of a SOAP request of a subscriber profile which includes a number of custom fields:

```
2014-02-24 17:28:38,admin,INSERT,1,<?xml version="1.0"
encoding="UTF-8"?><subscriber><field name="MSISDN">1</field>
<field name="BillingDay">1</field><field name="Entitlement">1</field>
```

```
<field name="Entitlement">14</field><field name="Entitlement">2</field>
<field name="Tier">Postpaid</field><field name="Custom15">allo1</field>
</subscriber>,0
```

This is an example which shows the update to a quota:

```
2014-02-24 17:32:40,10.15.60.145,UPDATE,1,<?xml version="1.0"
encoding="UTF-8"?><subscriber><field name="Quota"><![CDATA[<?xml version="1.0"
encoding="UTF-8"?><usage><version>1</version><quota
name="q1"><cid>9223372036854775807
</cid><time>1234</time><totalVolume>99999999999</totalVolume><inputvolume>5000
</inputvolume><outputvolume>15000</outputvolume><servicespecific>12</servicespecific>
<nextresettime>2010-05-12T16:00:00-05:00</nextresettime></quota><quota name="q12">
<cid>9223372036854775807</cid><time>1234</time><totalvolume>10</totalvolume>
<inputvolume>10</inputvolume><outputvolume>10</outputvolume><servicespecific>yes
</servicespecific><nextresettime>2010-05-12T16:00:00-05:00</nextresettime><type>
yes</type><grantedtotalvolume>10</grantedtotalvolume><grantedinputvolume>10
</grantedinputvolume><grantedoutputvolume>10</grantedoutputvolume><grantedtime>
</grantedtime><grantedservicespecific></grantedservicespecific><quotastate>
Valid/Inactive</quotastate><refinstanceid>1</refinstanceid></quota></usage>]]>
</field><field name="BillingDay"><![CDATA[0]]></field></subscriber>,0
```

Software Version

System Prompt

To determine which software version is running on the Tekelec SDM system, log in to the system controller card with a login name and password.

At the system prompt, type

`# BlueVersion`

The system will provide release information similar to the following:

```
* Tekelec version: 3.1.00(6080100_LNX_3_1_REL)_LOAD_BUILD
```

The number

```
3.1.00
```

is the software version number. The text

```
6080100_LNX_3_1
```

indicates the load build number.

CLI

From any navigation level within the CLI, at the system prompt `:>` type **version** to get the software release information.

WebCI

In the WebCI System Application folder, the software version is shown in the Shelf Inventory view. The software version and Load build is displayed at the bottom of the screen.

Active Host Name Indication

Active Host Name

To get the name of the active host on the shelf, run the following operation:

```
:Oamp[]:OampManager[]> GetActiveOampHostName ()
```

Chapter 6

System

Topics:

This chapter provides an overview of the system hierarchy and describes the entities that retrieve alarms and provision system features.

System hierarchy

The following figure provides a hierarchical view of the System entities.

Note: Lower level entities inherit key attributes from higher level entities. Attributes are shown in brackets.

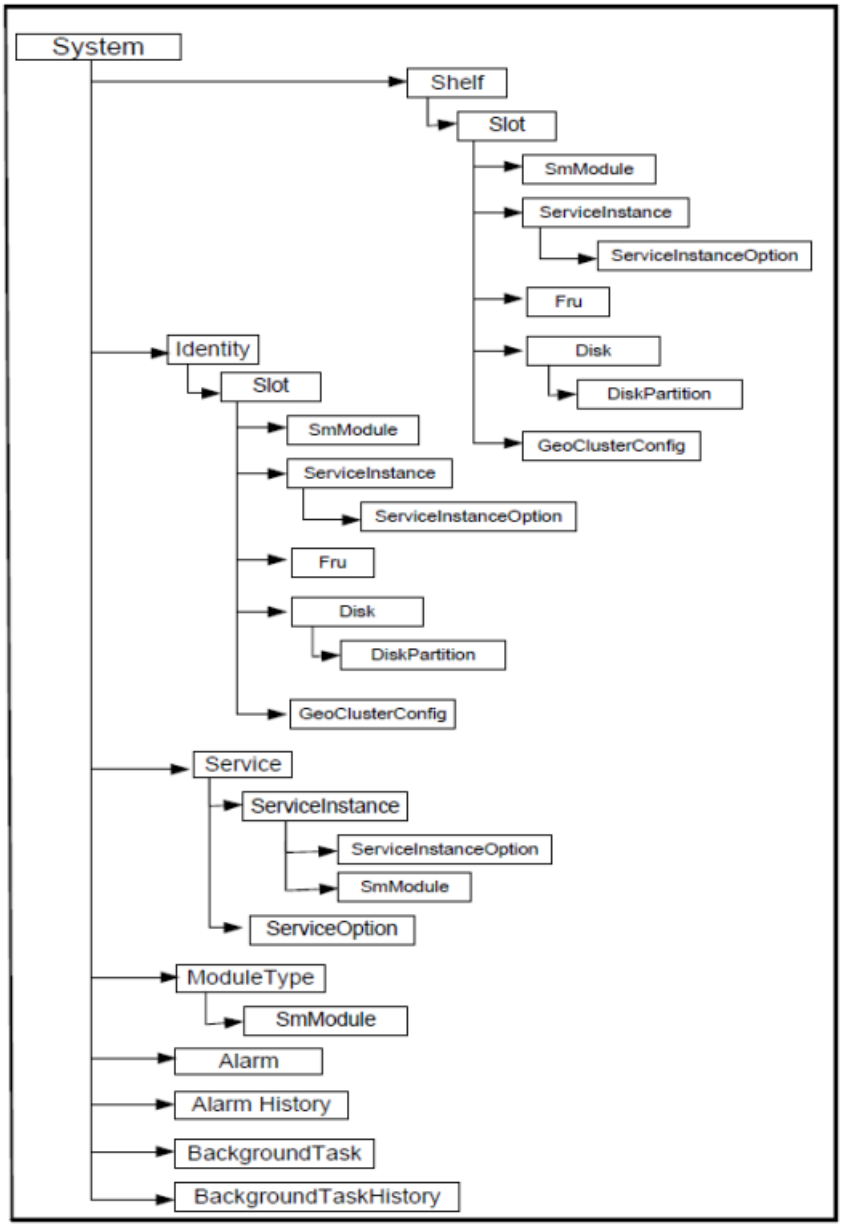


Figure 14: Hierarchy Of System CLI Commands

Shelf

Name

Shelf

Description

This represents the physical shelf.

CLI Navigation

System[]->Shelf

CLI Inherited Attributes

None

CLI Command Syntax

```
System[]> display Shelf[ShelfId = integer; Name = text; Description = text;
Location = text; Contact = text; PrivateOampVip=IP Address;
SnmpRWCommunity=string; SnmpAgentPort=0-65535; SnmpHeartbeatEnabled=0,1;
SnmpHeartbeatTime=30-240]
```

Operations Permitted

```
Display
```

Attributes and Values

Table 60: Shelf Mandatory Attributes

Attribute	Value Range	Default	Description
ShelfId	1 to 4294976295	N/A	Read only. The Shelf Id number assigned by system.
Name	Up to 65535 digits and/or letters	SDM	User defined name for the shelf.
Description	Up to 65535 digits and/or letters	Shelf	User defined description of application for the shelf.
Location	Up to 65535 digits and/or letters	Null	User defined location description for the shelf.
Contact	Up to 65535 digits and/or letters	info@blueslice.com	User defined contact name for the shelf. Shelf support contact info.

Table 61: Shelf Optional Attributes

Attribute	Value Range	Default	Description
PrivateOampVip	IP address		Internal IP address used by Tekelec applications to reach the Oamp.
SnmpRWCommunity	String	Blue	This parameter indicates the community for get/set.
SnmpAgentPort	0 to 65 535	161*	This parameter indicates the UDP port for the SNMP agent. **Warning:** The TPD SNMP Agent uses the "161" port, so for a SDM deployment running the TPD (Tekelec Software Platform), this parameter must be set to any value other than "161". We recommend using port "62008" instead of "161" on TPD installations.
SnmpHeartbeatEnabled	Bool 0 or 1	0	This parameter enables or disables the heartbeat notifications sent by the Tekelec SDM's SNMP Agent to the external Network Manager. 0: The SNMP Heartbeat Notification trap is disabled. 1: The SNMP Heartbeat Notification trap is enabled.
SnmpHeartbeatTime	30 to 240	30	Heartbeat frequency. Frequency in seconds at which the heartbeat notification traps are sent out to the Network Manager (NM). The SNMP heartbeat notification trap is sent to the NM on each

Attribute	Value Range	Default	Description
			heartbeat internal notification.

CLI Example

1 :System[]:Shelf[ShelfId = 1]> display

Shelf Operations

The following section provides a description of the operations that can be performed with the Shelf entity in the system.

AcknowledgeAllAlarms()

The operator can use this to acknowledge all the alarms on the system. An acknowledge notification with a date and time stamp will be recorded in the AlarmHistory for all the alarms. The acknowledge operation does not clear the alarms.

CLI Command Syntax:

System[]> AcknowledgeAllAlarms()

ClearAllAlarms()

Caution: The operator must be careful with this operation. This operation will remove all the alarms from the active alarm list. Updated alarm entries will appear in the AlarmHistory list. Even though the alarms have been cleared from the active alarm list, the conditions that caused the alarms still exist but will NOT be reported when these conditions no longer prevail. The AcknowledgeAllAlarms operation must be run first before running the ClearAllAlarms operation.

