Oracle® Communications
Subscriber Data Management

Monitoring, Maintaining, Troubleshooting User Guide

Release 9.3

910-6864-001 Revision B

October 2014

ORACLE®

Oracle® Communications Monitoring, Maintaining, Troubleshooting User Guide, Release 9.3

Copyright © 2013, 2014, Oracle and/or its affiliates. All rights reserved.

Table of Contents

Chapter 4: Viewing and editing subscriber profiles using WebCI..95

Chapter 5: Monitoring the system...138

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 monitoring tools, maintenance procedures, troubleshooting, and provides hardware installation instructions. It also describes how to view and modify subscriber profiles from the WebCI.

Scope and audience

This document provides information and procedures used for the maintenance and troubleshooting of the Subscriber Data Management system.

This document is intended for use by operators that are responsible and qualified for the subject matter of this document.

Document organization

This document is organized into the following chapters:

- *Introduction* contains general information about this document, how to contact the Tekelec *My Oracle Support (MOS)*, and *Locate Product Documentation on the Oracle Technology Network Site*.
- *Getting Started* provides information about beginning to use the Subscriber Data Management system.
- *User Interfaces* provides the procedures on how to use the user interfaces that allow the operator to configure the system or provision subscribers.
- *Viewing and editing subscriber profiles using WebCI* provides information used to manage profiles within the Subscriber Data Management system
- *Monitoring the system* provides information used to monitor the Subscriber Data Management system for alarms and other errors.
- *Maintenance* provides information used to perform maintenance on the Subscriber Data Management system.
- *Troubleshooting* provides information used to troubleshoot the Subscriber Data Management system.

About links and references

Information within the same document is linked and can be reached by clicking the hyperlink.

To follow references pointing outside of the document, use these guidelines:

General:

- Locate the referenced section in the Table of Content of the referenced document.
- Locate the same section name in the referenced document.
- Place the PDF files in one folder or on a disc and use the powerful Adobe PDF search functions to locate related information in one or more documents simultaneously.

Alarms

- *SDM Alarms Dictionary*

Product, features, concepts

- *SDM Product Description*

Monitoring, maintenance, or troubleshooting:

- Procedures: *Monitoring, Maintenance, Troubleshooting User Guide*
- Entities: *Monitoring, Maintenance, Troubleshooting Reference Manual*

Subscriber provisioning:

- Procedures: *Subscriber Provisioning User Guide*
- Entities: *Subscriber Provisioning Reference Manual*

System configuration:

- Procedures: *System Configuration User Guide*
- Entities: *System Configuration Reference Manual*

User Interfaces:

- *User guides*

    - How to use the user interface
    - How to set up users (permissions, groups, services)

- *Reference manuals*

    - About user interfaces
    - Entities for setting up users

To determine the components of the complete documentation set delivered with the software, refer to the *SDM Documentation Roadmap* delivered with each documentation set.

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	**Danger**: (This icon and text indicate the possibility of *personal injury*.)
WARNING	**Warning**: (This icon and text indicate the possibility of *equipment damage*.)

Icon	Description
⚠️ CAUTION	**Caution**: (This icon and text indicate the possibility of *service interruption*.)
🔺 TOPPLE	**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.

My Oracle Support (MOS)

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

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

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select **2** for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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

Emergency Response

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

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.

2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.

3. Click **Oracle Communications Documentation for Tekelec Products**.

4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).

5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter

2

Getting Started

Topics:

This chapter contains information regarding safety precautions, accessing the system, and logging in for the first time.

Safety Warnings and Cautions

It is important to read this section before attempting any of the hardware installation and maintenance procedures in this guide.

Only trained and qualified personnel should install, activate, and maintain the systems.

Warning:

- During installation, ensure the hardware being worked on is disconnected from the power supply until it is ready to be connected to a power source.
- Always turn OFF all power supplies and unplug all power and external cables before opening, installing, or removing a Tekelec hardware shelf.
- Do not wear loose clothing, jewelry (including rings and chains), or other items that might become trapped in the chassis.

Electrostatic Discharge (ESD)

The Tekelec Subscriber Data Management system contains electrical components which can be damaged by static electricity. Electrostatic discharge (ESD) damage occurs when electronic blades or components are improperly handled, which can result in complete or intermittent system failures. The following can help avoid ESD damage:

Caution: To prevent accidental damage that can be caused by static discharge, always use a grounding wrist strap or other static dissipating device while handling the equipment. Connect the wrist strap to the ESD jack located at the front top right corner of the chassis.

Do not touch components on the blades. Handle the blades only by their edges, face plates or extractor levers. When inserting or removing blades, do not touch any of the components.

Always place the blades with the component side up on an antistatic surface or in a static shielding bag.

Accessing the System

The Operating System and Tekelec Subscriber Data Management software are installed on the system prior to delivery. There are two ways to access the system: SSH client and serial connection.

Establish serial connection

Prerequisites:

- Terminal device with terminal emulation program
- Null-modem serial cable

1. Connect one end of cable to serial console connector on faceplate of Single Board Computer.
2. Connect other end of cable to PC or other terminal device running a terminal emulation program. Or create a Telnet connection via a Terminal server.
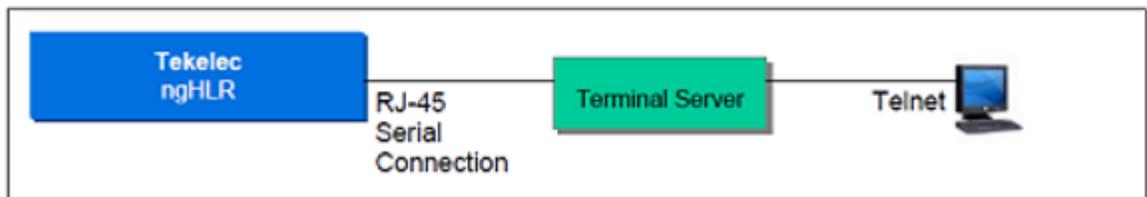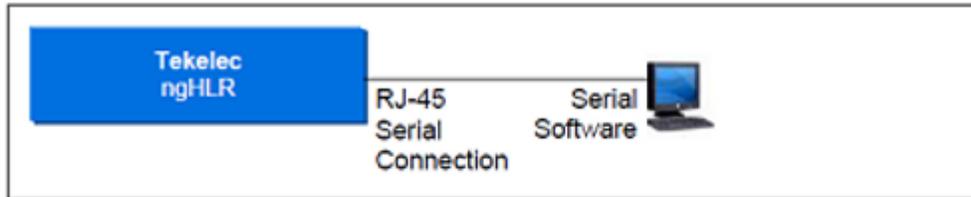
Establish Secure Shell (SSh) connection

Prerequisites

- *Configure SSh client (PuTTY)* (for example, OpenSSH, Cygwin, PuttY)
- Standard CAT 5 Ethernet cable

1. Connect one end of the cable to any one of the three Ethernet RJ-45 ports located on the front faceplate of the switch module.
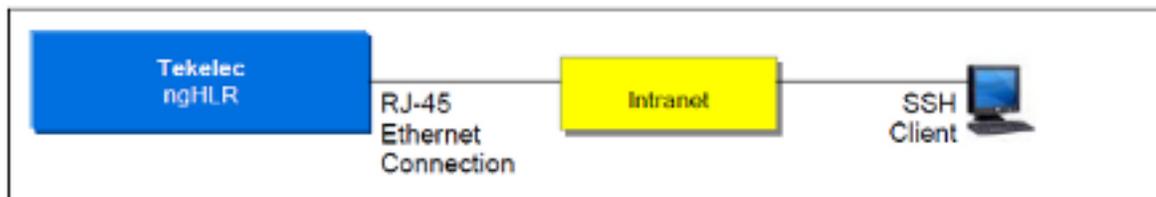
2. Connect other end of cable to PC or other terminal device running a terminal emulation program.
3. Start SSh client.

Configure SSh client (PuTTY)
When using PuTTY as the SSh client and connecting for the first time, install and configure PuTTY.

1. Locate the SDM software CD-ROM, which includes a version of PuTTY for Windows.
2. Copy the PuTTY directory to the system and run PUTTY.EXE.
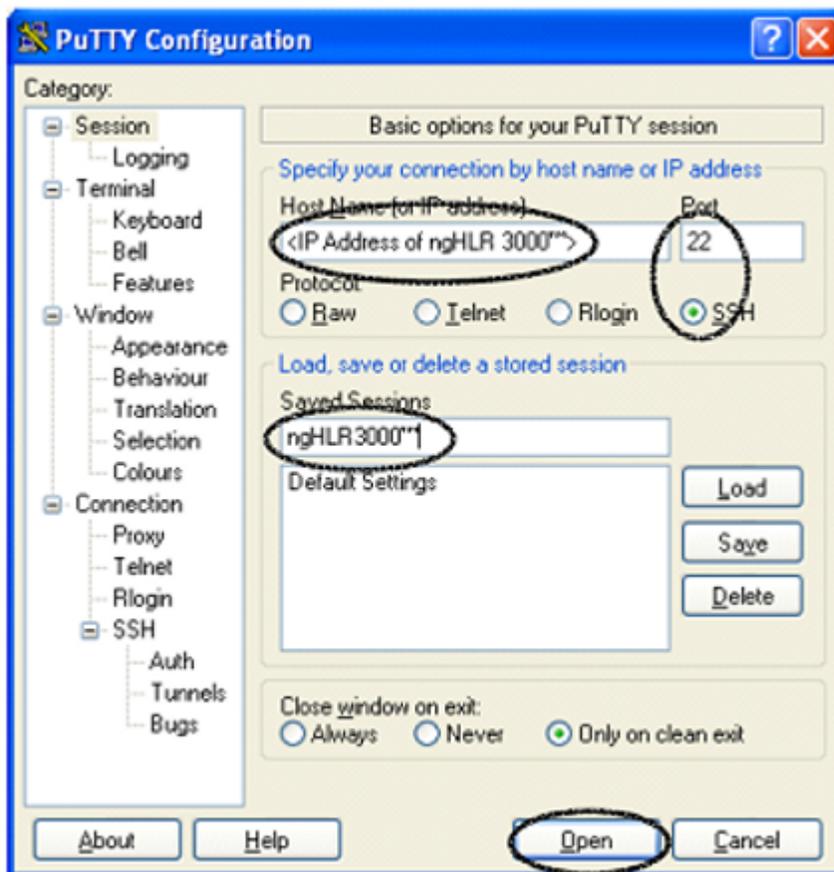
Figure 1: Configure SSh client (PuTTY)

3. Enter <**IP Address of the SDM**> and click SSH protocol.
4. Create session name.
5. Click **Open**

System login

You can access the system by entering a valid user ID and password to the System Controller (SC).

The User Security Management feature introduces Groups, in which users are categorized following their system use and to which access privileges are associated. Only the administrator has all the access privileges and permissions on the system.

At system installation, one default user is predefined for each of the following six predefined groups: user, operation, surveillance, admin, batch and simprov. Each default user is part of a group that has the same name as the user name (example: user admin is part of group admin). The password for each user is the user name by default. A user can be a member of only one user group. The table below displays the users pre-defined at installation, their UserName and UserPasswd and the name of the Group they are associated with.

Table 2: Pre-defined Users

User	Default UserName	Default UserPasswd	Group Name
Administrator	admin	admin	Admin
Surveillance	surveil	surveil	Surveillance
User	user	user	User
Batch	batch	batch	Batch
Operation	operation	operation	Operation
Sim provisioning	simprov	simprov	Simprov

The following groups are pre-defined in the system and categorized based on their system use:

- User: users are responsible for the system configuration and the subscriber provisioning. Typical use is through the WebCi and the Tekelec CLI. On rare occasions, they might also need to log in to the system to access the Tekelec CLI and the Command File Loader services.
- Operation: Operation regroups users responsible for the system operation and maintenance. Typical use is through the WebCi and the Tekelec CLI.
- Surveillance: Surveillance user are the groups involved in managing alarms produced by the system. Typical use is through an external network monitoring system (e.g., HP OpenView) and the Tekelec WebCi.
- Admin: The Administrators are responsible for a set of tasks that requires super user privileges. Their typical use is through the Unix Console
- Simprov: Simprov regroups users that are in charge of provisioning SIM cards.

Only the administrator of the system, already defined in the admin user group, can add users and associate them to one of the ten customizable groups, change its password and provision the groups by editing the services and permissions bind to them, all through the Tekelec CLI or WebCI.

Each group may contain several users and are categorized based on their system use.

Each Group has different access privileges assigned for specific services.

To view the access privileges predefined in the system for each Group, please refer to section 8.3 *User Management* of the *Reference Manual*.

The admin user is for the client set up administrator to access the SDM. Only the administrator of the system can manage the system's blades as well as enter the Tekelec CLI and manage all the Tekelec applications and their services. The administrator can perform a set of tasks that requires super user privileges. The administrator is the only one that can perform anything through the Unix Console.

Log in for the first time

1. Log in with the default username and password of a predefined group.

   Note: The system administrator has superuser permissions and should always be the first person to log in to change and assign passwords.

For example, as administrator, log in as shown below and press **Enter**.

```
login as: admin
password: admin
```

As user, log in as shown below:

```
login as: user
password: user
```

2. At the system prompt, start a CLI session to change the password. Type **cli** and press **Enter**.

```
[UserName@system UserName] $ cli
```

3. Go to the Oamp subsystem to change the password; type

```
:> Oamp[]
```

4. Continue to User Management; type

```
Oamp[]> SecurityManager[]
```

5. Specify the user to be modified (e.g., UserName=user2). Type

```
Oamp[]:SecurityManager[]> User [UserName=user2]
```

6. Change the password by using the modify operation and entering the new password. Type

```
Oamp[]:SecurityManager[]> User [UserName=user2]> modify .
Password=Xseries4users]
```

The following message displays:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

7. Type **y** if you wish to continue or **n** to cancel.
   If you typed **y**, the following message displays:

```
Modified:1
```

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.

Blueupdatesh help options

```
/opt/blue/blueupdate.sh –help
blueupdate.sh[-u] [-s] [-k] [-d] [-t dir] [-i interface] [-r release] [-f
[<host:>]<filename>>] [<buildId>]
```

- **-u:** uninstall only
- **-s:** start software after successful installation
- **-k:** keep current database
- **d:** use debug load
- **-t:** download tarball to given dir but do not install
- **-i:** use specified interface
- **-r:** use specified release
- **-f:** use specified installation file

    buildId is ignored if **-f** is specified

CFL help options

View the different Command File Loader (CFL) options through this command:

[UserName@system UserName] $ cfl -help

CmdFileLoader options:

- **[-c XmlConfigurationFileName]** (default: default value)
- **[-cmd XmlCommand]** (i.e., submitted inline)
- **[-d XmlCommandDirectoryName]**
- **[-f XmlCommandFileName]**
- **[-fo XmlOutputFileName]** (default: console)

    The **–fo <XmlOutputFileName.xml>** tracks the results of the provisioning request, where **<XmlOutputFileName>** is the path followed by the name of the XML output file in which you wish the system replies be stored (i.e., /tmp/template/Xmloutfile1.xml).

    All system replies are stored in the output file (including error reply codes). Specifying the output file is optional and when no output file name is given, the output is sent automatically to the console by default.