CLI Command Syntax:

System[]>ClearAllAlarms()

AddVip

The operator can use this operation to configure the public OAMP VIP(s) of the system. For a system using one IP connection to communicate with a single network, only the VIP of type OAMP needs to be configured. On the other hand, for a system using more than one IP connection to communicate with multiple networks (using the IP Subnet Separation feature), a VIP address of type OAMP must be configured on the ACCESS network as well as a VIP address per network. In this case, each network is organized per traffic type and a VIP must be configured per type. This operation can be used to bind one or more Vips to the shelf of the system. Note that only one VIP address can be bind at a time and only one VIP can be created per VipType. The Netmask and the VIP address as well as the VIP Type must be specified to run this operation. (as an example: Netmask: 255.255.255.0, Vip: *192.168.130.201* and *VipType: Oamp*)

Values VipType can have:

0 Default

1 Oamp

2 GeoReplication

3 Provisioning

CLI Command Syntax:

System[]>Shelf[ShelfId=1]> AddVip() Netmask=255.255.255.0; Vip=192.168.130.201; VipType=1

Note: Only one Vip per VipType can be bind to the system.

RemoveVip()

The operator can use this operation to remove a public VIP already configured in the system. Note that only one VIP can be removed at a time.

Warning: Removing a VIP will terminate all communication to this VIP. The VIP address must be specified to run this operation. (as an example: Vip:*192.168.130.201*)

CLI Command Syntax:

System[]>Shelf[ShelfId=1]> RemoveVip() Vip=192.168.130.201

AddVip

By default, no trap hosts are configured in the system. This operation allows the Network Operator to configure one SNMP trap host at a time. Multiple trap hosts can be configured in the system, simply by executing this operation for each trap host to be configured. The SnmpTrapHost parameter is the only mandatory parameter when executing this operation. The default values of the SnmpTrapPort and SnmpTrapCommunity are "162" and "public" respectively.

CLI Command Syntax:

System[]>Shelf[ShelfId=1]> AddSnmpTrapConfig() SnmpTrapHost=localhost

RemoveSnmpTrapConfig

This operation allows the Network Operator to remove one SNMP trap host at a time. The mandatory parameters are: SnmpTrapHost, SnmpTrapCommunity, SnmpTrapPort.

CLI Command Syntax:

System[]>Shelf[ShelfId=1]> RemoveSnmpTrapConfig() SnmpTrapHost=localhost; SnmpTrapPort=163; SnmpTrapCommunity=public

RefreshHaState()

The operator can use this operation to refresh the High-availability state of each service running on the shelf.

CLI Command Syntax:

System[]>Shelf[ShelfId=1]> RefreshHaState()

SNMP Trap Configuration

Name

SnmpTrapConfig

Description

The SnmpTrapConfig table allows you to view the SNMP trap(s) configured in the system through the AddSnmpTrapConfig() operation.

CLI Navigation

System[]>Shelf[]>SnmpTrapConfig

CLI Inherited Attributes

ShelfId

CLI Command Syntax

```
System[]:Shelf[ShelfId =ShelfId]> display SnmpTrapConfig[SnmpTrapHost=
string; SnmpTrapCommunity= string; SnmpTrapPort= string]
```

WebCI Navigation:

System > **Shelf View** > **SNMP Config**

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 62: SNMP Trap Configuration Mandatory Attributes

Attribute	Value Range	Default	Description
SnmpTrapHost	String (maximum size 255) ex: x.x.x.x or FQDN (Fully Qualified Domain Name)	N/A	This parameter indicates the host to which traps are sent.

Table 63: SNMP Trap Configuration Optional Attributes

Attribute	Value Range	Default	Description
SnmpTrapPort	String (maximum size 16)	162	This parameter indicates the port used by the remote host to receive traps
SnmpTrapCommunity	String (maximum size 255)	public	This parameter indicates the community string used to send traps.

CLI Example

```
1 :System[]:Shelf[Shelf[ShelfId = 1]>display SnmpTrapConfig[]
```

VIP

Name

Vip

Description

The Vip table allows you to view the OAMP VIP addresses configured in the system. This table acts as a repository to store the VIPs that are bind to the system.

CLI Navigation

System[]>Shelf[]>Vip

CLI Inherited Attributes

ShelfId

CLI Command Syntax

```
System[]:Shelf[ShelfId =ShelfId]>display Vip[Netmask= string; Vip= Virtual
IP address; VipType=0,1,2,3,4]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 64: VIP Optional Attributes

Attribute	Value Range	Default	Description
Vip	Virtual IP address (xxx.xxx.xxx.xxx)	N/A	Slot external IP Address.
VipType	**0 Default** **1 Oamp** **2 GeoReplication** **3 Provisioning** **4 Ldap**	0	Defines the purpose of the Vip.
Netmask	String(15)	N/A	Netmask used with slot IP address.

CLI Example

```
1 :System[]:Shelf[Shelf[ShelfId = 1]>display Vip[]
```

Slot

Name

Slot

Description

The Slot Entity represents one of the slots on the shelf. Slots numbered 1 through 15 represent their physical counterpart on the shelf.

CLI Navigation

You can have access to the SmModule entity by following one of these navigation paths:

- To access the Slot knowing the ShelfId it belongs to:**System[]>Shelf>Slot**
- To access the Slot knowing the Identity bound to it:**System[]>Identity>Slot**

CLI Inherited Attributes

- When accessing Slot through Shelf:**ShelfId.**
- When accessing Slot through Identity:**IdentityId**

CLI Command Syntax

- **`System[]:Shelf[ShelfId = ShelfId#]> display Slot[SlotId = integer; IsLocked=0,1; GeoClusterId=int; Hostname=string; IpAddress= IP address; AccessVip=string; IdentityId=integer]`**
- **`System[]:Identity[IdentityId = IdentityId#]> display Slot[SlotId = integer; IdentityId=uint; GeoClusterId=int; IsLocked=0,1; Hostname=string; IpAddress= IP address; AccessVip=string]`**

Operations Permitted Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 65: Slot Mandatory Attributes

Attribute	Value Range	Default	Description
`SlotId`	1 to 4294976295	N/A	Read only. Numerical slot Identification assigned by the system. For cards, this corresponds to the physical slot on the shelf. Values are unique for the shelf.
`GeoClusterId`	0	0	Identifier of the Geo-redundant cluster.
`IsLocked`	0 or 1	0	Read only. Indicates the Locked state of the FRU in this slot. 0=Unlocked 1=Locked
`IdentityId`	0 Default 1 SystemController 7 FrontEnd	N/A	Identification of the Identity bound to the slot.

Table 66: Slot Optional Attributes

Attribute	Value Range	Default	Description
`IpAddress`	String (15)	N/A	Slot IP Address.
`Hostname`	String	N/A	Slot hostname.
`AccessVip`	String (15)	N/A	Slot external access IP address.

CLI Example

```
1 :System[]:Shelf[Shelf[ShelfId = 1]>display Slot[SlotId = 5] IsLocked
```

Slot Operations

Add Service()

The operator can use this operation to bind a service to a slot. Only user service can be added by the operator. Binding a service to a slot will populate the system model with required module instances and deploy software process on the blade. When adding a service to a slot, the operator is actually defining the set of modules that will start on that slot. This is achieved using the Module Type.

Command syntax:

```
:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]> addService()
```

Remove Service()

The operator can use this operation to remove a service from this slot. Only user service can be removed by the operator. This operation will remove affected module instances from the system model and shutdown affected processes.

Command syntax:

```
:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]> RemoveService()
```

Start Services()

The operator can use this operation to start all services bound to this slot. All service processes will be launched if an SBC is assigned to this slot.

Warning: If the StopServices() operation was executed previously, a delay of 30 seconds must be taken into account before being able to execute the StartServices() operation.

Command syntax:

```
:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]> StartServices()
```

Stop Services()

The operator can use this operation to stop all services bound to this slot.

When stopping the services on a blade, you can choose to stop or not the database with the **Stopdb** parameter. This parameter can take the following values: 0: the database won't be stopped. The database will continue running on the blade.

1: the database is stopped at the same time as the services.

If you choose not to stop the database, the services on the blade will stop, but the database will continue running and the volatile data won't be lost.

Command syntax:

```
:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]> StopServices() Stopdb=0
```

Restart Services()

The operator can use this operation to restart all services running on a slot. When executing this operation, the system will stop all the services running on the slot selected and then automatically restart them. This operation should only be executed during down time for troubleshooting, as it could affect the traffic.

Command syntax:

```
:System[] :Shelf[ShelfId = #]:Slot[SlotId = #]> RestartServices()
```

Start Trace()

Warning: This operation cannot under any circumstances be executed by the operator without the permission of Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted in order to activate the necessary traces. When a Tekelec technician performs this operation, traces for all modules running on the specified slot will be enabled.

Stop Trace()

Warning: This operation cannot under any circumstances be executed by the operator without the permission of Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted and if needed will deactivate some traces by performing this operation and disabling the traces for all modules running on the specified slot.

Geo-Cluster Configuration

Name

```
GeoClusterConfig
```

Description

The GeoClusterConfig table allows you to configure the system for a Geo-Redundancy deployment.

CLI Navigation

```
System[]>Shelf[]>GeoClusterConfig
```

CLI Inherited Attributes

```
ShelfId
```

CLI Command Syntax

```
System[]:Shelf[ShelfId = ShelfId]>display GeoClusterConfig[GeoClusterId=int;
GeoLocalSiteIp= IP address; GeoLocalSiteNetmask= string; GeoRemoteSiteIp=
```

IP address; GeoRedundancyEnabled= 0,1; GeoRemotePort= string; GeoLocalPort= string]

WebCI Navigation:

System > Geo Redundancy View

Operations Permitted

Display, modify

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 67: Geo Cluster Configuration Mandatory Attributes

Attribute	Value Range	Default	Description
GeoClusterId	0	0	Id of the Geo cluster.
GeoLocalSiteIp	IP Address	N/A	Local virtual IP address of a site of type GeoReplication that works in a Geo-redundancy deployment.
GeoLocalSiteNetmask	String(15)	N/A	Netmask of the geo-redundant local site.
GeoRemoteSiteIp	IP Address	N/A	Virtual IP address of the peer site of type GeoReplication and with which it works with in a Geo-redundancy deployment.
GeoRedundancyEnabled	bool 0,1	0	Attribute that indicates if the Geo-Redundancy feature is enabled or not. 0=Disabled 1=Enabled

Table 68: Geo Cluster Configuration Optional Attributes

Attribute	Value Range	Default	Description
GeoRemotePort	0 to 65 535	62002	This parameter indicates the remote port on the geo-redundant peer site.
GeoLocalPort	0 to 65 535	62002	This parameter indicates the local listening port on the geo-redundant site.

CLI Example

```
System[]:Shelf[Shelf[ShelfId = 1]>display GeoClusterConfig[]
```

Geo-Redundancy Operations

DisableGeoRedundancy()

The operator can use this operation to disable the geo-redundancy feature. When disabling this feature, the parameter GeoRedundancy in the System entity will take the value of 0. Once you have executed this operation, you can verify the result by displaying the System entity and if the GeoRedundancy parameter has a value of 0, the feature has been disabled.

Command syntax:

```
System[]:Shelf[ShelfId = 1]> GeoClusterConfig[GeoClusterId=0]>
DisableGeoRedundancy()
```

EnableGeoRedundancy()

This operation is mostly useful at installation of the system in a geo-redundancy deployment to enable the geo-redundancy feature. When enabling this feature, the parameter GeoRedundancy in the System entity will take the value of 1. For a system with the geo-redundancy feature enabled, the GeoRedundancy parameter will have a value of 1 in the System entity.

Command syntax:

```
System[]:Shelf[ShelfId = 1]> GeoClusterConfig[GeoClusterId=0]>
EnableGeoRedundancy()
```

ForceGeoReference()

In the case where the system's database is the replica of the database of its reference peer in the remote site and where the connection between the two sites is lost, the operator can judge the situation and wait until the connection is re-established, in which case the system will eventually go back into the replica state. However, if the operator knows the connection will not be re-established soon, he can use the ForceGeoReference operation to force the database to become in a Reference state and therefore force the system to become the reference peer. Using this operation will force the system into becoming the reference for its remote site when the connection is re-established.

Command syntax:

```
System[]:Shelf[ShelfId = 1]> GeoClusterConfig[GeoClusterId=0]>
ForceGeoReference()
```

Note: When the ForceGeoReference() operation is executed on the former Replica HLR, it goes into database Reference immediately. When the Geo-Redundancy link is recovered, a replication negotiation won't start between two reference HLRs. So once this operation has been successfully completed, it is necessary to manually execute the following operations on the former Reference HLR to trigger replication negotiation and to complete the Geo 'switch-over':

ResumeGeoRedundancy()

In the case where the connection is lost between the geo-redundant sites and where it is later reestablished but then where the system could not detect which peer serves as the reference and which one is the replica (i.e, due to configuration changes), the system becomes in an unassignedEnabled state. When the system is in this unassigned state, the operator can execute the ResumeGeoRedundancy operation to bring the system back into the negotiating state at which point it goes into a detection process to determine which peer is the replica and which one is the reference.

Note: To view in which state the system's database is, display the GeoDatabaseState entity, part of the Database entity. For more information on the GeoDatabaseState entity and its parameters, please refer to the "Database Operations" chapter of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual*. For the step-by-steps instructions on how to display the GeoDatabaseState entity, please refer to the "Viewing/Modifying the information for a Geo-Redundant System" in the "Troubleshooting the system" chapter in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Command syntax:

```
System[]:Shelf[ShelfId = 1]> GeoClusterConfig[GeoClusterId=0]>
ResumeGeoRedundancy()
```

Module Type

Name

ModuleType

Description

A ModuleType is a kind of Module (i.e., or a kind of process) associated to a Service. This table contains the different Module Types already pre-configured in the system.

CLI Navigation

System[]>ModuleType

CLI Inherited Attributes

None.

CLI Command Syntax

```
System[]>display ModuleType[ModuleType = 0-37; Name = string; Description
= string; TraceEnable=0,1; MasterName = string; MasterInstance = string]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 69: Module Type Mandatory Attributes

Attribute	Value Range	Default	Description
ModuleType	0 Unknown 1 Framework 2 SchemaManager 4 SystemManager 5 DataProvider 6 DpController 7 OampEventViewer 8 OampEventMgr 9 OampManager 10 Oamp Performance Manager 11 HlrServer 12 HlrProvManager 13 HlrWgs 14 AucServer 15 SS7Manager 16 SipServer 17 SipProvManager 19 NodeManager 20 TestModuleType 21 DpReplicator 22 BlueCli 23 WebCI 24 SOAP 25 CmdFileLoader 26 SNMP 27 HssServer 28 HssProvManager 29 SipUa 30 XmlDataServer 31 DpProxy	N/A	Module type: kind of Module associated to a service.

Attribute	Value Range	Default	Description
	32 SubscriberManager 33 LdapDataServer 34 LteHssServer 35 LteHssProvManager 36 Drm 37 DataAccessServer 38 ExternalService		
Name	Up to 65535 digits and/or letters		Module type name.
Description	Up to 65535 digits and/or letters		Module type description.
TraceEnable	0,1	0	Enables/Disables the traces per module.

Table 70: Module Type Optional Attributes

Attribute	Value Range	Default	Description
MasterName	Up to 65535 digits and/or letters		This field indicates the name of the module that has been elected as master. This field is used for master election load dispatching. Read-Only attribute.
MasterInstance	Up to 65535 digits and/or letters		If the load dispatching is master election, this field indicates the instance number of the module that has been elected as master. Read-Only attribute.

CLI Example

```
1 :System[]:ModuleType[ModuleType = NodeManager]>display
```

Identity

Name

Identity

Description

Represents the identities bound to slots, which define the basic set of services that run on that specific slot. All identities with their associated services are statically defined and loaded at installation time.

CLI Navigation

System[]>Identity

CLI Inherited Attributes

None.

CLI Command Syntax

System[]> add Identity[IdentityId = 0,1,7; Name = string; Description = string]

Operations Permitted

Display

Attributes and Values

Table 71: Identity Mandatory Attributes

Attribute	Value Range	Default	Description
IdentityId	0 Default 1 SystemController 7 FrontEnd	0	Identity ID.
Name	Up to 65535 digits and/or letters	N/A	Identity name.
Description	Up to 65535 digits and/or letters	N/A	Identity description

CLI Example

```
1 :System[]:add Identity[IdentityId = 1; Name=SystemController;
Description=System Controller]
```

Service

Name

Service

Description

Represents the services and their type that are already statically defined and loaded at installation time.

CLI Navigation

System[]>Service

CLI Inherited Attributes

None.

CLI Command Syntax

```
System[]> add Service[ServiceId = 0,1,2,3,5,6,8; Name = string; Description
= string; ServiceType=0,1; Leader=0-26; ProtMode=0,1,2; MaxNbOfInstance=uint]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 72: Service Mandatory Attributes

Attribute	Value Range	Default	Description
ServiceId	1 CoreSystemController 2 CoreServiceNode 3 Hlr 5 Hss 7 Database 8 ChassisManagement 11 DataAccess 12 LteHss 14 Ldap	0	Service ID.
Name	Up to 65535 digits and/or letters	N/A	Service name.
Description	Up to 65535 digits and/or letters	N/A	Service description
ServiceType	0 Core 1 User	N/A	Set if it is a core service, user service, Framework service or backend service. Refer to the

Attribute	Value Range	Default	Description
	2 Fw 3 Backend		"Services running on the system" section in the*SDM Product Description* for a detailed description of these types of services.
Leader	0 Unknown 1 Framework 2 SchemaManager 3 ChassisManager 4 SystemManager 5 DataProvider 6 DpController 7 OampEventViewer 8 OampEventMgr 9 OampManager 10 Oamp Performance Manager 11 HlrServer 12 HlrProvManager 13 HlrWgs 14 AucServer 15 SS7Manager 16 SipServer 17 SipProvManager 19 NodeManager 20 TestModuleType 21 DpReplicator 22 BlueCli 23 WebCI 24 SOAP 25 CmdFileLoader 26 SNMP 27 HssServer 28 HssProvManager 29 SipUa		ModuleType of service leader.

Attribute	Value Range	Default	Description
	30 XmlDataServer 31 DpProxy 32 SubscriberManager 33 LdapDataServer 34 LteHssServer 35 LteHssProvManager 36 Drm 37 DataAccessServer 38 ExternalService		
ProtMode	0 NoProt 1 PureFT 2 PureDistributed		Service group protection mode. **0 (NoProt):** This means that the service group is not protected. If it fails, no other instance of this service group takes over. **1(PureFT):** This means that the service group is protected in a 1+1 mode (active/standby). One instance provides service and is active while the other one is standby and ready to provide service and take over upon failure of the active instance. **2 (PureDistributed):** This means that the service group is protected in a 1+N or 1+1+N mode (see the "Services running on the system" section in the*SDM Product Description* for a detailed description of these modes) and upon failure of an instance the other enabled instances take over the load of the failed instance in addition to their already assigned load. In the Protection modes 1 and 2, there is no loss of service upon failure of an instance.

Attribute	Value Range	Default	Description
MaxNbOfInstance	Uint32		Maximum number of instances of this service.

CLI Example