- **[-dbip]** (specifies the IP address of the database).
- **[-ip OampMgrIpAddress]**
- **[-observer]** (i.e., start observer; initiates notifications of changes to the database)
- **[-p OampManagerPort]** (default: 62001)
- **[-reso]** (produce result not encapsulated in xml and no other messages)
- **[-todb]** (i.e., load directly in the database) This is used in bulk provisioning to load subscriber profile information into the database without performing any validation of the xml requests.
- **[-trace]** (traces for errors)

- **[-user]** (user name)
- **[-validate]** (validate input against the global schema)

- **[-c XmlConfigurationFileName]** (default: default value)
- **[-cmd XmlCommand]** (i.e., submitted inline)
- **[-d XmlCommandDirectoryName]**
- **[-f XmlCommandFileName]**
- **[-fo XmlOutputFileName]** (default: console)

  The **-fo <XmlOutputFileName.xml>** tracks the results of the provisioning request, where
  <XmlOutputFileName> is the path followed by the name of the XML output file in which you
  wish the system replies be stored (i.e., /tmp/template/Xmloutfile1.xml).

  All system replies are stored in the output file (including error reply codes). Specifying the output
  file is optional and when no output file name is given, the output is sent automatically to the console
  by default.

- **[-ip OampMgrIpAddress]**
- **[-p OampManagerPort]** (default: 62001)
- **[-reso]** (produce result not encapsulated in xml and no other messages)
- **[-trace]** (traces for errors)
- **[-user]** (user name)
- **[-validate]** (validate input against the global schema)

Chapter

3

User Interfaces

Topics:

This chapter provides the procedures on how to use the user interfaces that allow the operator to configure the system or provision subscribers.

For an overview of the Command Line Interface (CLI), its commands, the command convention, navigation, and command descriptions, refer to the *User Interfaces* section in the related reference manual.

Command Line Interface (CLI)

This section provides step-by-step instructions on how to start a CLI session, how to get around in a CLI session, and how to end a CLI session. Refer to the *Command Line Interface* chapter in the *SDM System Configuration – Reference Manual* for an overview of the Command Line Interface (CLI) Commands, the command convention, navigation, and command descriptions.

Starting a CLI session

At installation time, five different users are automatically added. One user for each predefined user Group is added in the system with a default UserName and UserPasswd:

Table 3: Pre-defined users

User	Default UserName	Default UserPasswd	Group Name
Admin	admin	Admin	Admin
Surveillance	surveil	Surveil	Surveillance
User	user	User	User
Batch	batch	Batch	Batch
Operation	operation	Operation	Operation

All of these users can start a CLI session, but each with limited access and permissions to specific services. Only the administrator has access to all the services and all the permissions. To view the access privileges predefined in the system for each Group, refer to *Creating and Managing Users for the User Interfaces*.

To start a CLI session for the first time, the user must log in, as explained in *Accessing the system*, with its default UserName and UserPasswd. Afterwards, they must enter the following:

[UserName@system UserName] $ cli

After starting a CLI session for the first time, and with the user having changed its own password or as per the operator's convenience, with the administrator having changed the users' password, the user now accesses the system with its UserName and new password. Refer to *Creating and Managing Users for the User Interfaces* to know how to change a user's password.

The first thing recommended for the administrator to do once he has started a CLI session, is to initially provision users by creating one user name and give them different access privileges by associating them to groups following their system use and assigning them the access privileges desired for specific services.

Using the CLI

CLI prompt

After entering a CLI session, the user will be taken to the CLI prompt:
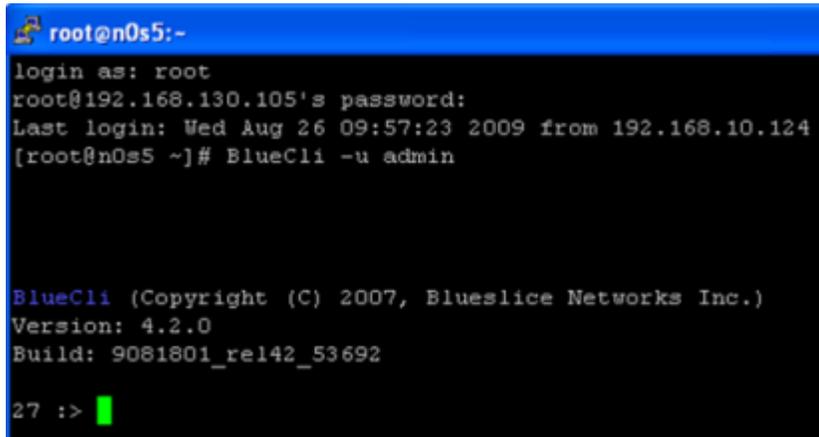
Figure 2: First CLI prompt

The CLI prompt consists of three different parts.

2: System[]>

The first part of the prompt is the command number (i.e., **2**:). This number is used to keep a history log of commands issued. The command number starts with 1 at system startup and auto-increments for each new command entered. The command number would restart again at 1 after a system restart.

The second part of the prompt indicates the current navigation level (i.e., **System[]**). This shows the user where they are within the navigational levels. If nothing identifies the navigation level, as shown in the figure above, this means that you have not navigated in any sub-system yet, you are at the highest level.

The third part is the prompt separator (**>**). Commands can be entered after the prompt.

Steps to Navigate and Perform Operations on Entities from the CLI

After starting a CLI session, you can enter the CLI commands on a level-by-level basis.

Commands can be entered as you progress down each level. Press the <TAB> key to view system prompts for acceptable values. Refer to the "Auto-Complete Functionality" section of the *SDM System Configuration – Reference Manual* for more information on the <TAB> key.

Navigating CLI with the Tab key

1. Wait for the first CLI prompt to appear.
2. Press the <Tab> key on your keyboard to display all the operations that can be performed and all the subsystems that can be accessed from this location.
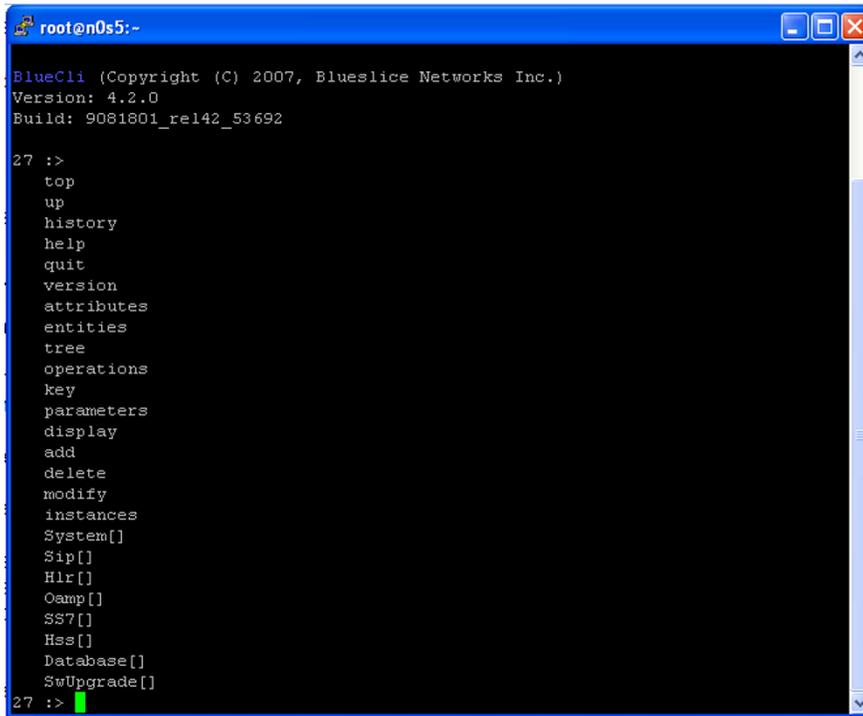
Figure 3: CLI subsystems

The following SDM subsystems can be accessed:

Table 4: Accessing subsystems through CLI

Command	Definition
Database[]	Access Database subsystem
Hlr[]	Access HLR subsystem
Oamp[]	Access OAMP subsystem
SS7[]	Access SS7 subsystem
System[]	Access System subsystem
Hss[]	Access HSS subsystem
Sip[]	Access the SIP functionalities of the Tekelec ngHLR.
Subscriptions[]	Access the Subscriptions subsystem
LteHss[]	Access to the LTE-HSS functionality

The subsystems can be accessed from anywhere in the CLI if the command is preceded by a colon (:). This defines an absolute navigation path:

```
2 :Hlr[]:SubscriberProfile[Imsi = 302370421001]> :System[]
3 :System[]>
```

3. Type the subsystem name you wish to access. For example, if you wish to perform operations on the HLR application, you must access the HLR subsystem. Type: **Hlr[]**
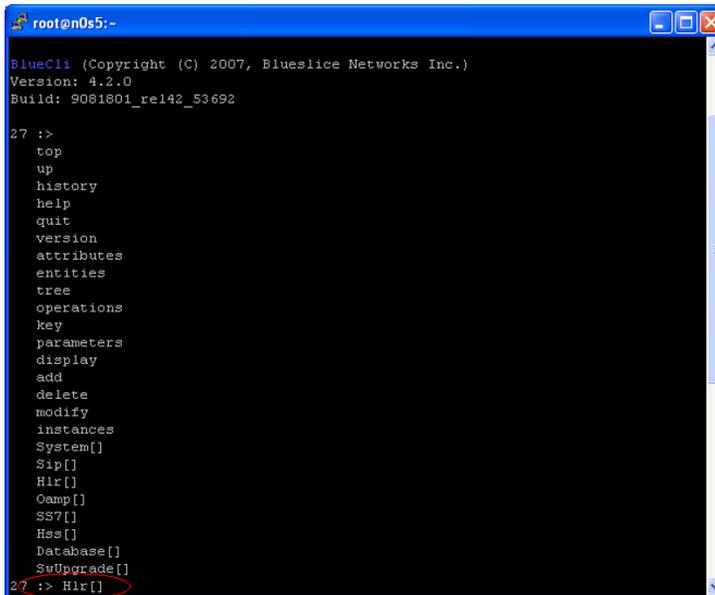
Figure 4: Accessing subsystems through CLI

4. Press **<Enter>**.
5. Press the **<TAB>** key to display the entities that can be accessed from this subsystem and the operations that can be performed.

```
  root@n0s5:~                                                    _ □ ×
37 :Hlr[]>
    top
    up
    history
    help
    quit
    version
    attributes
    entities
    tree
    operations
    key
    parameters
    display
    add
    delete
    modify
    instances
    UOS()
    UIS()
    CancelLoc()
    CancelGprsLoc()
    TestInterface()
    HssHlrInfoRequest()
    HssHlrInfoReply()
    DisplayTrilliumBufferSize()
    DisplayCounter()
    VolData()
    TransCount()
    ResetTransCount()
    TransList()
    ClearTransList()
    ViewHlrConfig()
    PrintHeap()
    DisplayNumberVolatileData()
    ImsiSwap()
    PrintOCPlmnData()
    CheckImsiAllowed()
    ConvertBinaryVolData()
    HlrConfig[]
    HlrUssdRtTable[]
    HlrCamelUGCsi[]
    SubscriberProfile[]
    MobileStation[]
    MultiImsi[]
    CamelGsmScf[]
    Plmn[]
    A4K4[]
    Algorithm[]
    Sim[]
    HlrSubscriberCount[]
    HlrProv[]
    HlrOCPlmnConfig[]
    HlrFtn[]
    GsmBearerCapabilities[]
    MtSmsRedirectTemplate[]
    SmsRelay[]
    CamelServiceMaskTemplate[]
37 :Hlr[]> ▮
```

Figure 5: Entities and operations available from the Hlr subsystem

The CLI commands are listed first.

Table 5: CLI commands

Command	Definition
add	Adds a new instance to the system
attributes	Show attributes of an entity

Command	Definition
`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.

The operations that can be performed on the HLR application are listed next; operations are identified by the () at the end.

The entities that can be accessed from the HLR subsystem are listed last.

Note: Other entities can only be accessed from these high-level entities.

6. Type the operation or entity you wish to access and press the <TAB> key to let the CLI auto-complete the command entry.

Figure 6: Entering an entity in the CLI

You can also press the <TAB> key several times until the command line is complete.

7. If the CLI returns a list of supported values, enter the value of the mandatory attribute.

```
70 :Hlr[]:SubscriberProfile[Imsi = 310910400000001]> add CallForward[Type=
33 CFU
41 CFB
```

```
42 CFNRY
43 CFNRC
```

If you don't know the value that has been configured already:

a) Type the UNIX command **UP** to go back to the next higher level, for example, the HLR subsystem level.

b) Type **display HlrConfig[]** to display the information configured in the entity you wish to access.

c) Press Enter.
The following confirmation prompt appears:

```
This Command could potentially display a very large number of instances. Proceed
 with display? (y/[n]):
```

d) Type **y**.
The information configured in the entity will be displayed with the name of the parameter and its value.

e) Type the value of the mandatory attribute.

8. Type a semicolon after the mandatory attribute and press <TAB> twice.

If the CLI doesn't add anything further, press <Backspace> until you erase the semicolon, then close the command with: **]** and press <Enter>. Otherwise, the CLI will enter the other mandatory attribute for which you need to also enter its value. Repeat this step until the CLI doesn't add anything.

Note: All attributes are separated by a semicolon.

Refer to the *SDM System Configuration – Reference Manual* for a description of the entity you are trying to access and provision to know which attributes are mandatory and for information on the attributes, their value range and default value.

9. Press the `<TAB>` key on your keyboard to see what other operations and entities can be accessed from this entity, as shown in the figure below.

Figure 7: Displaying operations and sub-entities from a CLI entity

At this point, you can perform one of the following actions:

- Display, modify or delete this entity, as follows:

  1. Display the HlrConfig by typing:

     ```
     Hlr[]:HlrConfig[HlrInstance = 1]> display
     ```

     This displays all the fields with information similar to the following:

     ```
     HlrInstance: 1
     RoutingNetworkType: ITU
     SccpRoutingNetworkIndicator: International
     RoutingSubSystemNumber: 6
     GtNumberingPlan: ISDN
     GtNatureOfAddress: International
     ImscAddr: 15634110123
     MaxNumCallForwardAllowed: 5
     MapMessageSegmentation: Deactivated
     RegionalSubscription: Activated
     SuperCharger: Activated
     UssdForwardVlrNumber: Activated
     RoutingOnSsn: Activated
     ```

```
DomainSelection: Deactivated
RoamingWelcomeMessage: Off
MapPolicing: Activated
SimKiTransportEncryption: Deactivated
FtnTranslation: Activated
SmsRedirection: Deactivated
UssdRouting: Deactivated
MapResetOptimization: Deactivated
SaiAckSegmentation: Activated
ActiveDeviceDetection: Deactivated
MobileNumberPortability: Unavailable
SubscriberSignalingRouter: Unavailable
AccessRestrictionData: Activated
DirectCallForwardRegistration: Deactivated
VlrMessageNotification: Deactivated
EnhancedControlOfSccpRouting: Unavailable
UpdateOfSccpCgAddrOnlyForUL: Unavailable
VolDataOptimization: Activated
```

Note: To view individual fields, specify them (i.e., RoutingNetworkType, MaxNumCallForwardAllowed) when issuing the Display operation.

]> **display . RoutingNetworkType; MaxNumCallForwardAllowed**

Information similar to the following will be displayed:

```
RoutingNetworkType: ITU MaxNumCallForwardAllowed: 5
```

2. Modify HlrConfig by typing

Hlr[]:HlrConfig[HlrInstance = 1]>**modify . UssdForwardVlrNumber = 0; SimKiTransportEncryption = 1**

The following warning will be displayed:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

Type **y** to proceed.