```
1 :System[]:add Service[ServiceId =
1;Name=CoreSystemController;Description=Core System
Controller;MaxNbOfInstance=2;ProtMode=PureFT;ServiceType=Core;Leader=NodeManager]
```

Service Option

Name

ServiceOption

Description

The ServiceOption entity is used to define an option bound to a specific service. A ServiceOption is bound to all instances of a service.

CLI Navigation

System[]>Service>ServiceOption

CLI Inherited Attributes

ServiceId

CLI Command Syntax

```
System[]> Service[ServiceId=0,1,2,3,5,6,8,11,12,14,15]> display
ServiceOption[OptionId = WebServiceSecurity, HlrInterfaceType,
HlrSctpSackTimeout, PublicIdentityBase, HttpsCertFile, HttpsKeyFile, Port,
RequireAuth, WebSecurity; OptionValue = string]
```

Operations Permitted

Display, Modify.**

Note: The service options must be configured/modified at installation/reboot of the system. They cannot be changed during running-time of the system, the services must be stopped and the system must be rebooted afterwards. Contact the *Customer Care Center* to request changes to be made to the service options.

Attributes and Values

Table 73: ServiceOption mandatory attributes

Attribute	Value Range	Default	Description
OptionValue	See *Table 74: OptionValue Value Range*		Values of OptionId attribute
OptionId	See *Table 75: OptionID Value Range*	N/A	See *Table 75: OptionID Value Range*
ServiceId	1 CoreSystem Controller 2 CoreService Node 3 Hlr 5 Hss 7 Database 8 Chassis Management 11 DataAccess 12 LteHss 14 Ldap	0	Service ID

Table 74: OptionValue Value Range

ServiceID	OptionID	Option Value	Default
1 (CoreSystem controller)	WebServiceSecurity	Enable or Disable	Disable
3 (Hlr)	HlrInterfaceType **OR**	E1 or T1	E1
	HlrSctpSackTimeout	Integer (milliseconds)	200
11 (DataAccess)	PublicIdentityBase **OR**	MSISDN, NAI, IMSI	MSISDN

Table 75: OptionID Value Range

ServiceID	OptionID	OptionID Description
1 (CoreSystem controller)	WebServiceSecurity	Attribute that allows to enable/disable the Web Service's security (http/https).
3 (Hlr)	HlrInterfaceType **OR**	Type of broadband telecommunication connection used (E1 or T1)
	HlrSctpSackTimeout	Kernel SCTP's SACK Timeout value.

CLI Example

```
System[]:Service[ServiceId = 1]>display ServiceOption[OptionId =
WebServiceSecurity]
```

Service Instance

Name

ServiceInstance

Description

The ServiceInstance entity is used to define the binding of a service to a slot. The Slot Entity represents one of the slots on the shelf. Slots numbered 1 through 15 represent their physical counterpart on the shelf.

CLI Navigation

You can have access to the ServiceInstance entity by following one of these navigation paths:

- Any ServiceInstance of a specific service in the system:

  System[]>Service[]>ServiceInstance

- Individual ServiceInstance bind to a specific slot on the shelf:

  System[]>Shelf>Slot>ServiceInstance

- Individual ServiceInstance bind to a specific slot to which is bind a specific identity:

  System[]>Identity[]>Slot[]>ServiceInstance

CLI Inherited Attributes

- For any ServiceInstance of a specific service in the system: ServiceId
- For individual ServiceInstance bound to a specific slot on the shelf: ShelfId, SlotId
- Individual ServiceInstance bound to a specific slot to which is bound a specific identity: IdentityId, SlotId

CLI Command Syntax

- Any ServiceInstance of a specific service in the system

  ```
  System[]> Service[ServiceId=0,1,2,3,5,6,8,11,12,14]> display
  ServiceInstance[ShelfId = uint; SlotId = 1-16;
  IdentityId=0,1,7;ServiceState=0,1]
  ```

- Individual ServiceInstance bound to a specific slot on the shelf:

  ```
  System[]:Shelf[ShelfId = ShelfId#]: Slot[SlotId = SlotId#]> display
  ServiceInstance[ServiceId=0,1,2,3,5,6,8,11,12,14;ServiceState=0,1]
  ```

- Individual ServiceInstance bound to a specific slot to which is bound a specific identity:

```
System[]:Identity[IdentityId =0,1,7]: Slot[SlotId = SlotId#]> display
ServiceInstance[ServiceId=0,1,2,3,5,6,8,11,12,14; ServiceState=0,1]
```

Operations Permitted

Display

Attributes and Values

Table 76: Service Instance Mandatory Attributes

Attribute	Value Range	Default	Description
ShelfId	1 to 4294976295	N/A	Read only. The Shelf Id number assigned by system.
SlotId	1 to 16	N/A	Read only. Numerical slot Identification assigned by the system. For cards, this corresponds to the physical slot on the shelf. Values are unique for the shelf.
IdentityId	0 Default 1 System Controller 7 FrontEnd	0	Read only. Identity ID.
ServiceState	0 Stopped 1 Started	0	Read only. Service state. It can be Started or Stopped.
ServiceId	0 Default 1 CoreSystem Controller 2 CoreService Node 3 Hlr 5 Hss 7 Database 11 DataAccess 12 LteHss 14 Ldap	0	Read only. Service ID.

Table 77: Service Instance Optional Attributes

Optional Attributes			
Attribute	**Value Range**	**Default**	**Description**
HaRole	0 Unassigned, 1 Standby, 2 Active	0	Read only. Indicates the High Availability role of modules running on this slot. 0 = Unassigned. Does not participate in providing service. 1 = Standby. Ready to take over service if active fails. 2 = Active. Actively providing service.
OpState	0 Disabled, 1 Troubled, 2 Initializing, 3 Enabled	0	Read only. Indicates the Operational state of the modules in this slot.
ResourceState	NoResource PoweredOff Uninitialized Healthy ShuttingDown ShuttingDownDone Failed	0	Read only. Resource state of the service's modules reported by the system. Indicates whether the process's resources are ready to be functional or not. Generally, for a process that has started, the Resource state appears as "healthy" and for a process that has stopped, the Resource state appears as "NoResource".
AdminState	0 Unlocked 1 Locked	0 Unlocked	Read only. Administrative state of the service instance.

CLI Example

```
Any ServiceInstance of a specific service in the
system:System[]:Service[ServiceId = 1]>display ServiceInstance[]
```

Service Instance Operations

Start Trace()

Warning: This operation cannot under any circumstances be executed by the operator without the permission of Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted in order to activate the necessary traces.

When a Tekelec technician performs this operation, traces for all modules running on the specified slot will be enabled.

Stop Trace()

Warning: This operation cannot under any circumstances be executed by the operator without the permission of Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted and if needed will deactivate some traces by performing this operation and disabling the traces for all modules running on the specified slot.

Start Service()

The operator can use this operation to start service. This will launch the processes of all SmModule contained in this service instance. In order to start a service, each of the processes of all SmModules contained in this service must be started.

Warning: If the StopService() operation was executed previously, a delay of 30 seconds must be taken into account before being able to execute the StartServices() operation.

CLI Command syntax

- **:System[]:Service[ServiceId = #]> ServiceInstance[ShelfId=#;SlotId=#]> StartService()**

Or

- **:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]:ServiceInstance[ServiceId=#]> StartService()**

Or

- **:System[]:Identity[IdentityId = #]:Slot[SlotId = #]> ServiceInstance[ServiceId=#;ShelfId=#]> StartService()**

Stop Service()

The operator can use this operation to stop service. This will kill the processes of all SmModule contained in this service instance.

CLI Command syntax

- **:System[]:Service[ServiceId = #]> ServiceInstance[ShelfId=#;SlotId=#]>StopService()**

Or

- **:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]:ServiceInstance[ServiceId=#]>StopService()**

Or

- **:System[]:Identity[IdentityId = #]:Slot[SlotId = #]> ServiceInstance[ServiceId=#;ShelfId=#]>StopService()**

Switch Over()

The operator can use this operation to order a switch over for this service.

Command syntax:

- **:System[]:Service[ServiceId = #]> ServiceInstance[ShelfId=#;SlotId=#;IdentityId=#]>SwitchOver()**

Or

- **:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]:ServiceInstance[ServiceId=#;IdentityId=#]>SwitchOver()**

Or

- **:System[]:Identity[IdentityId = #]:Slot[SlotId = #]> ServiceInstance[ServiceId=#;ShelfId=#]>SwitchOver()**

LockService()

The operator can use this operation to lock a service. This can be useful during maintenance in order to minimize the traffic impact when stopping a service. To achieve this, the service should be locked prior to being stopped.

CLI Command syntax

- **:System[]:Service[ServiceId = #]> ServiceInstance[ShelfId=#;SlotId=#;IdentityId=#]>LockService()**

Or

- **:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]:ServiceInstance[ServiceId=#;IdentityId=#]>LockService()**

Or

- **:System[]:Identity[IdentityId = #]:Slot[SlotId = #]> ServiceInstance[ServiceId=#;ShelfId=#]>LockService()**

UnlockService()

The operator can use this operation to unlock a service.

CLI Command syntax

- **:System[]:Service[ServiceId = #]> ServiceInstance[ShelfId=#;SlotId=#;IdentityId=#]>UnlockService()**

Or

- **:System[]:Shelf[ShelfId = #]:Slot[SlotId = #]:ServiceInstance[ServiceId=#;IdentityId=#]>UnlockService()**

Or

- **:System[]:Identity[IdentityId = #]:Slot[SlotId = #]> ServiceInstance[ServiceId=#;ShelfId=#]>UnlockService()**

Service Instance Option

Name

ServiceInstanceOption

Description

When a service is added to a slot, an option (ServiceInstanceOption) is automatically created. A ServiceInstanceOption is bound to a specific service instance. This entity can be configured by modifying the OptionValue attribute. With the ServiceInstanceOption, you can view the identification of the service and of the slot and shelf on which it runs. Moreover, you can view which protocol is used with SS7 (MTP2, SAAL, SIGTRAN).

CLI Navigation

You can have access to the ServiceInstanceOption entity by following one of these navigation paths:

- Any ServiceInstanceOption of a specific service instance of a service in the system:

  System[]>Service[]>ServiceInstance[]>ServiceInstanceOption

- Individual ServiceInstanceOption of a service instance bind to a specific slot on the shelf:

  System[]>Shelf>Slot>ServiceInstance>ServiceInstanceOption

- Individual ServiceInstanceOption of a service instance bind to a specific slot to which is bind a specific identity:

  System[]>Identity[]>Slot[]>ServiceInstance>ServiceInstanceOption

CLI Inherited Attributes

ServiceId, IdentityId, SlotId, ShelfId

CLI Command Syntax

- Any ServiceInstance of a specific service in the system:

  System[]>Service[ServiceId=0,1,2,3,5,6,8,11,12,14]> ServiceInstance[ShelfId = uint; SlotId = 1-16; IdentityId=0,1,6]> display ServiceInstanceOption[OptionId=OptionId#; OptionValue=string]

- Individual ServiceInstance bound to a specific slot on the shelf:

  System[]:Shelf[ShelfId = ShelfId#]: Slot[SlotId = SlotId#]>ServiceInstance[ServiceId=0,1,2,3,5,6,8,11,12,14; IdentityId= 0,1,6]> display ServiceInstanceOption[OptionId=OptionId#; OptionValue=string]

- Individual ServiceInstance bound to a specific slot to which is bound a specific identity:

  System[]:Identity[IdentityId = 0,1,6]: Slot[SlotId = SlotId#]>ServiceInstance[ShelfId=ShelfId#; ServiceId=

```
0,1,2,3,5,6,8,11,12,14]> display ServiceInstanceOption[OptionId=OptionId#;
OptionValue=string]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 78: Service Instance Option Mandatory Attributes

Attribute	Value Range	Default	Description
ShelfId	1 to 4294976295	N/A	Read only. The Shelf Id number assigned by system.
SlotId	1 to 16	N/A	Read only. Numerical slot Identification assigned by the system. For cards, this corresponds to the physical slot on the shelf. Values are unique for the shelf.
IdentityId	0 Default 1 SystemController 7 FrontEnd	0	Identity ID.
ServiceId	0 Default 1 CoreSystem Controller 2 CoreServiceNode 3 Hlr 5 Hss 7 Database 11 DataAccess 12 LteHss 14 Ldap	0	Service ID.
OptionId	SipIpAddress SS7Mtp2Layer SS7SaalLayer SS7Sigtran	N/A	Option Id. For the Hlr service, the SIP functionalities can or cannot be provisioned and all or either one of the MTP2, SAAL or SIGTRAN protocols can be used in the first few layers of the SS7 Stack.

Attribute	Value Range	Default	Description
OptionValue	For SipIpAddress: Provisioned or NotProvisioned For the SS7Mtp2Layer, SS7SallLayer and SS7Sigtran: Enable or Disable		Option value for the Option Id. For the OptionId: SipIpAddress, two values exist. Provisioned: the SIP functionalities are provisioned for the Hlr service. NotProvisioned: The SIP functionalities are not provisioned for the Hlr service. The values of the SS7Mtp2Layer are as follows: Enable: The SS7 Stack uses the MTP2 Layer protocol. Disable: The SS7 Stack does not use the MTP2 Layer protocol. The values of the SS7SaalLayer are as follows: Enable: The SS7 Stack uses the SAAL protocol. Disable: The SS7 Stack does not use the SAAL protocol. The values of the SS7Sigtran are as follows: Enable: The SS7 Stack uses the SIGTRAN protocol for layers 1-2-3. (TUCL, SCTP and M3UA protocols) Disable: The SS7 Stack does not use the SIGTRAN protocol.

CLI Examples:

- Any ServiceInstanceOption of a specific service instance of a service in the system:

```
1 :System[]:Service[ServiceId = 1]> ServiceInstance[SlotId =
5;ShelfId=1;IdentityId=SystemController]>display ServiceInstanceOption[]
```

- Individual ServiceInstanceOption of a service instance bound to a specific slot on the shelf:

```
1 : System[]:Shelf[ShelfId = 1]: Slot[SlotId = 5]>
ServiceInstance[ServiceId=1; IdentityId=1] >display ServiceInstanceOption[]
```

- Individual ServiceInstanceOption of a service instance bound to a specific slot to which is bound a specific identity:

```
1 : System []:Identity[IdentityId =1]: Slot[SlotId = 5]>
ServiceInstance[ShelfId=1; ServiceId=1] >display ServiceInstanceOption[]
```

SmModule

Name

SmModule

Description

This entity represents the modules running on the blades of the system. The modules are configured based on the identities bound to a given slot.

CLI Navigation

You can have access to the SmModule entity by following one of these navigation paths:

- Individual SmModule of a specific slot on the shelf:

  System[] >Shelf>Slot>SmModule

- Individual SmModule of a specific slot to which is bind a specific identity:

  System[]>Identity[]>Slot[]>SmModule

- Individual SmModule of a specific service instance of a service in the system:

  System[]>Service[]>ServiceInstance[]>SmModule

- Individual SmModule of a service instance bind to a specific slot on the shelf:

  System[]>Shelf>Slot>ServiceInstance>SmModule

- Individual SmModule of a service instance bind to a specific slot to which is bind a specific identity:

  System[] >Identity[]>Slot[]>ServiceInstance>SmModule

- Individual SmModule of a specific ModuleType:

  System[] >ModuleType[]>SmModule

CLI Inherited Attributes

- For individual SmModule of a specific slot on the shelf: ShelfId, SlotId
- For individual SmModule of a specific slot to which is bound a specific identity:IdentityId,SlotId
- For individual SmModule of a specific service instance of a service in the system: ServiceId, ShelfId, SlotId, IdentityId

- Individual SmModule of a service instance bound to a specific slot on the shelf: ServiceId, ShelfId, SlotId, IdentityId
- Individual SmModule of a service instance bound to a specific slot to which is bound a specific identity: ServiceId, ShelfId, SlotId, IdentityId
- Individual SmModule of a specific ModuleType:ModuleType

CLI Command Syntax

```
System[]: ModuleType[ModuleType = 0-37] >display SmModule [Orl= string;
Cgname= string; ShelfId=uint; SlotId= uint; IdentityId=uint; ServiceId=uint;
HaRole= 0,1,2; Description= string ; Instance= string; TraceEnable=0,1]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Table 79: SmModule Mandatory Attributes

Attribute	Value Range	Default	Description
Orl	Up to 255 digits and/or letters	N/A	Read only. Module Identification used internally by the system. An ORL is a name structure separated by slashes. For example, the Node Manager has the following ORL:"/NodeManager5". This is the NodeManager running on blade 5.
ModuleType	0 Unknown 1 Framework 2 SchemaManager 4 SystemManager 5 DataProvider 6 DpController 7 OampEventViewer 8 OampEventMgr 9 OampManager 10 Oamp PerformanceManager 11 HlrServer 12 HlrProvManager	0	ModuleType of this module.

Attribute	Value Range	Default	Description
	13 HlrWgs 14 AucServer 15 SS7Manager 16 SipServer 17 SipProvManager 19 NodeManager 20 TestModuleType 21 DpReplicator 22 BlueCli 23 WebCI 24 SOAP 25 CmdFileLoader 26 SNMP 27 HssServer 28 HssProvManager 29 SipUa 30 XmlDataServer 31 DpProxy 32 SubscriberManager 33 LdapDataServer 34 LteHssServer 35 LteHssProvManager 36 Drm 37 DataAccessServer 38 ExternalService		
Cgname	String	N/A	Name of cluster group that this module takes part.
ShelfId	1 to 4294976295	N/A	ID of the shelf where this module stands.
SlotId	1 to 16	N/A	ID of the slot where this module stands.
IdentityId	0 Default 1 SystemController	0	Identity ID of the slot where this module is deployed.

Attribute	Value Range	Default	Description
	7 FrontEnd		
ServiceId	0 Default 1 CoreSystemController 2 CoreServiceNode 3 Hlr 5 Hss 7 Database 8 ChassisManagement 11 DataAccess 12 LteHss 14 Ldap	0	Service Id of the service that contains this module.
HaRole	0 unassigned 1 standby 2 active	0	Module HA role.
Description	String	N/A	Module description.
Instance	Uint32	N/A	Module Instance number.
TraceEnable	0,1	0	To enable or disable the Trace for this module. 0=disable 1=enable

Table 80: SmModule Optional Attributes

Attribute	Value Range	Default	Description
AdminState	0 Unlocked 1 Locked	0 Unlocked	Read only. Administrative state of the module established by the system.
ResourceState	NoResource PoweredOff Uninitialized Healthy ShuttingDown ShuttingDownDone	0	Read only. Resource state of the module reported by the system. Indicates whether the process's resources are ready to be functional or not. Generally, for a process that has started, the Resource state appears as "healthy" and for a process that has stopped, the

Attribute	Value Range	Default	Description
	Failed		Resource state appears as "NoResource".
OpState	0 Disabled, 1 Troubled, 2 Initializing, 3 Enabled	0	Read only. Indicates the Operational state of the modules in this slot.

CLI Example