The following message displays:

```
 Modified: 1
```

3. Delete HlrConfig by typing

Hlr[]:HlrConfig[HlrInstance = 1]>**delete**

The following warning displays:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

Type **y** to proceed.

- Add an entry in one of the sub-entities displayed in the list (as shown in figure above). For example, type

  HlrNumberConfig:

Add the HlrNumberConfig attribute as shown below.

Note: After typing add HlrNumberConfig, press on the <TAB> key to let the CLI complete the command line further):

```
:Hlr[]:HlrConfig[HlrInstance = 1] >add HlrNumberConfig[HlrNumberConfigId
= 1; HlrAddrCC = 1; HlrAddrNDC = 123; HlrAddrSN = 1230001; HlrAddrIDD
= 001; HlrAddrNDD = 0]
```

The following message will be displayed.

```
Added: 1
```

- Access one of the sub-entities. For this, simply repeat steps 6 to 9 until you have reached the entity on which you wish to perform an action or until the navigation path ends.

Operations and command conventions

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 6: Supported operations

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

The following are basic UNIX shell commands to facilitate usage of the CLI:

Table 7: UNIX shell commands

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

Command	Definition
`<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).

The following provides a description of the characters used in CLI.

Table 8: 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
`.`	Specifies the current instance
`:`	Separates different levels between entities

Determine mandatory attributes using CLI
Displays mandatory attributes in CLI.

1. Type the command to add an entry in the entity, for example, type **:Hlr[]> add MSISDN[**

2. Press **Tab** .
   The CLI displays the entity attributes; the mandatory attributes are preceded by an asterisk (*).

```
root@n0s5:~
53 :Hlr[]> add MSISDN[
    * SubscriptionID
    * MsIsdn
    PortingStatus
    Published
    DefaultBsg
    BsgOverride
    BearerCapName
    Shared
    ForceToSip
    ADDSupport
```
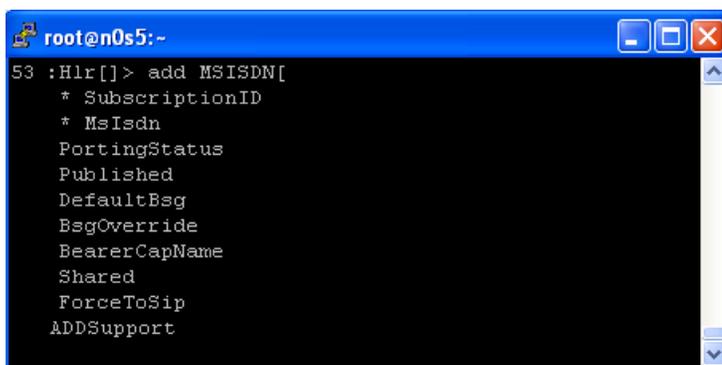
3. Press **Enter** to exit the command.
   The CLI returns `Invalid command` but returns to the previous navigation level.

Provisioning an entity - HLR Number Configuration

This section explains how to provision an entity using the add, modify, delete, and display operations. The provisioning procedures use the HLR Number Configuration entity as an example and provision the HLR identities (addresses). Multiple HLR Number Configurations can be provisioned to the HLR where each is represented by an identifier and will be associated to IMSI ranges.

This example uses these procedures:

- Adding HLR Number Configuration
- Modifying HLR Number Configuration
- Deleting HLR Number Configuration
- Displaying HLR Number Configuration

Adding HLR Number Configuration

This procedure describes the steps to add an identity to the HLR by defining a number (address). You can add more than one identity (address) to the HLR by repeating this procedure for each HLR identity you want the HLR to have and by giving it a different identification number (HlrNumberConfigId) each time.

1. Go to the HLR subsystem by typing,

   :>Hlr[]

2. Go to the HlrConfig by specifying the Instance and typing

   ```
   :Hlr[]> HlrConfig[HlrInstance = 1]
   ```

3. The HlrNumberConfig attributes are listed in the table below.

   Table 9: HLRNumberConfig attributes

Attribute	Value Range
HlrNumberConfigId	integer
HlrAddrCC	up to 3 digits
HlrAddrNDC	1 to 6 digits
HlrAddrSN	up to 15 digits
HlrAddrIDD	Up to 5 digits
HlrAddrNDD	Up to 5 digits

   Add the HlrNumberConfig as shown below:

   ```
   :Hlr[]:HlrConfig[HlrInstance = 1] > add HlrNumberConfig[HlrNumberConfigId =
    1; HlrAddrCC = 1; HlrAddrNDC = 123; HlrAddrSN = 1230001; HlrAddrIDD =
   001; HlrAddrNDD = 0]
   ```

The following message will be displayed.

```
Added: 1
```

Modifying HLR Number Configuration

This procedure describes the steps to modify the HLR Number Configuration. For details on the HLR
Number Configuration, refer to the *SDM Reference Manual* – HLR entities.

1. Go to the Hlr subsystem by typing,

```
:> Hlr[]
```

2. Go to the Hlr Config by specifying the Hlr Instance and typing,

```
:Hlr[]> sHlrConfig[HlrInstance = 1]
```

3. Go to the HlrNumberConfig by specifying the HlrNumberConfigId and typing,

```
:Hlr[]:HlrConfig[HlrInstance = 1]> aHlrNumberConfig[HlrNumberConfigId=1]s
```

4. The following attributes can be modified: HlrAddrCC, HlrAddrNDC, HlrAddrSN, HlrAddrIDD,
   HlrAddrNDD.
   a) Modify the Hlr Number Config by specifying the parameter(s) you wish to modify (i.e., in this
      case, swe choose to only modify the HlrAddrCC) and providing its new value as follows:

```
Hlr[]:HlrConfig[HlrInstance = 1]:HlrNumberConfig[HlrNumberConfigId=1]> modify
. HlrAddrCC = 31
```

The following warning will be displayed:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

5. Type **y**, to proceed.

The following message will be displayed.

```
Modified: 1
```

Modifying HLR Number Configuration – Alternate Method

1. Go directly to the Hlr Number Config by specifying the HLR instance, HlrNumberConfigId, and typing,

```
:> Hlr[]:HlrConfig[HlrInstance=1]:HlrNumberConfig[HlrNumberConfigId=1]
```

2. The following attributes can be modified: HlrAddrCC, HlrAddrNDC, HlrAddrSN, HlrAddrIDD, HlrAddrNDD.

    Modify the Hlr Number Config by specifying the parameter(s) you wish to modify (i.e., in this case, we choose to only modify the HlrAddrCC) and providing its new value as follows:

```
Hlr[]:HlrConfig[HlrInstance = 1]:HlrNumberConfig[HlrNumberConfigId=1]> modify
. HlrAddrCC = 31
```

    The following warning will be displayed:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

3. Type **y** , to proceed.

    The following message will be displayed.

```
Modified: 1
```

Deleting HLR Number Configuration

This procedure describes the steps to delete a HLR identity by deleting its Number Configuration.

1. Go to the Hlr subsystem by typing,

```
:> Hlr[]
```

2. Go to the Hlr Config by specifying the Hlr Instance and typing,

```
:Hlr[]> HlrConfig[HlrInstance = 1]
```

3. Delete the HlrNumberConfig by specifying the HlrNumberConfigId and typing,

```
:Hlr[]:HlrConfig[HlrInstance = 1]> delete HlrNumberConfig[HlrNumberConfigId=1]
```

The following warning will be displayed:

```
Warning ,you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

4. Type **y**, to proceed.

The following message will be displayed.

```
Deleted: 1
```

Deleting HLR Number Configuration – Alternate Method

1. Go to the Hlr Config by specifying the Hlr Instance and typing,

```
:> Hlr[]: HlrConfig[HlrInstance = 1]
```

2. Delete the Hlr Number Config by specifying the HlrNumberConfigId and typing,

```
Hlr[]:> delete HlrNumberConfig[HlrNumberConfigId=1]
```

The following warning will be displayed:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

3. Type **y** , to proceed.

The following message will be displayed.

```
Deleted: 1
```

Displaying HLR Number Configuration

This procedure describes the steps to display the HLR identities by displaying their Number Configuration.

1. Go to the Hlr subsystem by typing,

```
:> Hlr[]
```

2. Go to the Hlr Config by specifying the Hlr Instance and typing,

```
:Hlr[]> HlrConfig[HlrInstance = 1]
```

a) Display the HlrNumberConfig by specifying the HlrNumberConfigId and typing,

```
:Hlr[]:HlrConfig[HlrInstance = 1]>display
HlrNumberConfig[HlrNumberConfigId=1]
```

Information similar to the following will be displayed:

```
HlrInstance: 1
HlrNumberConfigId: 1
HlrAddrCC: 1
HlrAddrNDC: 123
HlrAddrSN: 1230001
HlrAddrIDD: 001
HlrAddrNDD: 0
```

b) To Display all the identities defined in the HLR, type the following:

```
:Hlr[]:HlrConfig[HlrInstance = 1]> display HlrNumberConfig[]
```

The following warning will be displayed:

```
This Command could potentially display a very large number of instances.
Proceed with display? (y/[n]): y
```

1. Type **y**, to proceed.

Information similar to the following will be displayed:

```
HlrInstance|HlrNumberConfigId|HlrAddrCC|HlrAddrNDC|HlrAddrSN|HlrAddrIDD|HlrAddrNDD|
---------------------------------------------------------------------------------
1|                1|        1|       123| 1230001|        001|         0|
1|                2|        1|       563| 4210100|        011|         1|
Displayed: 2
```

View command history

A history of the CLI commands that have been entered can be viewed.

View the command history by using one of these methods:

- 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.

  For example, to view the five most recent commands, type: history 5

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

Ending a CLI Session

To end the CLI session type quit at the system prompt, as follows:

```
2 :Hlr[]> quit
```

Note: When entering text in CLI, there is no need to enclose it in quotations. Type the text to be added without quotations.

Web Craft Interface (WebCI)

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, troubleshooting of subscriber profiles and alarm management.

Starting a WebCI Session

The Web Craft Interface (WebCI) supports the following versions of web browsers:

- Internet Explorer version 8 on Windows.
- Mozilla Firefox version 12.0.

Accessing the Web Craft Interface

To access the Web Craft Interface (WebCI), enter the following URL in the web browser:

```
https://<IP Address:8443/webci
```

where IP Address = address of module and the default port is 8443.

e.g., *https://193.10.20.100:8443/webci* . The default port is 8443.

The following login window appears:

Log in to the WebCI by entering a valid username and password. Click **Submit**.

For the first login, the valid username and password for the following users set by default in the system are:

Table 10: Pre-defined users

User	Default UserName	Default UserPasswd	Group Name
Admin	admin	admin	admin
Surveillance	surveil	surveil	surveillance
User	user	user	user
Batch	batch	batch	batch
Operation	operation	operation	operation
Sim provisioning	simprov	simprov	Simprov

Each of these users have predefined access privileges, only the admin user has access to all services and the Read, Write and Execute permissions. To view the access privileges predefined in the system for each Group, please refer to *Creating and Managing Users for the User Interfaces* in this document.

Note: The customizable groups: usergroup1, usergroup2,…usergroup10 have no default user or default access privileges. The administrator, already defined in the admin group, can (if needed) provision these groups by creating a user and associating it to one of these groups and customizing the group by setting access privileges as it wishes.

After each user starts their first session with WebCI, they must change their own password or have the administrator change it for each user including himself, for security purposes in order to limit access to services for different users.

Moreover, the first thing recommended for the administrator to do once he has started a WebCI session, is to initially provision users, if not done already through CLI, by creating users and giving them a username and password, and different access privileges by associating them to groups following their system use and assigning them the access privileges desired for specific services.

From this point forward, each user can log in to the WebCI by entering their username and password provisioned by the administrator in the system.

Using the WebCI

The WebCI is used to facilitate system configuration, troubleshooting of subscriber profiles and alarm management.

Displaying a WebCI window

1. Locate the main menu in the left panel of the WebCI page.
   The main menu consists of folders next to hyperlinks labeled with the application name.
2. Click the folder or the hyperlink to display the submenu.
   A blank WebCI window displays.
3. Click a submenu item to display its WebCI window.

   • The window displays the name of the submenu item and any applicable tables to configure.
   • If the submenu has its own submenu items, the WebCI window displays those items in tabs and opens to the content of the first tab.

4. Click the hyperlink on the tab to navigate between tabs.

The figure shows the WebCI main menu with the open HLR menu item, the selected HLR Configuration submenu and all the tabs applicable for HLR configuration.
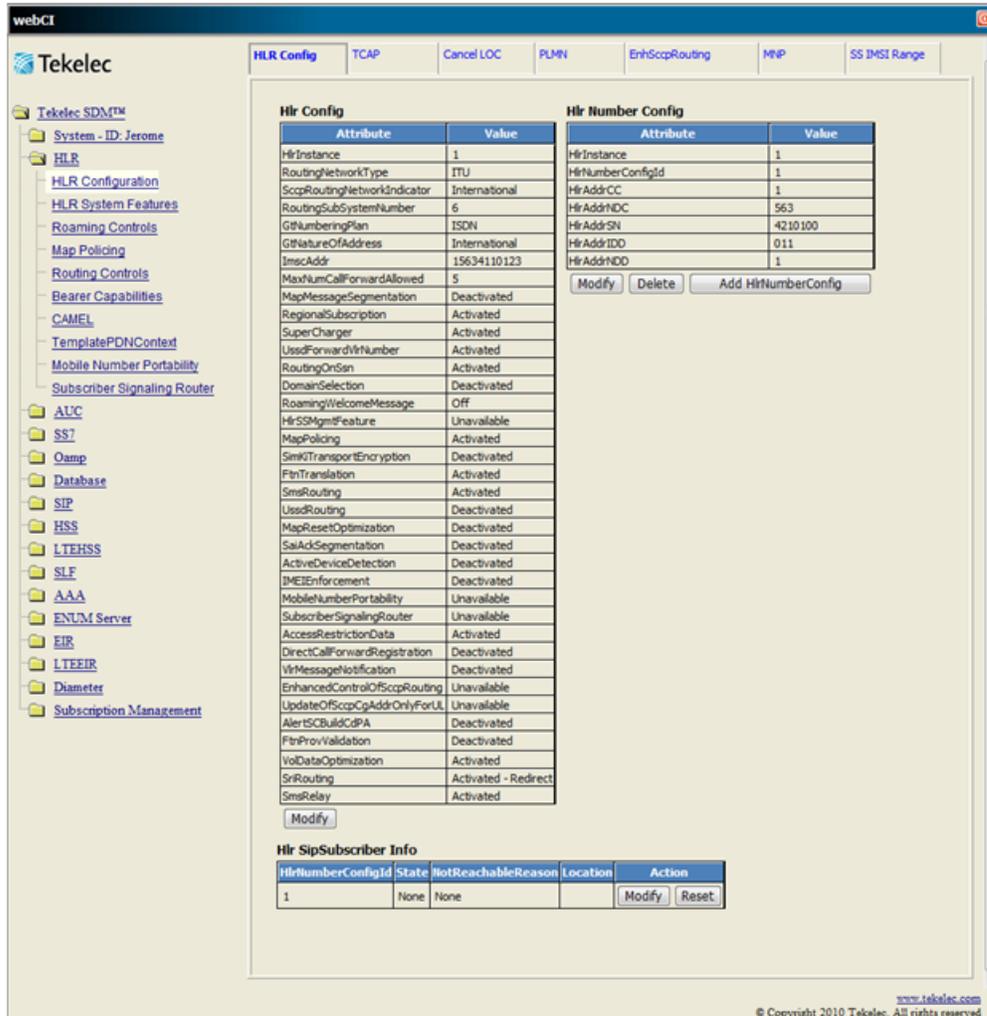
For a description of each window that can be accessed from the WebCI and for a more detailed description of the navigation system in the WebCI, refer to the *Web Craft Interface (WebCI)* section in the *SDM System Configuration - Reference Manual*.

Provisioning a Table

In the WebCI, the system's 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 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. These operations are usually the following:

- **Add**: this operation allows to add an entry in the table. This button usually also specifies what kind of entry it will create (i.e. Add HlrNumberConfig). When the table is empty and hasn't been provisioned yet, this is the only button available. It is usually located underneath the table name or underneath the table, when provisioned with data.
- **Delete**: this operation allows to delete an entry in the table. This operation only becomes available when the table is provisioned. It is usually available for each entry, located in the same row as the entry for which it applies for.
- **Modify**: this operation allows to modify some information already provisioned for an entry in the table. This operation only becomes available when the table is provisioned. It is usually available for each entry, located in the same row as the entry for which it applies for.

Some tables have a **Display/Modify** button. This button allows to display another table (usually a sub-table that can only be provisioned once the main table for which it applies for is already provisioned), which is otherwise hidden. After clicking on this button, the table is displayed or simply the title of the table with the Add button, in the case where this table is not yet provisioned. In some cases, when the sub-table is displayed, the button text changes and becomes: **Hide** <*table name or entry name*> (e.g., Hide HPLMN Country Nodes). This button allows to hide the sub-table.

Some WebCI windows also display buttons that are not specific to a table (e.g., TCAP out of service). 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 information on all the different symbols displayed in the WebCI, refer to the "Operations available" section of the "Web Craft Interface (WebCI)" chapter in the *SDM System Configuration – Reference Manual*.

Hereunder are the procedures that describe step-by-step how to add, display, modify and delete the AuC algorithm table from the WebCI. To provision any other table, follow the same logic as described below, but apply it to the table you wish to provision.

Display a table - AuC Algorithm

This procedure describes how to display a table in the WebCI by using the Authentication (AuC) algorithm files as an example.

1. From the main menu, click on the application folder or the hyperlink next to it, for example, click **AUC**
2. Click the submenu item, for example, click **Algorithm**.
   The submenu item window displays, for example, the Algorithm window with the Algorithm table and all the algorithm files provisioned.

Add an entry - AuC Algorithm

The new algorithm file must be stored in the `/blue/lib` directory prior to running this procedure and it must have a *.so* file extension.

This procedure describes how to add a table entry by using the Authentication (AuC) algorithm files as an example.

1. From the main menu, click on the application folder or the hyperlink next to it, for example, click **AUC**

2. Click the submenu item, for example, click **Algorithm**.
   The submenu item window displays, for example, the AuC Algorithm window.
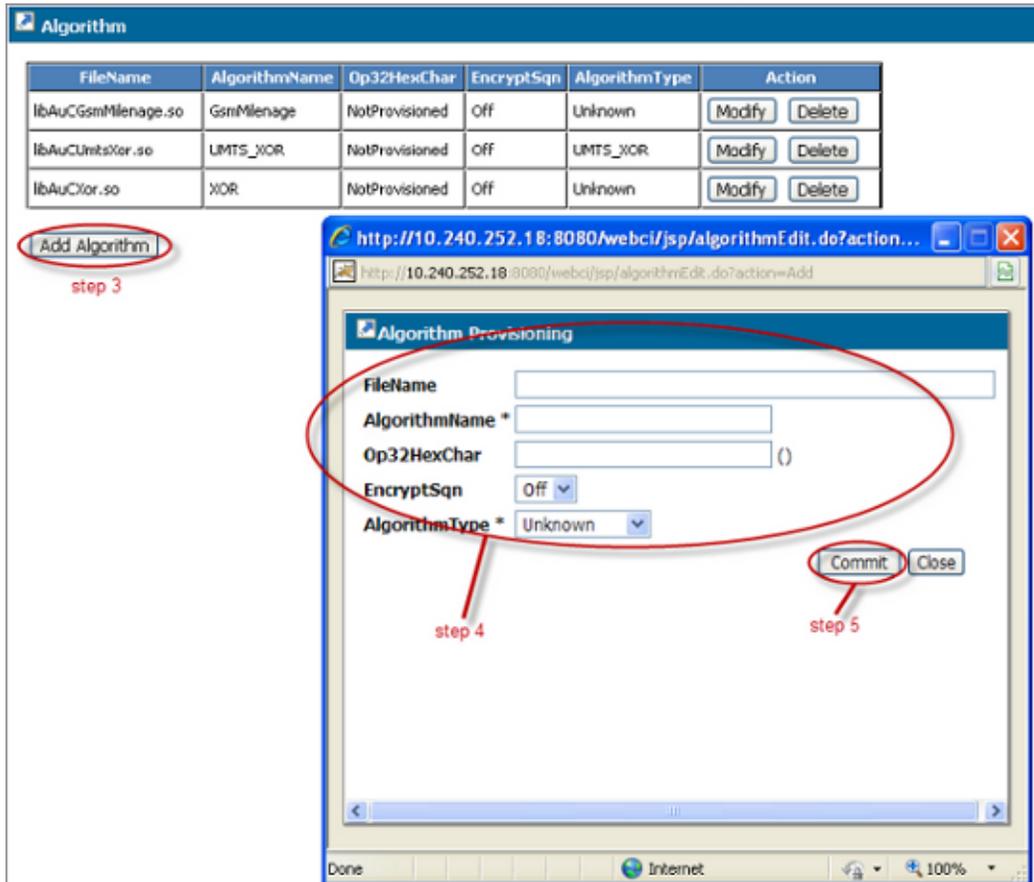
3. Click the **Add** button, for example, click **Add Algorithm**.
   A provisioning pop-up window opens, for example, *Algorithm Provisioning*.

4. Enter the required information, for example, enter the filename, algorithm name, and the Operator-defined GSM milenage algorithm. Select the encryption sequence and the algorithm type.

   For a description of each parameter, value range, and default value, refer to the respective entity in the associated reference manual; for example, for the AUC Algorithm entity, refer to the HLR section in the *SDM System Configuration – Reference Manual*.

5. Click **Commit**.
   The system returns a confirmation message:

   ```
   Algorithm entry was successfully committed
   ```

6. Click **OK**.

Modify an entry - AuC Algorithm

This procedure describes how to modify a table entry by using the Authentication (AuC) algorithm files as an example.

Note:

- The AlgorithmType cannot be modified from Unknown, XOR, Comp128, GsmMilenage to Milenage. However, it can be modified between the four values Unknown, XOR, Comp128 and GsmMilenage.
- If the AlgorithmType is created as Milenage, it cannot be modified. You would need to delete it and recreate it.
- Be careful when modifying the FileName to make sure the library is matching the AlgorithmType.

1. From the main menu, click on the application folder or the hyperlink next to it, for example, click **AUC**

2. Click the submenu item, for example, click **Algorithm**.
   The submenu item window displays, for example, the Algorithm window.
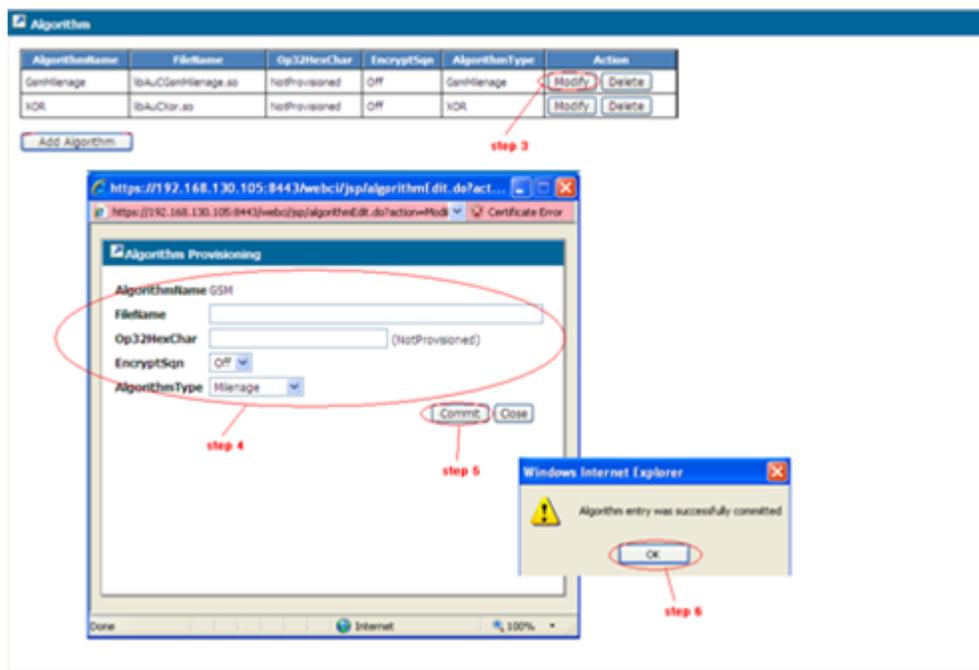
3. Click the **Modify** button next to the algorithm to be modified.
   A provisioning pop-up window opens, for example, *Algorithm Provisioning*.

4. Modify the required information.

5. Click **Commit**.
   The system returns a confirmation message:

   ```
   Algorithm entry was successfully committed
   ```

6. Click **OK**.

Delete an entry - AuC Algorithm

This procedure describes how to delete a table entry in the WebCI by using the Authentication (AuC) algorithm files as an example.

1. From the main menu, click on the application folder or the hyperlink next to it, for example, click **AUC**

2. Click the submenu item, for example, click **Algorithm**.
   The submenu item window displays, for example, the Algorithm window with the Algorithm table and all the algorithm files provisioned.
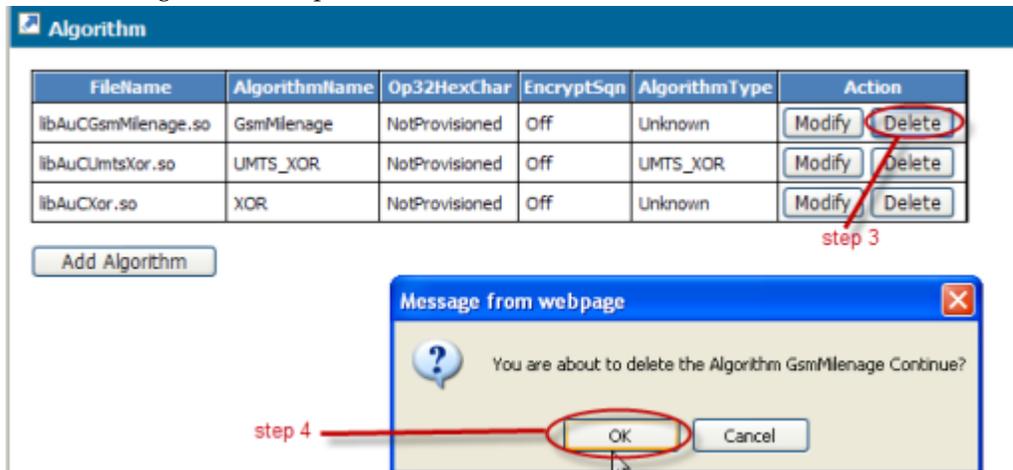
3. Click the **Delete** button next to the algorithm to be deleted.
   The system returns a confirmation message to verify the delete request:

   ```
   You are about to delete the (Name of Algorithm) Continue?
   ```

4. Click **OK**.
   The system returns a confirmation message about the successful deletion:

   ```
   Algorithm entry was successfully deleted
   ```

5. Click **OK**.

Displaying content of a WebCI window through a search engine

Some of the windows in the WebCI, such as the SIP User Agent window, offer a search engine tool that allows the Network Operator to specify the entries that must be displayed in the window's table. The search is done based on the value range specified by the Network Operator for one of the table's parameters. To achieve this, the Network Operator must select the parameter, the operand (>, <, >=, <= or =) and a value.

The procedure hereunder is an example of the steps to follow in order to display the SIP User Agent RegistrationBinding table using the WebCI's search engine. The logic used in this procedure can be used for any WebCI window that requires the search engine to be used in order to display its content.

Displaying WebCI window content using a search

This procedure describes how to display custom content in the WebCI window. The procedure uses the SIP UaRegistrationBinding table as an example.

1. From the main menu, click on the application folder or the hyperlink next to it, for example, click **SIP**

2. Click the submenu item, for example, click **UserAgent**.
   The submenu item window displays with tabs, for example, **User Agent** and **Registration Binding**.
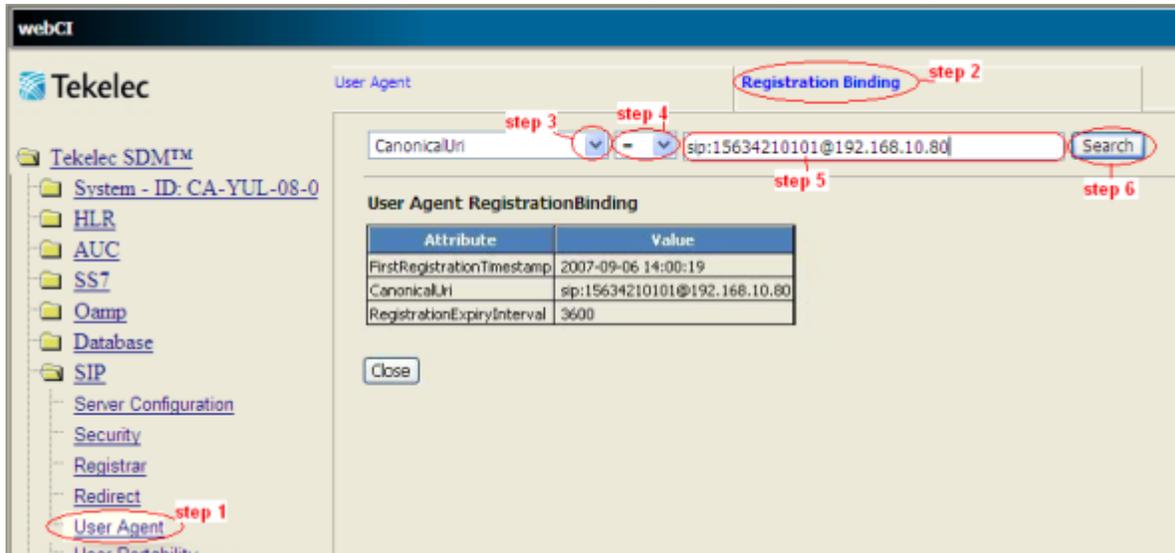
3. Click the **UaRegistrationBinding** tab.

4. Select one of the following RegistrationBinding attributes from the first drop-down menu:

```
CanonicalUri
FirstRegistrationTimestamp
RegistrationExpiryInterval
```

5. Select one of the operands from the next drop-down menu.

   If you wish to search a specific UaRegistrationBinding, select " = ", otherwise select one of the other operands to search a range of UaRegistrationBinding.

6. Select the attribute value from the third drop-down menu.

7. Click **Search**.

   Note: To display all entries, select the '>' operand and write the '0' value.
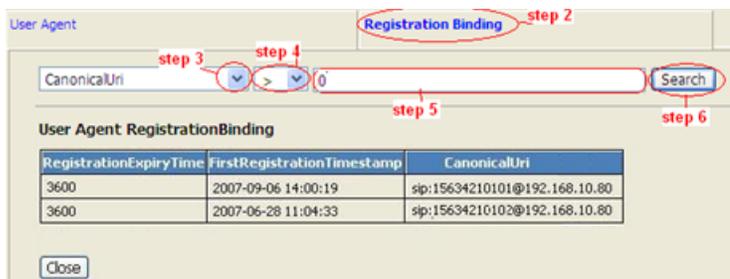
   The search results display the User Agent RegistrationBinding table with one or more RegistrationBindings.

Access Subscriber Provisioning submenu

View and modify subscriber profiles for each application and use the data for troubleshooting.

Subscribers are represented by Subscriptions in the SDM. One subscriber has one single Subscription (SubscriptionID) but can have a subscriber profile for each application supported by the SDM.

The Subscriber Provisioning submenu provides access to all subscriber profiles.

1. From the WebCI main menu, go to **Subscription Management** > **Subscriber Provisioning**. The Subscriber Provisioning window displays.

2. (Optional) Click the **Display The First 25 Subscriptions** button. The Display25Subscriptions window displays a list of the first 25 subscription IDs.

3. Type a Subscription ID into the **SubscriptionID** field and click the corresponding **Search** button. The system returns a hyperlinked button with the subscription ID displayed.

4. Click the **SubscriptionID** hyperlink to go to the Subscriber Provisioning submenu.
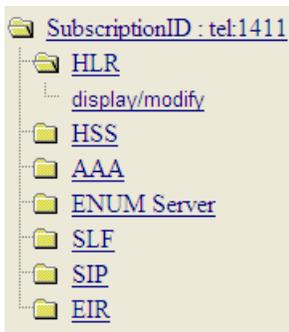
5. Expand the application folder and click **display/modify** to view or edit a profile.

Ending a WebCI session

Log out of a WebCI session by clicking the logout icon (ⓞ) located at the top right corner of the window.

Bulk and Template Provisioning

The Tekelec OAM&P Manager provides provisioning and configuration management. The OAM&P manager accepts XML commands to handle bulk (multiple) requests as well as Template Invoking files.

- Bulk subscriber provisioning is done by first generating a file that contains XML requests (commands). XML provisioning files can only be written and stored in the /tmp folder. Then the commands stored in the file are processed by the command file loader tool (CmdFileLoader). Refer to the SDM Subscriber Provisioning - Reference Manual for details on the XML file and Request types.
- Subscriber provisioning by templates is done by generating a Template Invoking file that contains XML requests of type -Template‖, which means that are based on Templates. These Templates must have already been defined and loaded in the database using the Command Template Loader tool. Template files can only be written and stored in the /tmp folder. It is also possible to view the templates defined in the database with the Command Template Viewer tool. Refer to the SDM Subscriber Provisioning - Reference Manual for details on the XML Template Invoking file.

Preparing template files

Prior to provisioning the Subscriber Data Management system with templates and using the template tools, all templates must be written and validated.

1. Write all template files and invoking files necessary for provisioning.

   Note: Make sure to have an operation request for authentication, which is required to execute an invoking file with the Command File Loader.

   For XML file syntax and a description of what must be defined in each template, refer to the *SDM Subscriber Provisioning - Reference Manual*; for template examples, refer to the XML template section.

2. Open XML file(s) in an XML editor or reader of your choice to validate the basic XML syntax.

   Internet Explorer is a good example of an XML reader that can be used to perform the validation.

   The XML editor or reader will report any errors in the basic syntax. Correct any errors before continuing.

3. Save the template file(s) and the corresponding invoking file(s) in the `/tmp/templates/` directory, for example, `/tmp/templates/Xmlfile1.xml`.

The files are now ready to be uploaded with the Command Template Loader (CTL).

Running Command Template Loader

Prerequisites:

- User must belong to admin, batch, or operation group.

- Template files must be completed and ready for upload. See *Preparing template files*.

The Command Template Loader loads templates into the system database, which allows the operator to provision subscribers with an Invoking file that executes those templates.

1. *Establish Secure Shell (SSh) connection*.

2. Prior to running the Command Template Loader tool, you must first write the templates you wish to load into the system's database and then save them in the /tmp/templates/ directory

   The operator can then run the Command Template Loader (CTL) tool in order to load these templates and the template requests that constitute them.

3. At the prompt, type

   [UserName@system UserName] $ ctl -f <XmlInputFileName.xml>

   where **XmlInputFileName** is the path followed by the name of the Invoking file that is to be executed, for example, /tmp/templates/Xmlfile1.xml).

4. Load the templates one at a time in this order:
   a) Load the Template files, which contain the Command template and all template requests.
   b) Load the Invoking files.

      The Invoking file references the Template file and then provisions the subscribers with the specific values provided.

The template files are now ready to be viewed or executed by the Command File Loader (CFL)

CTL help options

Display the CmdTemplateLoader (CTL) help option by typing **ctl –h**.

These options are available to run the Command Template Loader tool:

- **[-u]** → username to access the database (this should be known at installation)
- **[-p]** → password to access the database(this should be known at installation)
- **[-f XmlInputFileName]** → the XML input file name where the templates is stored
- **[-d XmlInputDirectoryName]** → The directory where the <XmlInputFileName> can be found.
- **[-cmd XmlCommand]** → (i.e. submitted inline) It allow you to directly type your XML command instead of using a file.
- **[-del tp/tpr/all id/all]** → other command line params ignored. allow you to delete a template <tp> or a template request <tpr> or both <all> with the specific id.

  ☞   **Important:** When performing the delete operation with the **all** option, templates and template requests are deleted without any warning or indication.

- **[-dbip]** → the ip address where the database is running
- **[-trace]** → enables the tool traces to view traces for errors)

Deleting a template from the database

Editing a template requires the deletion of the old template from the database and the reloading of the new template. For example, deleting template with template id =1 that refers to a template request with id=100 and a template request with id=101 requires the deletion of all template requests it refers to, one at a time, by entering the following:

* CmdTemplateLoader Execution time: 0 sec

- **[UserName@system UserName] $ ctl –del tpr 101**

- ** TemplateRequest id[100] has been deleted

*CmdTemplateLoader Execution time: 0 sec

Deleting all the template requests referenced by a Command Template deletes the latter. As a result, the template is deleted automatically.

Note: Keep in mind that executing an Invoking file that refers to the Command Template you just deleted will fail.

You can now load into the database the template file you have just edited by using the Command Template Loader.

1. At the prompt, type

   [UserName@system UserName] $ ctl –del tpr 100

   ** TemplateRequest id[100] has been deleted

   * CmdTemplateLoader Execution time: 0 sec

2. Type

   [UserName@system UserName] $ ctl –del tpr 101

   Deleting all the template requests referenced by a Command Template deletes the latter. As a result, the template is deleted automatically.

   Note: Executing an Invoking file that refers to a deleted Command Template will fail.

3. Reload the template. See *Running Command Template Loader*

Running Command File Loader

- User must belong to admin, batch, or operation group.

- Template files must have been uploaded. See *Running Command Template Loader*.

The Command File Loader provisions the subscribers in the database by executing the Invoking files, which reference the template requests.

1. *Establish Secure Shell (SSh) connection* to access the blade.
2. At the prompt, type

   [UserName@system UserName] $ cfl -f <XmlInvokingFileName.xml> to run the Command File Loader

   Where **XmlInvokingFileName** is the path followed by the name of the Invoking file that is to be executed, for example, /tmp/templates/Xmlfile1.xml).

The Command File Loader accepts the Invoking file and then executes it by processing each XML request.

Recommendations for using the Command File Loader

There are a number of limitations associates with the Command File Loader tool. We recommend the following for optimal performance:

- Check the input file for XML syntax errors. Errors in the input file can cause the tool to stop processing. The output file will list the transactions that were completed successfully. Failed transactions will need to be resubmitted.
- Limit the size of the input file to 1.4 GB. Submit small input files in sequence. Large files increase parsing overhead and that consumes CPU resources. The output file is approximately 3 times the size of the input file.
- Review each output log file. See section "Analyzing system reply" for more information.

CFL help options

View the different Command File Loader (CFL) options through this command:

[UserName@system UserName] $ cfl -help

CmdFileLoader options:

- **[-c XmlConfigurationFileName]** (default: default value)
- **[-cmd XmlCommand]** (i.e., submitted inline)
- **[-d XmlCommandDirectoryName]**
- **[-f XmlCommandFileName]**
- **[-fo XmlOutputFileName]** (default: console)

  The **–fo <XmlOutputFileName.xml>** tracks the results of the provisioning request, where **<XmlOutputFileName>** is the path followed by the name of the XML output file in which you wish the system replies be stored (i.e., /tmp/template/Xmloutfile1.xml).

  All system replies are stored in the output file (including error reply codes). Specifying the output file is optional and when no output file name is given, the output is sent automatically to the console by default.

- **[-dbip]** (specifies the IP address of the database).
- **[-ip OampMgrIpAddress]**
- **[-observer]** (i.e., start observer; initiates notifications of changes to the database)
- **[-p OampManagerPort]** (default: 62001)
- **[-reso]** (produce result not encapsulated in xml and no other messages)
- **[-todb]** (i.e., load directly in the database) This is used in bulk provisioning to load subscriber profile information into the database without performing any validation of the xml requests.
- **[-trace]** (traces for errors)
- **[-user]** (user name)
- **[-validate]** (validate input against the global schema)

- **[-c XmlConfigurationFileName]** (default: default value)
- **[-cmd XmlCommand]** (i.e., submitted inline)
- **[-d XmlCommandDirectoryName]**
- **[-f XmlCommandFileName]**
- **[-fo XmlOutputFileName]** (default: console)

The **–fo <XmlOutputFileName.xml>** tracks the results of the provisioning request, where **<XmlOutputFileName>** is the path followed by the name of the XML output file in which you wish the system replies be stored (i.e., `/tmp/template/Xmloutfile1.xml`).

All system replies are stored in the output file (including error reply codes). Specifying the output file is optional and when no output file name is given, the output is sent automatically to the console by default.

- **[-ip OampMgrIpAddress]**
- **[-p OampManagerPort]** (default: 62001)
- **[-reso]** (produce result not encapsulated in xml and no other messages)
- **[-trace]** (traces for errors)
- **[-user]** (user name)
- **[-validate]** (validate input against the global schema)

Analyzing system reply

To verify the provisioning request, view the output file for any errors. Refer to the "System Replies and Error Codes" section of the *SDM Subscriber Provisioning - Reference Manual* for a description of how to interpret the system replies and their error codes.

1. *Establish Secure Shell (SSh) connection*.

2. Perform one of these steps:

    - If you used the **–fo** option and saved the output file, you can view the output file by typing at the prompt

        view /tmp/template/Xmloutfile1.xml to view the templates in the database.

        Note: To exit View Mode, type **q**

    - If you didn't use the **–fo** option, the output data is sent automatically to the console and is only temporarily displayed. Search for the error tag by typing **/error**

3. Then search for the error tag by typing: **/error**

    a) Look for error responses:

        1. `error ="0"` implies no provisioning error occurred.

        2. error ="code #" implies an error with code # occurred. To view the meaning of the error code #, refer to the Database Error Notifications, HLR Error Notifications, and System Error Notifications in the *SDM Monitoring, Troubleshooting, Maintenance - Reference Manual*.

            Note: When provisioning with templates, if an error occurred in one of the template requests, the system returns a general error code that simply informs that an error occurred while processing XML database request (**error# 7029**).

    b) View the actual error by typing **less /blue/var/log/current.xml**.

        View the actual error by typing **less /blue/var/log/sdmlog.xml**.

        This command lists the logs recently generated. In one of the logs, you will see the xml file that was processed with the exact error code.

        Example:

When provisioning the Invoking file with the Command File Loader, the error code 7029 is returned to inform that an error occurred while processing XML database request.

c) Look for the log that contains in its description the template you just ran with the Command File Loader.

d) In the log file, another error code will indicate the problem. For a description of the error code returned, refer to the "Error Notifications" section in the *SDM Monitoring, Troubleshooting, Maintenance - Reference Manual*.

4. Enter **q** to exit the log list and return to the prompt.

⚠️ **WARNING** **Warning:** When using the Tekelec 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 Tekelec 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 Tekelec 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.

XML file syntax using Command File Loader (CFL) for HLR subscriber provisioning

The CFL uses this template (short format) to bulk-provision Tekelec ngHLR subscribers. This Bulk Request file contains insert, update, and delete requests. The requests can be provided on a single line in the XML file. Due to margin limits, the update and delete requests are shown continuing onto subsequent lines as follows.

```
<file>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100000</Imsi><MsIsdnAlertInd>15634210100</MsIsdnAlertInd></ent>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100001</Imsi><MsIsdnAlertInd>15634210101</MsIsdnAlertInd></ent>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100002</Imsi><MsIsdnAlertInd>15634210102</MsIsdnAlertInd></ent>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100003</Imsi><MsIsdnAlertInd>15634210103</MsIsdnAlertInd></ent>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100018</Imsi><MsIsdnAlertInd>15634210104</MsIsdnAlertInd></ent>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100018</Imsi><MsIsdnAlertInd>15634210105</MsIsdnAlertInd></ent>
<ent name = "SubscriberProfile"
ns="bn"><Imsi>31091052100006</Imsi><MsIsdnAlertInd>15634210106</MsIsdnAlertInd></ent>
<req name="update"><ent name = "SubscriberProfile"
ns="bn"/><set><expr><attr name="MsIsdnAlertInd"/> <value val=
"15634210100"/></expr></set><where><expr><attr name="Imsi"/><op
value="="/><value val="0123456789012345"/> </expr></where></req>
<req name="delete"><ent name = "SubscriberProfile"
ns="bn"/><where><expr><attr name="Imsi"/><op value="="/><value val=
"0123456789099999"/></expr></where></req>
</file>
```

XML File Syntax Using Command File Loader for HSS Subscriber Provisioning

The following is an example (short format) of bulk subscriber provisioning for the HSS with a Bulk Request file with insert, update, and delete requests. The requests can be provided on a single line in the XML file. Due to margin limits, the update and delete requests are shown continuing onto subsequent lines as follows. For details on the HSS Subscriber Profile entities, attributes, and their values refer to the *SDM Subscriber Provisioning - Reference Manual*.