```
1 : System[]:ModuleType[ModuleType=6]>display SmModule[Orl = /NodeManager3]
```

SmModule Operations

Start Trace

Warning: This operation cannot under any circumstances be executed by the operator without the permission of Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted in order to activate the necessary traces. When a Tekelec technician performs this operation, traces for all modules running on the specified slot will be enabled.

Stop Trace

Warning: This operation cannot under any circumstances be executed by the operator without the permission of Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted and if needed will deactivate some traces by performing this operation and disabling the traces for all modules running on the specified slot.

Add Filter Component

Warning: This operation cannot under any circumstances be executed by the operator unless given the permission and instructions by Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted and if necessary may reduce the number of traces produced by filtering on components for a given module's traces.

Remove Filter Component

Warning: This operation cannot under any circumstances be executed by the operator unless given the permission and instructions by Tekelec's Customer Care Center. When troubleshooting, the Tekelec Customer Care Center must be contacted and if needed will remove the necessary filters that were previously added on components for a given module's traces.

Alarm

Name

Alarm

Description

This is used to retrieve the alarms that are currently active on the system.

CLI Navigation

System[]>Alarm

CLI Inherited Attributes

None

CLI Command Syntax

```
System[]>display Alarm[SequenceId = integer; SlotId = integer; Description
= text; ShelfId = integer; AlarmId = integer; ModuleId = 4,6,8-12,14,15,19;
ModuleInstance = integer; ComponentId = 0-9; SetTimestamp = timestamp;
AckTimestamp = timestamp; IsAcknowledge = 0,1; ComponentInstanceContext =
text; Severity = AlarmSeverity; SetBy = text; AckBy= text]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 81: Alarm Mandatory Attributes

Attribute	Value Range	Default	Description
SequenceId	1 to 4294976295	N/A	Read only. Numerical identifier uniquely identifies this specific alarm occurrence.

Table 82: Alarm Optional Attributes

Attribute	Value Range	Default	Description
SlotId	1 to 4294976295	N/A	Read only. Numerical identification of slot on shelf. Identifies the slot that could be related to this alarm.

Attribute	Value Range	Default	Description
Description	Up to 65535 digits and/or letters	Null	Text description of alarm condition.
ShelfId	1 to 4294976295	N/A	Read only. Identifies the shelf.
AlarmId	1 to 4294976295	N/A	Read only. Identifier which represents a specific type of alarm.
ModuleId	0 Unknown 1 Framework 2 SchemaManager 3 ChassisManager 4 SystemManager 5 DataProvider 6 DpController 7 OampEventViewer 8 OampEventMgr 9 OampManager 10 Oamp Performance Manager 11 HlrServer 12 HlrProvManager 13 HlrWgs 14 AucServer 15 SS7Manager 16 SipServer 17 SipProvManager 19 NodeManager 20 TestModuleType 21 DpReplicator 22 BlueCli 23 WebCI 24 SOAP 25 CmdFileLoader 26 SNMP 27 HssServer	N/A	Read only. Identifier of software module related to the alarm.

Attribute	Value Range	Default	Description
	28 HssProvManager 29 SipUa 30 XmlDataServer 31 DpProxy 32 SubscriberManager 33 LdapDataServer 34 LteHssServer 35 LteHssProvManager 36 Drm 37 DataAccessServer 38 ExternalService		
ModuleInstance	1 to 4294976295	N/A	Read only. Instance number of software module.
ComponentId	0 (Unknown), 1 (Framework), 2 (SystemProv), 3 (SystemManager), 4 (OampManager), 5 (HlrProvManager), 6 (HlrServer), 7 (SS7), 8 (AucServer), 9 (SystemHardware)	N/A	Read only. The component which generated the alarm.
SetTimestamp	Timestamp in format: day MMM DD hh:mm:ss YYYY	N/A	Read only. The date and time the alarm was generated, where: MMM = month DD = date hh = hour mm = minute ss = second YYYY = year

Attribute	Value Range	Default	Description
AckTimestamp	Timestamp in format: day MMM DD hh:mm:ss YYYY	Null	Read only. The date and time the alarm was acknowledged, where: MMM = month DD = date hh = hour mm = minute ss = second YYYY = year
IsAcknowledge	0 or 1	0	Read only. 0 = alarm not acknowledged 1 = alarm has been acknowledged.
Component-Instance-Context	Up to 255 digits and/or letters	Null	Read only. Represents the specific instance of the module and/or component which generated the alarm condition.
Severity	AlarmCritical AlarmMajor AlarmMinor AlarmWarning	N/A	Read only. The severity of the alarm (see table below for severity definition).
SetBy	text	'null'	Read only. Name of the system's process (ModuleType, i.e. OampManager, HlrServer, etc.) that set the alarm. The value of this parameter is generated by the system.
AckBy	text	'null'	Read only. Username of the user that acknowledged the alarm. The value of this parameter is generated by the system.

CLI Example

```
1 : System[]>display Alarm[SequenceId = 1]
```

Table 83: Alarm Severity Definition

Alarm Severity	Definition
Critical	Service affecting. A serious problem has occurred. This alarm should be cleared immediately. Resource is completely disabled.
Major	Service affecting. This alarm should be cleared immediately. Resource is partially disabled.
Minor	Non-service affecting. Problem exists. This alarm should be cleared as soon as possible. Resource is partially disabled.
Warning	Non-service affecting. Potential problem exists, resource is operational.

Alarm History

Name

`AlarmHistory`

Description

This represents the history of all alarms generated. This includes active alarms and cleared alarms. Additionally, alarm acknowledgements are also recorded in the alarm history.

CLI Navigation

`System[]>AlarmHistory`

CLI Inherited Attributes

None.

CLI Command Syntax

```
System[]>display AlarmHistory[SequenceId = integer; SlotId = integer;
Description = text; ShelfId = integer; AlarmId = integer; ModuleId =
4,6,8-12,14,15,19; ModuleInstance = integer; ComponentId = 0-9; Timestamp
= Timestamp; AckTimestamp = Timestamp; IsAcknowledge = 0,1;
ComponentInstanceContext = text; Severity = AlarmSeverity; IsCleared = 0,1;
SetBy = text; AckBy = text; ClearBy = text]
```

Operations Permitted

`Display`

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 84: Alarm History Mandatory Attributes

Attribute	Value Range	Default	Description
SequenceId	1 to 4294976295	N/A	Read only. Numerical identifier uniquely identifies this specific alarm occurrence.

Table 85: Alarm History Optional Attributes

Attribute	Value Range	Default	Description
SlotId	1 to 4294976295	N/A	Read only. Numerical identification of slot on shelf. Identifies the slot to which this alarm is related, if appropriate.
Description	Up to 65535 digits and/or letters	Null	Text description of alarm condition.
ShelfId	1 to 4294976295	N/A	Read only. Identifies the shelf.
AlarmId	1 to 4294976295	N/A	Read only. Identifier which represents a specific alarm code.
ModuleId	4 (SystemManager), 6 (DPController), 8 (OampEventMgr), 9 (Oamp Manager), 10 (Oamp Performance Manager), 11 (HlrServer), 12 (HlrProvManager), 14 (AucServer), 15 (SS7Manager), 19 (NodeManager)	N/A	Read only.
ModuleInstance	1 to 4294976295	N/A	Read only.Instance number of application.
ComponentId	0 (Unknown), 1 (Framework), 2 (SystemProv),	N/A	Read only. The component which generated the alarm.

Attribute	Value Range	Default	Description
	3 (SystemManager), 4 (OampManager), 5 (HlrProvManager), 6 (HlrServer), 7 (SS7), 8 (AucServer), 9 (SystemHardware)		
Timestamp	Timestamp in format: day MMM DD hh:mm:ss YYYY	N/A	Read only. The date and time the alarm was generated where: MMM = month DD = date hh = hour mm = minute ss = second YYYY = year
AckTimestamp	Timestamp in format: day MMM DD hh:mm:ss YYYY	Null	Read only. The date and time the alarm was acknowledged. where: MMM = month DD = date hh = hour mm = minute ss = second YYYY = year
IsAcknowledge	0 or 1	0	Read only. 0 = alarm not acknowledged 1 = alarm has been acknowledged.
Component-Instance-Context	Up to 255 digits and/or letters	Null	Read only. Represents the specific instance of the module and/or component which generated the alarm condition.

Attribute	Value Range	Default	Description
Severity	AlarmCritical AlarmMajor AlarmMinor AlarmWarning	N/A	Read only. The severity of the alarm.
IsCleared	0 or 1	0	Type of alarm. 0 = set alarm. An alarm occurred on the system. 1 = cleared alarm.
SetBy	Text	'null'	Read only. Name of the system's process (ModuleType, i.e. OampManager, HlrServer, etc.) that set the alarm. The value of this parameter is generated by the system.
AckBy	Text	'null'	Read only. Username of the user that acknowledged the alarm. The value of this parameter is generated by the system.
ClearBy	Text	'null'	Read only. Name of the system's process (ModuleType, i.e. OampManager, HlrServer, etc.) that cleared the alarm. The value of this parameter is generated by the system. When the alarm is cleared by the system, the latter creates a new entry in the AlarmHistory to represent the cleared alarm and it generates the value for this parameter. **Note:** The SetBy and AckBy parameters are set to 'null' for the cleared alarm entry.

CLI Example

```
: System[]>display AlarmHistory[SequenceId = 1]
```

Alarm Operations

The following section describes the operations that can be done with alarms.