```
<file>
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-1</SubscriptionID><ChargingID>ChargingID-1</ChargingID></ent>
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-2</SubscriptionID><ChargingID>
ChargingID-1</ChargingID></ent>
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-3</SubscriptionID><ChargingID>
ChargingID-1</ChargingID></ent>
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-4</SubscriptionID><ChargingID>
ChargingID-2</ChargingID></ent>
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-5</SubscriptionID><ChargingID>
ChargingID-1</ChargingID></ent>
```

```
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-6</SubscriptionID><ChargingID>
ChargingID-2</ChargingID></ent>
<ent name = "HssSubscription"
ns="bn"><SubscriptionID>sub-7</SubscriptionID><ChargingID>
ChargingID-1</ChargingID></ent>
<req name="update"><ent name = "HssSubscription" ns="bn"/><set><expr><attr
 name="ChargingID"/> <value val=
"ChargingID-2"/></expr></set><where><expr><attr name="SubscriptionID"/><op
 value="="/><value val="sub-1"/> </expr></where></req>
<req name="delete"><ent name = "HssSubscription"
ns="bn"/><where><expr><attr name="SubscriptionID"/><op value="="/><value
 val= "sub-7"/></expr></where></req>
</file>
```

Running the Command Template Viewer

- User must belong to admin, batch, or operation group.

- Template files must have been uploaded. See *Running Command Template Loader*.

The Command Template Viewer (CTV) is used to view the templates currently loaded in the database.

1. *Establish Secure Shell (SSh) connection*.

2. Once the user is logged in the blade, in order to use the Command Template Viewer, the user must write the following:

   `[UserName@system UserName] $ ctv –t <tp/tpr> -id <template id>`

3. At the prompt, type

   [UserName@system UserName] $ ctv –t <tp/tpr> -id <template id> to view the templates in the database.

The Command File Loader accepts the Invoking file and then executes it by processing each XML request.

CTV help options

Display the help options of the Command Template Viewer by typing **CmdTemplateViewer -h**

This command displays the options when running the Command Template Loader:

- **[-u]** → username to access the database (this should be known at installation)
- **[-p]** → password to access the database(this should be known at installation)
- **[-t tp/tpr]** → specifies if you want to view a complete template <tp> or a template request <tpr> (i.e. template/template request)
- **[-tid (template id)]** → the id of the target template or template request (digits only)
- **[-dbip]** → the ip address where the database is running

XML Template Invoking File Syntax for HLR Subscriber Provisioning

Once the Templates have been defined and loaded onto the database of the system using the Command Template Loader, it is possible to provision subscribers by creating Template Invoking file(s) that refer to those templates. The following shows an example of a Template Invoking file that refers to the template with an Id=1. For more information on the Template Invoking file fields and attributes, please refer to the *SDM Subscriber Provisioning - Reference Manual*. Refer to that same document for details on the HLR, SIP, HSS and AAA Subscriber Profile entities, attributes, and their values.

```
<tp id="1">
            <tpi nm="Imsi" val="310910421000100"/>
            <tpi nm="MsIsdn" val="15634210100"/>
            <tpi nm="MsIsdnAlertInd" val="15634210100"/>
            <tpi nm="DefaultFtn" val="15634213333"/>
            <tpi nm="SimId" val="234445666000"/>
</tp>
```

Creating and Managing Users for the User Interfaces

With the USM functionality, the SDM user interfaces (CLI, WebCI, XML interfaces) support multiple types of user accounts, which can be managed only by the administrator.

The administrator modifies the access privileges table as needed, for example, when an existing group requires modification.

shows the predefined access privileges entries associated to the six predefined groups (user, operation, surveil, admin, batch, simprov):

Table 11: Access Privileges

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	
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		
ExternalService				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)

Each user belongs to a specific Group that has a specific access to the system's services (entities). Only the Admin Group has full access privileges. The admin user is able to:

- View and modify operational aspects of the system
- Add, delete, modify, and delete subscriber provisioning information
- View and acknowledge system alarms
- View system logs, and performance measurements

Changes made to the system configuration or subscriber provisioning data takes effect immediately. There is no rollback mechanism.

User management using CLI

User management procedures provision users, groups, access privileges, and services. The operator manages users through the CLI at the Security Manager level by performing the following procedures and using the indicated tables:

- Provision users in the User table
- Provision groups in the Group table

- Provision access privileges in the AccessPrivileges table
- Provision services in the Service table

Provisioning users in the User table

The User table defines users and includes user name, password, and group name. Users must be provisioned first in the User table. Users belonging to the Admin group can add, display, modify, and delete users. The exact operations depend on the user interface.

Table 12: User table operations per user interface

CLI	WebCI
Add user	Add user
Modify user	Modify user
Display user	Delete user

All users can change (modify) their passwords. The exact permissions per user group depend on the settings defined in *Creating and Managing Users for the User Interfaces*.

Create User from the CLI

The following CLI procedure shows how to create a user and give it a username and password. This procedure can only be done by the administrator and is recommended to be one of the first things to do once a CLI session is started for the first time. For details on the User parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*. To perform the task in the following table, refer to the procedure for the step by step instructions.

1. Go to the Oamp subsystem by typing,

```
:> Oamp[]
```

2. Go to User Management by typing,

```
Oamp[]> SecurityManager[]
```

3. Add a user as shown below by specifying the UserName and UserPasswd you wish to attribute to the user (i.e. UserName:user2, UserPasswd: #Xseries4users)

```
Oamp[]:SecurityManager[]> add User [UserName=user2; UserPasswd=
#Xseries4users]
```

   The following message will be displayed.

```
Added: 1
```

Display User from the CLI

The following CLI procedure displays the steps on how to view the User table, its UserName, UserId and GroupId. It is important to note that the UserPasswd is confidential and cannot be viewed.

1. Go to the Oamp subsystem by typing,

```
:> Oamp[]
```

2. Go to User Management by typing,

```
Oamp[]> SecurityManager[]
```

3. To display the entire User Table, go to User without specifying any attributes, as follows:

```
Oamp[]> SecurityManager[]> User[]
```

To display the User Table only for specific users, go to User and specify the user's name (i.e. UserName: user):

```
Oamp[]> SecurityManager[]> User[UserName=user]
```

4. Display the User Table by typing:

```
Oamp[]> SecurityManager[]> User[]> display
or
Oamp[]> SecurityManager[]> User[UserName=user]> display
```

Information similar to the following will be displayed if you displayed the entire User Table:

```
|  UserName|  UserPasswd       |  GroupName       |
----------------------|---------------------------
user         |                |       user         |
operation    |                |       operation    |
surveil      |                |       surveil      |
admin        |                |       admin        |
batch        |                |       batch        |
simprov      |                |       simprov      |
user2        |                |       user         |


Displayed: 7
```

Information similar to the following will be displayed if you only displayed a specific user:

```
|UserName      |UserPasswd             |GroupName|
-----------------------------------
user          |                       |     user |
Displayed: 1
```

Modify user from the CLI

Each user can modify the user password by entering a new value of the password in the User[] entity.

Only the system administrator can modify:

- The password of each user.
- The group to which a user is associated by modifying the GroupName field.
- The UpgradeMode and the PersistOS (whether to store the user information in the Operating System)

This procedure describes how to modify any user information from the User[ ] entity. For details on User parameters, refer to the *User Management through CLI* section of the *SDM System Configuration - Reference Manual*.

1. Go to the Oamp subsystem by typing

```
:> Oamp[]
```

2. Go to User Management by typing

```
Oamp[]> SecurityManager[]
```

3. Specify the user for which you wish to modify information (i.e., UserName=user2). Type

```
Oamp[]:SecurityManager[]> User [UserName=user2]
```

4. Modify the user specified in the previous step by executing the modify command and specifying the fields you wish to modify and their new values. For example, type

```
Oamp[]:SecurityManager[]> User [UserName=user2]> modify .
Password=Xseries4users]
```

   The following message displays:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

5. Type **y** if you wish to continue or **n** if you wish to cancel
   If you typed **y**, the following message displays:

```
Modified:1
```


Provisioning groups in the Group table

The Group table defines a user group based on system use and common access privileges and permissions. Each group consists of a group name and the access granted for each service.

The Subscriber Data Management system pre-defines six groups with certain access privileges for each service: user, operation, surveil, admin, batch, and simprov. The user group can be displayed by all users, but only the administrator can display, add, modify, or delete access privileges of each service associated to the group. See also *Table 11: Access Privileges*.

Provisioning groups from the CLI

The following CLI procedure is a generic procedure on how to provision the Group entity. Follow this logic whether you wish to add/display/modify/delete an entry in the Group[ ] entity.

1. Go to the Oamp subsystem by typing,

```
:> Oamp[]
```

2. Go to User Management by typing,

```
Oamp[]> SecurityManager[]
```

3. From here, you can add/display/delete/modify an entry in the Group entity. Perform one of the following actions, as needed:

   • To display the Group entity, perform the following:

```
Oamp[]> SecurityManager[]> display Group[]
```

   • To display a specific entry in the Group entity, simply specify the GroupName of the group you wish to display, as follows:

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

   • To add an entry, perform the following (i.e.: GroupName: usergroup1):

```
Oamp[]> SecurityManager[]> add Group[GroupName=usergroup1]
```

   • To modify an entry, specify the GroupName of the group you wish to modify and perform the 'modify' command with the attributes you wish to modify and their new values (i.e.: modify the PersistOS from '0' (Off) to '1' (On):

```
Oamp[]> SecurityManager[]> Group[GroupName=usergroup1]> modify . PersistOS=1
```

   • To delete an entry, simply specify the GroupName of the group you wish to delete, as follows:

```
Oamp[]> SecurityManager[]> delete Group[GroupName=usergroup1]
```

4. Depending on the action taken in the previous step, the CLI will return one of the following messages:

```
This Command could potentially display a very large number of instances.
Proceed with display? (y/[n]):

or

Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

5. Type in 'y' if you wish to continue or 'n' if you wish to cancel.
6. If you typed 'y', the result will be displayed.

Provisioning access privileges in the Access Privileges table

The Access Privileges table defines access privileges for a user group by making an association between a user group, a service, and access permissions. Each access privilege gives a single group access permission to a single service. Only the administrator can modify the AccessPrivileges table.

Each service has its own associated entities based on functionalities; see Table *Predefined services and associated entities* in the *SDM System Configuration Reference Manual*. All services are predefined in the system with these access permissions: Read, Write, and Execute. Services cannot be created or modified.

The Subscriber Data Management system pre-defines six groups with certain access privileges for each service: user, operation, surveil, admin, batch, and simprov. The user group can be displayed by all users, but only the administrator can display, add, modify, or delete access privileges of each service associated to the group. See also *Creating and Managing Users for the User Interfaces*.

These access privileges operations are available per user interface and associated table:

Table 13: Access privileges operations per user interface

CLI SecurityAccessPrivileges table	WebCI UserAccessPrivileges table
Display access privileges	Display access privileges
Modify access privileges	Modify access privileges
	Display All Groups

Displaying access privileges from the CLI

This CLI procedure displays the AccessPrivileges table with GroupId, ServiceId, and Permission.

1. Go to the Oamp subsystem by typing **:> Oamp[]**

2. Continue to User Management by typing **SecurityManager[]**

3. Continue to Group and specify the GroupName (i.e., GroupName: admin) to display its associated AccessPrivileges table. Type **Group[GroupName=admin]**

4. To display the entire AccessPrivileges table associated to the specified Group, type **display SecurityAccessPrivileges []**
    The complete syntax is shown below:

```
Oamp[]> SecurityManager[]>Group[GroupName=admin]> display SecurityAccessPrivileges
 []
```

To display a specific entry of the SecurityAccessPrivileges table for the specified Group, specify the ServiceId, Permission, or both attributes, for example, type **display SecurityAccessPrivileges [ServiceName=HlrConfig]**

• If you displayed the entire AccessPrivileges table, the system returns information similar to the one shown below:

```
ServiceName      | GroupName |   Permission     |
----------------------------------------
 Database        |   admin   |ReadWriteExecute|
 ExternalService |   admin   |ReadWriteExecute|
```

```
HlrConfig        |   admin    |ReadWriteExecute|
HlrSimProv       |   admin    |ReadWriteExecute|
HlrSubsProv      |   admin    |ReadWriteExecute|
HssConfig        |   admin    |ReadWriteExecute|
Oamp             |   admin    |ReadWriteExecute|
Policy           |   admin    |ReadWriteExecute|
Schema           |   admin    |ReadWriteExecute|
SipConfig        |   admin    |ReadWriteExecute|
SipSubsProv      |   admin    |ReadWriteExecute|
Ss7Config        |   admin    |ReadWriteExecute|
subscriberProv   |   admin    |ReadWriteExecute|
System           |   admin    |ReadWriteExecute|
user             |HssSubsProv |ReadWriteExecute|

Displayed: 15
```

- If you displayed only a specific group, the system returns information similar to the one shown below:

```
GroupName: admin
ServiceName: HlrConfig
Permission: ReadWriteExecute
```

Modify AccessPrivileges from the CLI

This procedure describes how to modify the SecurityAccessPrivileges table. The only modifiable attribute of the SecurityAccessPrivileges table is the Permission attribute.

1. Go to the Oamp subsystem by typing

```
:> Oamp[]
```

2. Go to User Management by typing

```
Oamp[]> SecurityManager[]
```

3. Go to Group and specify the GroupName (i.e., GroupName: batch) of the Group for which you would like to modify the associated AccessPrivileges table.

```
Oamp[]> SecurityManager[]> Group[GroupName=batch]
```

4. Go to AccessPrivileges by typing

```
Oamp[]> SecurityManager[]> Group[GroupName=batch]> SecurityAccessPrivileges
[]
```

5. Modify the AccessPrivileges table by specifying the Permission attribute and providing its new value (i.e, Permission: ReadWriteExecute):

```
Oamp[]> SecurityManager[]> Group[GroupName=batch]> SecurityAccessPrivileges []>
 modify . Permission=ReadWriteExecute
```

The following warning displays:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

6. Type **y** to proceed.

    The following message displays:

```
Modified: 1
```

Provisioning services in the Service table

The Service table adds, displays, modifies, and deletes external services.

The Subscriber Data Management system pre-defines internal services and their associated entities; see Table *Predefined services and associated entities* in the *SDM System Configuration Reference Manual*. Any user can display these services within the Service table.

WARNING

Warning: Pre-defined services cannot be deleted by any user (including the system administrator) because deleting these internal services could impact the system.

The system administrator can define other services for external entities by adding them manually to the Global Schema. To assign external entities to a newly defined service, the system administrator must define the association when creating a new entity in the Global Schema (contact the Tekelec *My Oracle Support (MOS)* for assistance).

The system administrator can then

- modify the description given to these services
- delete the newly added services

Provisioning services from the CLI

This procedure describes how to provision the Service[ ] entity using the add, display, modify, or delete operation.

1. Go to the Oamp subsystem by typing

```
:> Oamp[]
```

2. Go to User Management by typing

```
Oamp[]> SecurityManager[]
```

3. Perform one of the following actions:

    - To display the Service entity, type **display**:

```
Oamp[]> SecurityManager[]> display Service[]
```

- To display a specific entry in the Service entity, type **display** and specify the ServiceName of the service to display:

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

- To add an entry, type **add** and specify the ServiceName with the ExternalService value, which regroups the ExternalServiceManager entity):

```
Oamp[]> SecurityManager[]> add Service[ServiceName=ExternalService]
```

- To modify an entry, type **modify** and specify the ServiceName of the group to modify:

```
Oamp[]> SecurityManager[]> Service[ServiceName=ExternalService]> modify .
Description=service regrouping external services
```

- To delete an entry, specify the ServiceName of the service to delete:

```
Oamp[]> SecurityManager[]> delete Service[ServiceName=ExternalService]
```

Warning: The pre-defined services cannot be deleted by any user (including the system administrator) since these are internal services and a deletion could impact the system.

Depending on the action taken in the previous step, the CLI will return one of the following messages:

```
This Command could potentially display a very large number of instances.
Proceed with display? (y/[n]):

Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

4. Type **y** if you wish to continue; type **n** if you wish to cancel.
If you typed **y**, the result displays.

User management using WebCI

User management procedures provision users, groups, access privileges, and services. The operator manages users through the WebCI in the User Manager by performing the following procedures and using the indicated windows or tables:

- View all User Management information in the User Manager window
- Provision users in the User table
- Provision groups in the Group table
- Provision access privileges in the AccessPrivileges table
- Provision services in the Service table

View all User Management Information from the WebCI

This procedure describes how to display the User Manager window.

The User Manager window displays all user management information.

1. From the main menu, go to **Oamp** > **UserManager**.

   The User Manager window displays the tables required for user management provisioning.

Figure 8: User Manager Window

2. View additional tables by clicking the hyperlinks.

   - To view the AccessPrivileges table for a Group name, click the Group name in the Group table. To return to the User Manager window, click the **Display All Groups** button.
   - To view Services parameters, click the Services name in the Service table. To return to the User Manager window, click the **Display All Services** button.

Provisioning users in the User table

The User table defines users and includes user name, password, and group name. Users must be provisioned first in the User table. Users belonging to the Admin group can add, display, modify, and delete users. The exact operations depend on the user interface.

Table 14: User table operations per user interface

CLI	WebCI
Add user	Add user
Modify user	Modify user
Display user	Delete user

All users can change (modify) their passwords. The exact permissions per user group depend on the settings defined in *Creating and Managing Users for the User Interfaces*.

Creating User from the WebCI

The following WebCI procedure shows how to create a user, give it a username and password, and associate a group to it. This procedure can only be done by the administrator and is

recommended to be one of the first things to do once a WebCI session is started for the first time. For details on the User parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*.

1. From the main menu, navigate to **Oamp** > **User Manager**.
   The User Manager window displays.
2. Click the **Add User** button below the User table.
   The User Provisioning pop-up window displays.
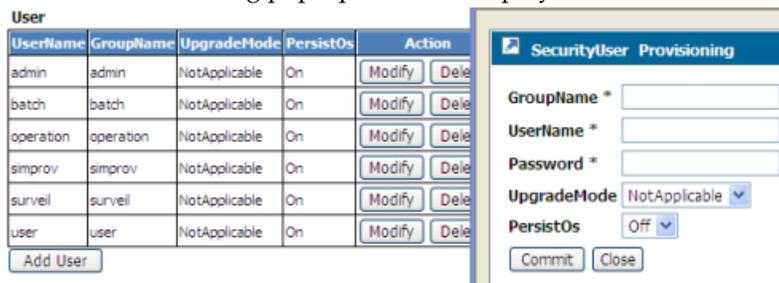
3. Enter the information to be added (the asterisk (*) identifies a mandatory attribute).
4. Click **Commit**.
   The system returns a confirmation message `User entry was successfully committed`
5. Click **OK**.

Modifying a User from the WebCI

Each user can modify its own password by modifying the User[ ] entity and entering the value of the new password desired. However, only the administrator of the system can modify the following:

- The password of each user.
- The group to which a user is associated to, by modifying the GroupName field.
- The UpgradeMode and the PersistOS (to store or not the user information in the Operating System)

The following WebCI procedure shows how to modify any user information from the User[ ] entity. For details on the User parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual.* To perform the task in the following table, refer to the procedure for the step by step instructions.

1. From the main menu, navigate to **Oamp** > **User Manager**. This will display the User Manager window (as shown in the figure below)
2. Click the **Modify** button beside the User entry of the User you wish to modify.
3. When the User Provisioning window appears (see figure below), enter the new value(s).

   Note: The figure below is for the administrator of the system. The other users can only modify the Password.

Figure 9: User Provisioning Window to Modify a User

4. Click **Commit** when all the information has been entered.

5. When the confirmation message "`UserProfile entry was successfully committed`" appears, click **OK**.

Deleting a User from the WebCI

The administrator can delete a user entry from the WebCI. The following WebCI procedure shows how to modify any user information from the User[ ] entity. For details on the User parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual.* To perform the task in the following table, refer to the procedure for the step-by-step instructions.

1. From the main menu, navigate to **Oamp** > **User Manager**. This will display the User Manager window.

2. Click the **Delete** button beside the User entry of the User you wish to delete

3. The following message is returned: "`You are about to delete this entry, Continue?`"

4. Click '**OK**' if you wish to continue or '**Cancel**' otherwise.

Provisioning groups in the Group table

The Group table defines a user group based on system use and common access privileges and permissions. Each group consists of a group name and the access granted for each service.

The Subscriber Data Management system pre-defines six groups with certain access privileges for each service: user, operation, surveil, admin, batch, and simprov. The user group can be displayed by all users, but only the administrator can display, add, modify, or delete access privileges of each service associated to the group. See also *Table 11: Access Privileges*.

Display groups from the WebCI

This procedure describes the steps to view the Group table, all of the groups defined in the system. For details on the Group attributes, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*.

1. From the main menu, navigate to **Oamp** > **User Manager**.

2. This will display the User Manager window (as shown in User Manager window).

   The Group table displays all of the groups defined in the system.

Create a group from the WebCI

This procedure creates a group and defines access privileges by provisioning permissions for each service.

Only the system administrator has permission to perform this procedure.

1. From the main menu, navigate to **Oamp** > **User Manager**.

    The User Manager window displays.

2. Click the **Add Group** button below the Group table.
    The SecurityGroup Provisioning pop-up window displays.
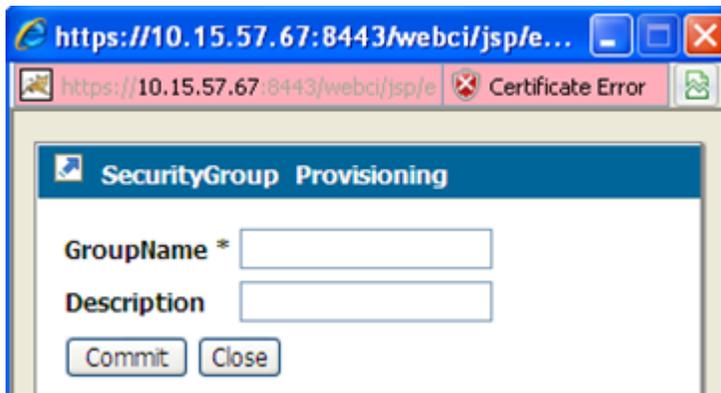
3. Enter the information; the asterisk (*) identifies a mandatory attribute.

4. Click **Commit**.
    The system returns a confirmation message `User entry was successfully committed`

5. Click **OK**.

Modifying a group from the WebCI

The administrator of the system i s the only one that can modify the groups and the description is the only field that can be modified from the Group table.

The following WebCI procedure shows how to modify a group entry from the Group[ ] entity. For details on the User parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual.* To perform the task in the following table, refer to the procedure for the step by step instructions.

1. From the main menu, navigate to **Oamp** > **User Manager**. This will display the User Manager window.

2. Click the **Modify** button beside the Group entry of the group you wish to modify.

3. When the Group Provisioning window appears (see figure below), enter the new description you wish to give to the group.
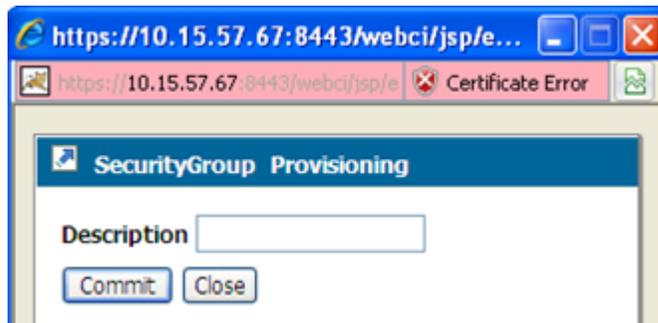
Figure 10: Group Provisioning Window to Modify a Group

4. Click **Commit** when all the information has been entered.

5. When the confirmation message "Entity entry was successfully committed" appears, click **OK**.

Delete a group from the WebCI

The administrator of the system can delete a group entry from the WebCI's Group table. The following WebCI procedure shows how to delete a group from the Group[ ] entity. For details on the Group parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*. To perform the task in the following table, refer to the procedure for the step by step instructions.

1. From the main menu, navigate to **Oamp** > **User Manager**. This will display the User Manager window.

2. Click the **Delete** button beside the Group entry of the group you wish to delete.

   The following message is returned: "You are about to delete this entry, Continue?"

3. Click '**OK**' if you wish to continue or '**Cancel**' otherwise.

Provisioning access privileges in the Access Privileges table

The Access Privileges table defines access privileges for a user group by making an association between a user group, a service, and access permissions. Each access privilege gives a single group access permission to a single service. Only the administrator can modify the AccessPrivileges table.

Each service has its own associated entities based on functionalities; see Table *Predefined services and associated entities* in the *SDM System Configuration Reference Manual*. All services are predefined in the system with these access permissions: Read, Write, and Execute. Services cannot be created or modified.

The Subscriber Data Management system pre-defines six groups with certain access privileges for each service: user, operation, surveil, admin, batch, and simprov. The user group can be displayed by all users, but only the administrator can display, add, modify, or delete access privileges of each service associated to the group. See also *Creating and Managing Users for the User Interfaces*.

These access privileges operations are available per user interface and associated table:

Table 15: Access privileges operations per user interface

CLI **SecurityAccessPrivileges table**	WebCI **UserAccessPrivileges table**
Display access privileges	Display access privileges
Modify access privileges	Modify access privileges
	Display All Groups

Display AccessPrivileges table from the WebCI

This procedure describes how to display the AccessPrivileges table associated to a specific Group.

1. From the main menu, navigate to **Oamp** > **User Manager**.
    The User Manager window displays the Group table.
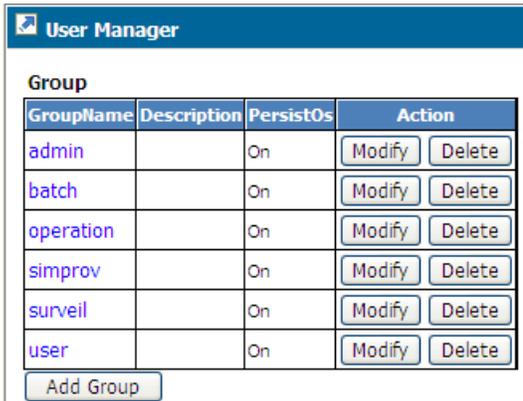
2. In the Group table, click the GroupName hyperlink (blue) to display the associated AccessPrivileges table.
    The UserAccessPrivileges Provisioning window displays service names and permissions.

3. Click **Display All Groups** to return to the User Manager window.

Modify Access Privileges from the WebCI

This procedure describes the steps to modify the AccessPrivileges table associated to a specific Group. Only the administrator can modify the permissions assigned to specific services for each Group. For details on the AccessPrivileges Management attributes, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*.

1. From the main menu, navigate to **Oamp** > **User Manager**.

   This will display the User Manager window (as shown below).

2. In the Group table, click on the **GroupName** (written in blue) of the Group to which you would like to modify the associated AccessPrivileges table.

3. When the UserAccessPrivileges Provisioning window appears, select the new permission you want to give to that Group for each service to which you wish to modify the permission.

ServiceName	Permission
HlrConfig	ReadWriteExecute
HlrSimProv	ReadWriteExecute
HlrSubsProv	ReadWriteExecute
HssConfig	ReadWriteExecute
HssSubsProv	ReadWriteExecute
Oamp	Read
SipConfig	ReadWriteExecute
SipSubsProv	ReadWriteExecute
Ss7Config	ReadWriteExecute
SubscriberProv	ReadWriteExecute
System	Read
Database	Unprovision
ExternalService	Unprovision
Policy	Unprovision
Schema	Unprovision
SystemValidation	Unprovision

Figure 11: UserAccessPrivileges provisioning window

4. Click **Commit** when all the changes have been entered.

5. When the confirmation message