Acknowledge()

The operator can use this to acknowledge a specific alarm. An acknowledge notification with a date and time stamp will be recorded in the AlarmHistory. The acknowledge operation does not clear the alarm. An alarm SequenceId will need to be specified to run this operation.

CLI Command syntax

```
System[]:Alarm[SequenceId = #]> Acknowledge()
```

Clear()

Caution: the operator must be careful with this operation.

This operation will remove the alarm from the active alarm list. An updated alarm entry appears in the AlarmHistory list. From the CLI, an alarm can be cleared even if the conditions that caused the alarm to be raised remain. In this scenario, take note that even though the alarm is no longer part of the active alarm list, the conditions that caused the alarm still exist and will NOT be reported when these conditions no longer prevail. It is strongly recommended to only clear alarms for which the conditions have not been rectified.

An Alarm SequenceId will need to be specified to run this operation. The Acknowledge operation must be run first before running the Clear operation.

CLI Command syntax

```
System[]:Alarm[SequenceId = #]> Clear()
```

Background Task

Name

BackgroundTask

Description

This entity allows to view all the operations (tasks) that are currently being performed by the system in the background.

CLI Navigation

```
System[]>BackgroundTask
```

CLI Inherited Attributes

None

CLI Command Syntax

```
System[]>display BackgroundTask[OperationId = integer; ModuleId = integer;
SequenceId = int; TaskContext = text; TaskStatus = 0,1; Timestamp = time]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 86: Background Task Mandatory Attributes and Values

Attribute	Value Range	Default	Description
SequenceId	1 to 4294976295	N/A	Read only. Numerical identifier that uniquely identifies a background task. The system generates the numerical ID in a sequential order in which the background tasks are performed.
ModuleId	0 Unknown 1 Framework 2 SchemaManager 3 ChassisManager 4 SystemManager 5 DataProvider 6 DpController 7 OampEventViewer 8 OampEventMgr 9 OampManager 10 Oamp PerformanceManager 11 HlrServer 12 HlrProvManager 13 HlrWgs 14 AucServer	N/A	Read only. Identifier of the software module affected by the task performed.

Attribute	Value Range	Default	Description
	15 SS7Manager 16 SipServer 17 SipProvManager 19 NodeManager 20 TestModuleType 21 DpReplicator 22 BlueCli 23 WebCI 24 SOAP 25 CmdFileLoader 26 SNMP 27 HssServer 28 HssProvManager 29 SipUa 30 XmlDataServer 31 DpProxy 32 SubscriberManager 33 LdapDataServer 34 LteHssServer 35 LteHssProvManager 36 Drm 37 DataAccessServer 38 ExternalService		

Table 87: Background Task Optional Attributes and Values

Optional Attributes			
Attribute	**Value Range**	**Default**	**Description**
`OperationId`	string	N/A	Read only. String identifying the type of operation being performed in the background. Most performed operations: StartService, StopService, StartServices, StopServices, RestartService, SwitchOver.

Optional Attributes			
Attribute	**Value Range**	**Default**	**Description**
TaskContext	string	Null	Read only. This parameter identifies the context of the operation: the type of operation, the module affected, the instance and slot on which runs that module,etc.
TaskStatus	1 (InProgress)	N/A	Read only. Status of the task. The entries in this entity display the tasks currently being performed in the background, therefore, these tasks are always in progress.
Timestamp	Timestamp in format: day MMM DD hh:mm:ss YYYY	Null	Read only. The date and time at which the background task was performed, where: MMM = month DD = date hh = hour mm = minute ss = second YYYY = year

CLI Example

```
1 : System[]>display BackgroundTask[]
```

Background Task History

Name

BackgroundTaskHistory

Description

This entity allows to view all the operations (tasks) that have been performed by the system in the background. The tasks stored in this entity are no longer in progress.

CLI Navigation

System[]>BackgroundTaskHistory

CLI Inherited Attributes

None

CLI Command Syntax

```
System[]>display BackgroundTaskHistory[OperationId = integer; ModuleId =
integer; SequenceId = int; TaskContext = text; TaskStatus = 0,1; Timestamp
= time]
```

Operations Permitted

Display

Note: Not all users (User Groups) are allowed to perform these operations.

Attributes and Values

Table 88: Background Task History Mandatory Attributes

Attribute	Value Range	Default	Description
SequenceId	1 to 4294976295	N/A	Read only. Numerical identifier that uniquely identifies a background task. The system generates the numerical ID in a sequential order in which the background tasks have been performed.
ModuleId	0 Unknown 1 Framework 2 SchemaManager 3 ChassisManager 4 SystemManager 5 DataProvider 6 DpController 7 OampEventViewer 8 OampEventMgr 9 OampManager 10 OampPerformance Manager 11 HlrServer 12 HlrProvManager 13 HlrWgs	N/A	Read only. Identifier of the software module affected by the task performed.

Attribute	Value Range	Default	Description
	14 AucServer 15 SS7Manager 16 SipServer 17 SipProvManager 19 NodeManager 20 TestModuleType 21 DpReplicator 22 BlueCli 23 WebCI 24 SOAP 25 CmdFileLoader 26 SNMP 27 HssServer 28 HssProvManager 29 SipUa 30 XmlDataServer 31 DpProxy 32 SubscriberManager 33 LdapDataServer 34 LteHssServer 35 LteHssProvManager 36 Drm 37 DataAccessServer 38 ExternalService		

Table 89: Background Task History Optional Attributes and Values

Attribute	Value Range	Default	Description
OperationId	string	N/A	Read only. String identifying the type of operation that has been performed in the background. Most performed operations: StartService, StopService, StartServices, StopServices, RestartService, SwitchOver.

Attribute	Value Range	Default	Description
TaskContext	string	Null	Read only. This parameter identifies the context of the operation: the type of operation, the module affected, the instance and slot on which runs that module,etc.
TaskStatus	0 Default 2 Done 3 Cancelled 4 Timeout 5 Failed	N/A	Read only. Status of the task. The tasks stored in this entity are no longer in progress.
Timestamp	Timestamp in format: day MMM DD hh:mm:ss YYYY	Null	Read only. The date and time at which the background task was performed, where: MMM = month DD = date hh = hour mm = minute ss = second YYYY = year

CLI Example

```
1 : System[]>display BackgroundTaskHistory[]
```

Self Healing (Database Replication Monitoring)

Name
DrmConfig

Description

This entity is used to configure/control the Database Replication Monitoring (DRM) process, which monitors the data replication between the system's different servers and which produces report files. The DRM can be configured/controlled during running time and will have the impacts on the DRM process thereafter.

CLI Navigation

`Database[]>DrmConfig`

CLI Inherited Attributes

None

CLI Command Syntax

`Database[]>display DrmConfig[DrmState = 0,1; DrmRunMode = Once, Repeatedly; DrmRunTime = integer; DrmScanPeriod = integer; DrmScanMethod = AllDatabase; DrmSite=LocalSite,LocalSiteAndGeo;DrmAction =SyncData,PrintDiff]`

Operations Permitted

`Display, modify`

Note: Not all users (User Groups) are allowed to perform these operations. Please see *Security Access Privileges* to know which ones have access to this entity and which operations they have permission to do.

Attributes and Values

Table 90: Operations Permitted Attributes and Values

Attribute	Value Range	Default	Description
`DrmState`	Bool (0,1)	0 (disabled)	This parameter allows the Network Operator to control the DRM functionality's activation status by enabling/disabling it. By default it's disabled. The Network Operator can disable and re-enable it as required. 0 (disabled): The DRM process will never run. 1 (enabled): The DRM process runs as configured in the DrmConfig [ ] entity.
`DrmRunMode`	Once Repeatedly	repeatedly	This parameter allows the Network Operator to set the monitoring mode of the DRM: Once or repeatedly. If the DRM needs to run only once, the monitoring will scan all databases

Attribute	Value Range	Default	Description
			(refer to point 'Action' field described below) and the operator has the choice to configure a start time or now.
DrmRunTime	Time (hour) 00:00	01:00 (1 AM)	This parameter allows the Network Operator to monitor the start time (on an hourly basis) at which the DRM must start to run.
DrmScanPeriod	Time (in days) 1 to 30	7 (the DRM runs and produces a report once a week)	This parameter allows the Network Operator to monitor the period of time (in days) that must elapse before the DRM can run again and produce the report. In other words, it is the frequency at which the DRM can run on a regular basis.
DrmScanMethod	Alldatabase	Alldatabase	This parameter allows the Network Operator to monitor the method of monitoring that must be done by the In this current release, the only DRM scanning method supported is: All database.
DrmSite	LocalSite LocalSiteAndGeo	LocalSite	The DRM module can perform schema or data validation either on single chassis system or Geo-Redundant systems. This parameter allows the Network Operator to monitor either only the Local Site or the Local Site and its Geo-Redundant Site. For Geo-Redundant systems, the DRM module should be enabled on both active

Attribute	Value Range	Default	Description
			SystemControllers and DrmSite should be configured as LocalSite on one system and LocalSiteAndGeo on another system. The DRM module that monitors local site should be scheduled to be ran first (by controlling the monitoring start time), at least 1 hour before the DRM module that monitors local and Geo-Redundant sites.
DrmAction	SyncData PrintDiff	SyncData	This parameter allows the Network Operator to configure the action to be taken by the DRM process after its monitoring session: Print out the differences into the report file or re-synchronize the databases. **Note:** Even if the Sync option is chosen, it may happen that some discrepancies can't be corrected and requires manual intervention.

CLI Example

```
1 : Database[]>display DrmConfig[]
```

Glossary

A

AMS	An open standard that specifi es standardized management methods for applications and business systems throughout their whole lifecycle. Active Message Store Provides store-and-forward functionality for SMS messages.
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.
AOR	Address of Record
AS	Application Server A logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination. The AS contains a set

A

	of one or more unique Application Server Processes, of which one or more normally is actively processing traffic. Authentication Server Authentification servers provide public access to certificates, and are integrated with electronic information retrieval systems to this end. Free access to certificates is necessary to support authentication in open systems. Application Simulator Test tool that can simulate applications and/or SMSCs.
ASP	Abstract Service Primitive Application Server Process A process instance of an Application Server. An Application Server Process serves as an active or standby process of an Application Server (e.g., part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances of) MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP end-point, and may be configured to process signaling traffic within more than one Application Server. Application Service Part Application Server Process

C

CLI	Command-line interface
CSCF	Call Session Control Function
CSV	Comma-separated values

C

	The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).
CUG	Closed User Group

D

DB	Database Data bus
Diameter	Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.
DNS	Domain Name Services Domain Name System A system for converting Internet host and domain names into IP addresses.
DPC	Destination Point Code

D

	DPC refers to the scheme in SS7 signaling to identify the receiving signaling point. In the SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. This point code can be adjacent to the EAGLE 5 ISS, but does not have to be.
DRA	Destination Routing Address Diameter Relay Agent
DSA	Delete Subscriber Data Answer

E

EIR	Equipment Identity Register A network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). Use of the EIR can prevent the use of stolen handsets because the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being registered on the network, thus making them useless.
ENUM	T**E**lephone **NU**mber **M**apping A technology for unifying various communications and telephone addresses for private and business numbers, facsimile and mobile phone numbers, SMS services, Instant Messaging and email. ENUM integrates legacy phone numbers with the Domain Name System (DNS). Users can access

E

	and maintain a directory that supports all forms of wired communication, mobile communications networks, and the Internet. ENUM allows for an end user to be reached on multiple devices via one phone number and allows the end user to determine which device to contact first or multiple devices simultaneously.

F

FQDN	Fully qualified domain name The complete domain name for a specific computer on the Internet (for example, www.tekelec.com). A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GPRS	General Packet Radio Service A mobile data service for users of GSM mobile phones.
GSM	Global System for Mobile Communications A second generation digital PCS mobile phone standard used in many parts of the world.
GT	Global Title Routing Indicator
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.

H

HA	High Availability High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.
HLR	Home Location Register A component within the Switching Subsystem of a GSM network. The HLR database is the central database within the GSM architecture. This is where information about the mobile communications subscribers who are assigned to a specific location area is stored. The subscriber data is used to establish connections and control services. Depending on the network size, the number of subscribers and the network organization, a number of HLRs can exist within a GSM network.

I

IMEI	International Mobile Equipment Identifier
IMS	IP Multimedia Subsystem These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication.
IMSI	International Mobile Subscriber Identity

I

	A unique internal network ID identifying a mobile subscriber. International Mobile Station Identity
ITU	International Telecommunications Union An organization that operates worldwide to allow governments and the private telecommunications sector to coordinate the deployment and operating of telecommunications networks and services. The ITU is responsible for regulating, coordinating and developing international telecommunications, and for harmonizing national political interests.

L

LOC	The primary function of the LOC server is to locate subscribers on GSM and IS-41 networks.

M

M3UA	SS7 MTP3-User Adaptation Layer M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MAP	Mated Application Part Mobile Application Part An application part in SS7 signaling for mobile communications systems.
MCC	Mobile Country Code A three-digit number that uniquely identifies a country served by

M

	wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.
MIB	Management Information Database A database of network management information that is used and maintained by the SNMP protocol.
MNC	Mobile Network Code A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.
MO	Mobile Originated Refers to a connection established by a mobile communication subscriber. Everything initiated by the mobile station is known as mobile originated.
MSISDN	Mobile Station International Subscriber Directory Number The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber. Mobile Subscriber Integrated Services Digital Network [Number] Mobile Station International Subscriber Directory Number. The unique, network-specific subscriber number of a mobile communications subscriber.

M

MSISDN follows the E.164 numbering plan; that is, normally the MSISDN is the phone number that is used to reach the subscriber.

MTP2 — Message Transfer Part, Level 2

MTP3 — Message Transfer Part, Level 3

N

NAI — Network Access Identifier

The user identity submitted by the client during network authentication.

NAPTR — Name Authority Pointer

Domain Name System resource record that identifies possible URLs and numbers that can be returned.

NDC — Network destination code

Network Data Collection

NM — Network Management

The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating and monitoring the resources of a telecommunications network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting

N

	management. Note: Network management does not include user-terminal equipment.
	Notification manager
NP	Number Plan
	Numbering Plan
	Number Portability
	A capability that permits telecommunications users to maintain the same telephone access number as they change telecommunication suppliers.

O

OAM&P	Operations, Administration, Maintenance, and Provisioning. These functions are generally managed by individual applications and not managed by a platform management application, such as PM&C
	Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.
	Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.
	Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).
	Provisioning – Setting up user accounts, devices, and services.
OID	Object Identifier

O

An identifier for a managed object in a Management Information Base (MIB) hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB OIDs belong to different standard organizations. Vendors define private branches that include managed objects for their own products.

OS

Operating System

Operations Systems

P

PC

Point Code

The identifier of a signaling point or service control point in a network. The format of the point code can be one of the following types:

- ANSI point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Non-ANSI domestic point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Cluster point codes in the format network indicator-network cluster-* or network indicator-*-*.
- ITU international point codes in the format **zone-area-id**.
- ITU national point codes in the format of a 5-digit number (**nnnnn**), or 2, 3, or 4 numbers (members) separated by dashes (**m1-m2-m3-m4**) as defined by

P

	the Flexible Point Code system option. A group code is required (**m1-m2-m3-m4-gc**) when the ITUDUPPC feature is turned on. • 24-bit ITU national point codes in the format main signaling area-subsignaling area-service point (**msa-ssa-sp**).
PDN	Packet Data Network A digital network technology that divides a message into packets for transmission.
PDP	Permissive Dialing Period Power Distribution Panel Monitors primary and secondary power sources on a continuous basis. Packet Data Protocol
PEM	Power Entry Module There are two pluggable redundant Power Entry Modules (PEMs) that are located at the rear bottom side of each shelf. Each PEM provides power terminals for four 30 amp power feeds. Privacy Enhanced Mail
PLMN	Public Land Mobile Network

R

RAS	REST Application Server

S

S

SAAL	Signaling ATM Adaptation Layer
SAP	Service Access Point
SBC	Single-board computer
SC	System Controller
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.
S-CSCF	Serving - Call Session Control Function Provides user and service authentication and authorization, client registration, SIP-routing capabilities, service integration, data management, FW/NAT traversal, multi-network integration and an interface to third-party applications.
SCTP	Stream Control Transmission Protocol 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

S

	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.
SDM	Subscriber Data Management
SDU	Service Data Unit
SIGTRAN	The name given to an IETF working group that produced specifications for a family of protocols that provide reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols. The most significant protocol defined by the SIGTRAN group was the Stream Control Transmission Protocol (SCTP), which is used to carry PSTN signalling over IP. The SIGTRAN group was significantly influenced by telecommunications engineers intent on using the new protocols for adapting VoIP networks to the PSTN with special regard to signaling applications. Recently, SCTP is finding applications beyond its original purpose wherever reliable datagram service is desired.
SIP	Session Initiation Protocol A peer-to-peer protocol used for voice and video communications.
SLF	Subscription Locator Function

S

SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAP	Simple Object Access Protocol
SPR	Subscriber Profile Repository A logical entity that may be a standalone database or integrated into an existing subscriber database such as a Home Subscriber Server (HSS). It includes information such as entitlements, rate plans, etc. The PCRF and SPR functionality is provided through an ecosystem of partnerships.
SS7	Signaling System #7 A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE 5 ISS is an STP, which is a device that routes these messages through the network.
SSH	Secure Shell

S

	A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.
SSN	Subsystem Number A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry. Subsystem Number Used to update the CdPA.
SSR	SIP Signaling Router Function responsible for querying a redirection server and proxying requests to other SSR servers, redirect servers, SSR Service Points, and Gateways. It helps in evolving a Flat NGN network into a hierarchical network.

T

TCAP	Transaction Capabilities Application Part A protocol in the SS7 protocol suite that enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the Signaling Connection Control Part connectionless service. TCAP also supports remote control - ability to

T

	invoke features in another remote network switch.
TCP	Transfer-Cluster-Prohibited Transfer Control Protocol Transmission Control Protocol A connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner.
TLS	Transport Layer Security A cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the transport layer end-to-end. TLS is an IETF standards track protocol.
TPD	The Oracle Communications Tekelec Platform (TPD) is a standard Linux-based operating system packaged and distributed by Oracle. TPD provides value-added features for managing installations and upgrades, diagnostics, integration of 3rd party software (open and closed source), build tools, and server management tools.

U

URI	Uniform Resource Identifier An internet protocol element consisting of a short string of characters that conform to a certain syntax. The string comprises a name or address that can be used to refer to a resource.

U

USM	User Security Management
USSD	Unstructured Supplementary Service Data

V

VIP	Virtual IP Address Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.
VLR	Visitor Location Register A component of the switching subsystem, within a GSM network. The switching subsystem includes various databases which store individual subscriber data. One of these databases is the HLR database or Home Location Register; and the VLR is another. Virtual Location Register

W

WebCI	Web Craft Interface

X

XML	eXtensible Markup Language A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.