```
UserAccessPrivileges entry was successfully committed
```

appears, Click **OK**.

6. Click **Display All Groups** to return to the User Manager window.

Provisioning services in the Service table

The Service table adds, displays, modifies, and deletes external services.

The Subscriber Data Management system pre-defines internal services and their associated entities; see Table *Predefined services and associated entities* in the *SDM System Configuration Reference Manual*. Any user can display these services within the Service table.

Warning: Pre-defined services cannot be deleted by any user (including the system administrator) because deleting these internal services could impact the system.

WARNING

The system administrator can define other services for external entities by adding them manually to the Global Schema. To assign external entities to a newly defined service, the system administrator must define the association when creating a new entity in the Global Schema (contact the Tekelec *My Oracle Support (MOS)* for assistance).

The system administrator can then

• modify the description given to these services
• delete the newly added services

Display services from the WebCI

This procedure describes how to view the Service table with all of the services defined in the system. For details on the Services attributes, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*.

1. From the main menu, navigate to **Oamp** > **User Manager**
   The User Manager window displays including the Services table. The Service table displays all the services defined in the system.

Service

ServiceName	Description	Action	
Database		Modify	Delete
ExternalService		Modify	Delete
HlrConfig		Modify	Delete
HlrSimProv		Modify	Delete
HlrSubsProv		Modify	Delete
HssConfig		Modify	Delete
HssSubsProv		Modify	Delete
Oamp		Modify	Delete
Policy		Modify	Delete
Schema		Modify	Delete
SipConfig		Modify	Delete
SipSubsProv		Modify	Delete
Ss7Config		Modify	Delete
SubscriberProv		Modify	Delete
System		Modify	Delete
SystemValidation		Modify	Delete

Add Service

2. Click the hyperlink of the service name to display the entities for this service.

Creating a service from the WebCI

The administrator of the system can define services (service name and description) for external entities (entities manually added in the Global Schema by the system administrator) through the WebCI's Service table (e.g., ServiceName: 'ExternalService', which regroups the ExternalServiceManager entity).

In order to assign external entities to a newly defined service, the system administrator must define the association when creating new entities in the Global Schema (contact the Customer Care Center for assistance).

The following WebCI procedure shows how to create a new service. For details on the Service entity's parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*.

1. From the main menu, navigate to **Oamp** > **User Manager**. This will display the User Manager window.

2. Click the **Add Service** button below the Service table.

3. When the Service Provisioning window appears (see figure below), enter the information to be added (the '*' identifies a mandatory attribute).
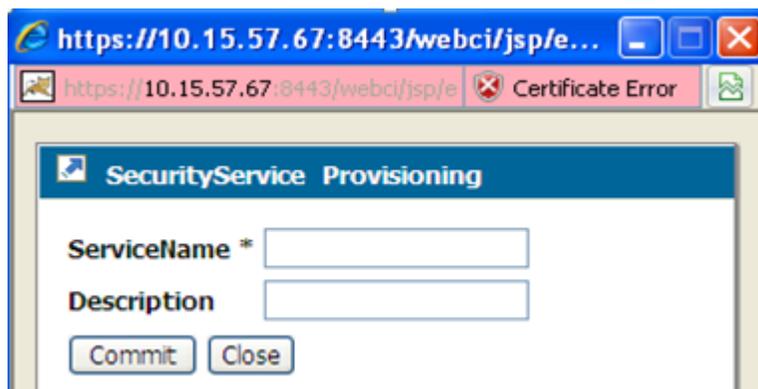
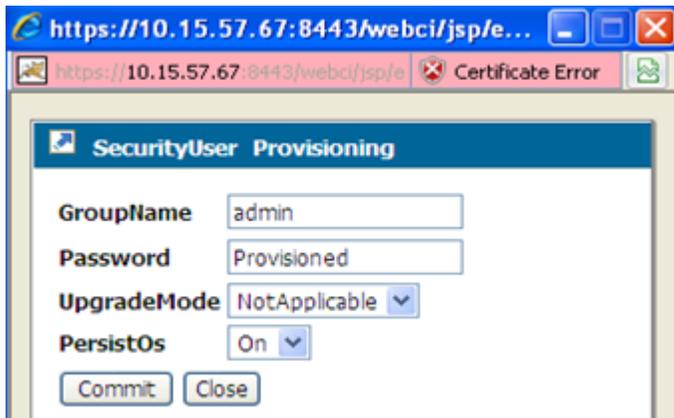**Figure 12: Service Security Provisioning Window**

4. Click **Commit** when all the information has been entered.

5. When the confirmation message "Entity entry was successfully committed" appears, click **OK**.

Modifying a service from the WebCI

The administrator of the system can modify the description given to each service.

The following WebCI procedure shows how to modify a service entry from the Service[ ] entity. For details on the Service parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*.

To perform the task in the following table, refer to the procedure for the step-by-step instructions.

1. From the main menu, navigate to **Oamp** > **User Manager**. This will display the User Manager window.
2. Click the **Modify** button beside the Service entry of the service you wish to modify.
3. When the Service Provisioning window appears, enter the new description you wish to give to the service.
4. Click **Commit** when all the information has been entered.
5. When the confirmation message "Entity entry was successfully committed" appears, click **OK**.

Deleting a service from the WebCI

The pre-defined services cannot be deleted by any user (including the administrator of the system) since these are internal services and a deletion could impact the system. However, the administrator of the system can delete services that he has added himself that regroup external entities (not pre-defined ones).

The following WebCI procedure shows how to delete a service from the Service[ ] entity. For details on the Service parameters, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual*. To perform the task in the following table, refer to the procedure for the step by step instructions.

1. From the main menu, navigate to **Oamp** > **User manager**. This will display the User Manager window.
2. Click the **Delete** button beside the Service entry of the service you wish to delete.
3. The following message is returned: "You are about to delete this entry, Continue?"
4. Click **OK** if you wish to continue or **Cancel**, otherwise.

Creating and Managing Users for Notifications

The Notification Management functionality allows the management of users with notification subscription permissions for specific applications, entities and parameters.

The CLI and WebCI support multiple types of user accounts, which can only be managed by the administrator. For an external application to be able to subscribe to notifications for specific applications/entities/attributes, it must have a user account defined by the SDM system administrator with a username, password and application name. The SDM system administrator must associate applications to user accounts, by provisioning the UserApplicationMap[ ] entity. The users must first

be defined in the User[ ] entity and the applications must also be defined with notification subscription permissions for each entity/attribute as as well as with notification properties. This can be provisioned in the ApplicationIdentity[ ], NotificationSubscribe[ ] and ApplicationProperty[ ] entities. Take note that one user can have multiple applications associated to it, which allows the user to subscribe notifications for various applications.

For more details on the system's behavior, refer to the "Security Management" section of the *SDM Product Description*. For more details on the entities to provision for Notification Management, refer to the "Notification Security Management" section of the *SDM System Configuration - Reference Manual*.

Take note that changes made to the system configuration or subscriber provisioning data take effect immediately. There is no rollback mechanism.

Notification Management Using CLI

Notification management requires the provisioning of users, their applications, and notification subscriptions/properties. Use these procedures:

- Provision applications
- Provision notification subscription permissions
- Provision notification properties
- Provision users

Requirements: All CLI provisioning procedures require the operator to log into a CLI session with a valid username and password.

Define/Provision applications from the CLI

The following CLI procedure shows how the system's administrator can provision applications in the ApplicationIdentity[ ] entity.

1. Go to the Oamp subsystem by typing,

```
:> Oamp[]
```

2. Go to Notification Management by typing,

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

3. Provision the ApplicationIdentity[ ] entity by performing one of the following commands, as needed:

   - Display the applications provisioned in the ApplicationIdentity[ ] entity by performing the following:

```
Oamp[]> NotificationManager[]> display ApplicationIdentity[]
```

   - Add an application by performing the following:

```
Oamp[]:NotificationManager[]> add ApplicationIdentity[ApplName=interface2]
```

The following message will be displayed:

```
Added: 1
```

- Modify an application by performing the following and specifying the new value:

```
Oamp[]:NotificationManager[]> ApplicationIdentity[ApplName=interface2]> modify
. Description=RESTful interface
```

The following message will be returned:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

Type **y** if you wish to continue or **n** to cancel.

- Delete an application by performing the following:

```
Oamp[]:NotificationManager[]> delete ApplicationIdentity[ApplName=interface2
```

The following message will be returned:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

Type **y** if you wish to continue or **n** to cancel.

Provision notification subscription permissions from the CLI

1. Go to the Oamp subsystem by typing **:> Oamp[]**
2. Go to User Management by typing **NotificationManager[]**

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

3. Provision the NotificationSubscribe[ ] entity by performing one of the following commands:
   - Display entities and attributes to which notifications can be subscribed for a specific application by typing **Oamp[]> NotificationManager[]> ApplicationIdentity[ApplName=BlueCli] >display NotificationSubscribe[]**
   - Add an entity or attribute to which notifications can be subscribed for a specific application by typing **Oamp[]> NotificationManager[]> ApplicationIdentity[ApplName=BlueCli] > add NotificationSubscribe[Namespace=bn; Entity=MSISDN; Attribute=DefaultBsg]**

     The following message displays:

```
Added: 1
```

   - Delete notification properties for an application by typing **Oamp[]> NotificationManager[]> ApplicationIdentity[ApplName=BlueCli] > delete NotificationSubscribe[Namespace=bn; Entity=MSISDN; Attribute=DefaultBsg]**

The following message displays:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

Type **y** to continue or **n** to cancel.

Provisioning notification properties from the CLI

Notification properties define per application whether the previous value (before update) must be
included in the notifications in addition to the current value (after update). The administrator defines
these properties in the ApplicationProperty[ ] entity.

1. Go to the Oamp subsystem by typing,

```
:> Oamp[]
```

2. Go to Notification Management by typing

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

3. Provision the ApplicationProperty[ ] entity by performing one of the following commands, as
   needed:

   • Display an application's notification properties, by performing the following:

```
Oamp[]> NotificationManager[]> ApplicationIdentity[ApplName=BlueCli] > display
 ApplicationProperty[]
```

   • Add notification properties to an application, by performing the following:

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

   The following message will be displayed:

```
Added: 1
```

   • Delete notification properties for an application, by performing the following:

```
Oamp[]> NotificationManager[]> ApplicationIdentity[ApplName=BlueCli] > delete
ApplicationProperty[Namespace=bn; Entity=MSISDN; isValueBefore=1]
```

   The following message will be returned:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

4. Type **y** if you wish to continue or **n** to cancel.

Provisioning Users

By default, the system pre-defines these users in the User table: user, operation, surveil, admin, batch and simprov. Each of these pre-defined users are associated with an application in the UserApplicationMap table.

Table 16: UserApplicationMap table

User	Applications associated to each user at installation (pre-defined)
User	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Operation	BlueCli, WebCI, LdapDataServer
Surveil (surveillance)	BlueCli, WebCI, LdapDataServer
Admin	BlueCli, WebCI, SOAP, CmdFileLoader, SNMP, LdapDataServer
Batch	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Simprov	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer

The administrator can display, add, or delete user-application combinations and modify their logging options. For an external application to be able to subscribe to notifications for specific applications, entities, or attributes, it must have a user account defined by the SDM system administrator with a username, password (in the User[ ] entity) and application name (user-application association defined in the UserApplicationMap[ ] entity). For the defined user accounts (in User[ ] entity), the SDM system administrator must associate them with applications by provisioning the UserApplicationMap[ ] entity.

Note: The application must already be defined in the ApplicationIdentity[ ] entity (see previous sub-sections).

These procedures define users and associate applications to them by provisioning the UserApplicationMap table. Users can create and display the User table, modify user passwords, and assign a group to each user.

For details on the User table, refer to the "Notification Security Management through CLI" section of the *SDM System Configuration - Reference Manual*.

WebCI	CLI
Creating user	Provisioning users
Modifying user	
Deleting user	

Provisioning user/application combinations from the CLI

This CLI procedure shows how to create user/application combinations.

The user must have been defined in the User[ ] entity, and the applications must have been defined in the ApplicationIdentity[ ] entity.

1. Go to the Oamp subsystem by typing **:> Oamp[]**

2. Go to User Management by typing

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

3. Provision the UserApplicationMap[ ] entity by performing one of the following commands:

   • Display user accounts by typing:

```
Oamp[]> NotificationManager[]> display UserApplicationMap[]
```

   • Add new users by typing:

```
Oamp[]> NotificationManager[]> add
UserApplicationMap[UserName=user2;ApplName=BlueCli]
```

   The following message displays:

```
Added: 1
```

   • Delete notification properties for an application by typing:

```
Oamp[]> NotificationManager[]> delete UserApplicationMap[UserNames=user2;
ApplName=WebCI]
```

   The following message displays:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

   Type **y** to continue or **n** to cancel.

   • Modify the logging option of user accounts by typing:

```
Oamp[]>NotificationManager[]>UserApplicationMap[UserName=user2;ApplName=BlueCli]>
 modify . LogOption=1
```

   The following message displays:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

   Type **y** to continue or **n** to cancel.

   If you typed **y**, the system returns

```
Modified: 1
```

Provisioning Users

By default, the system pre-defines these users in the User table: user, operation, surveil, admin, batch and simprov. Each of these pre-defined users are associated with an application in the UserApplicationMap table.

Table 17: UserApplicationMap table

User	Applications associated to each user at installation (pre-defined)
User	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Operation	BlueCli, WebCI, LdapDataServer
Surveil (surveillance)	BlueCli, WebCI, LdapDataServer
Admin	BlueCli, WebCI, SOAP, CmdFileLoader, SNMP, LdapDataServer
Batch	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Simprov	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer

The administrator can display, add, or delete user-application combinations and modify their logging options. For an external application to be able to subscribe to notifications for specific applications, entities, or attributes, it must have a user account defined by the SDM system administrator with a username, password (in the User[ ] entity) and application name (user-application association defined in the UserApplicationMap[ ] entity). For the defined user accounts (in User[ ] entity), the SDM system administrator must associate them with applications by provisioning the UserApplicationMap[ ] entity.

Note: The application must already be defined in the ApplicationIdentity[ ] entity (see previous sub-sections).

These procedures define users and associate applications to them by provisioning the UserApplicationMap table. Users can create and display the User table, modify user passwords, and assign a group to each user.

For details on the User table, refer to the "Notification Security Management through CLI" section of the *SDM System Configuration - Reference Manual*.

WebCI	CLI
Creating user	Provisioning users
Modifying user	
Deleting user	

Provisioning user/application combinations from the CLI

This CLI procedure shows how to create user/application combinations.

The user must have been defined in the User[ ] entity, and the applications must have been defined in the ApplicationIdentity[ ] entity.

1. Go to the Oamp subsystem by typing **:> Oamp[]**

2. Go to User Management by typing

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

3. Provision the UserApplicationMap[ ] entity by performing one of the following commands:

   • Display user accounts by typing:

```
Oamp[]> NotificationManager[]> display UserApplicationMap[]
```

   • Add new users by typing:

```
Oamp[]> NotificationManager[]> add
UserApplicationMap[UserName=user2;ApplName=BlueCli]
```

   The following message displays:

```
Added: 1
```

   • Delete notification properties for an application by typing:

```
Oamp[]> NotificationManager[]> delete UserApplicationMap[UserNames=user2;
ApplName=WebCI]
```

   The following message displays:

```
Warning, you are about to delete this instance(s) permanently, Proceed with
delete? (y/[n]):
```

   Type **y** to continue or **n** to cancel.

   • Modify the logging option of user accounts by typing:

```
Oamp[]>NotificationManager[]>UserApplicationMap[UserName=user2;ApplName=BlueCli]>
 modify . LogOption=1
```

   The following message displays:

```
Warning, you are about to modify this instance(s) permanently, Proceed with
modify? (y/[n]):
```

   Type **y** to continue or **n** to cancel.

   If you typed **y**, the system returns

```
Modified: 1
```

Notification Management Using WebCI

This section outlines the WebCI procedures to provision the users, their applications and notification subscriptions/properties. To perform the tasks in the following table, refer to the procedures for the step by step instructions.

Task
View all User Management information
Provision applications
Provision notification subscription permissions
Provision notification properties
Provision users

Requirements: All WebCI provisioning procedures require the operator to log into a WebCI session with a valid username and password.

View all notification management information from the WebCI

This procedure displays the Notification Management information.

From the main menu, navigate to **Oamp** > **Notification Manager**.

The Notification Manager window opens.

Define/Provision Applications from the WebCI

The following WebCI procedure shows how the system's administrator can provision applications in the ApplicationIdentity table.

1. From the main menu, navigate to **Oamp** > **NotificationManager**. This will display the Notification Manager window.

2. Click the **Add ApplicationIdentity** button below the ApplicationIdentity table.

3. When the ApplicationIdentity Provisioning window appears (see figure below), enter the information (ApplName) to be added.

Figure 13: ApplicationIdentity Provisioning Window to Create Applications

4. Click **Commit** when all the information has been entered.

5. When the confirmation message "Entity entry was successfully committed" appears, click **OK**.

   --- end ---

Provisioning notification subscription permissions from the WebCI

Notification subscription permissions define per application the entities and attributes to which the user (external application) can subscribe notifications. The administrator defines these permissions in the NotificationSubscribe[ ] entity. This procedure describes how to provision the NotifSubscribe[ ] entity using the add or delete operation.

1. From the main menu, navigate to **Oamp** > **NotificationManager**.
   The Notification Manager window displays.

2. Click the **Display/Modify NotifSubscribe** button of an application in the ApplicationIdentity table.
   The NotifSubscribe window with the NotifSubscribe entity opens.

3. Perform one of the following operations:
   - Click **Add NotifSubscribe** to add notification subscription permissions (Namespace, Entity, Attribute) to the existing application.
   - Click **Delete** to delete an entry one at a time.

4. Click **Commit** in the pop-up window when all the information has been entered.

The system returns a confirmation message similar to `Entity entry was successfully committed.`

5. Click **OK**.

Provisioning notification properties from the WebCI

Notification properties define per application whether the previous value (before update) must be included in the notifications in addition to the current value (after update). The administrator defines these properties in the ApplicationProperty[ ] entity. This procedure describes how to provision the ApplProperty[ ] entity using the add, modify, or delete operation.

1. From the main menu, navigate to **Oamp** > **NotificationManager**.
   The Notification Manager window displays.

2. Click the **Display/Modify ApplProperty** button of an application in the ApplicationIdentity table.
   The ApplProperty window with the ApplProperty entity opens.

ApplProperty

Attribute	Value
Namespace	bn
Entity	MSISDN
ApplName	BlueCli
isValueBefore	Off

[Modify] [Delete] [Add ApplProperty]

3. Perform one of the following operations:

   • Click **Add ApplProperty** to add new properties to the existing application in the ApplProperty Provisioning pop-up window.

ApplProperty Provisioning

Namespace * [   ]
Entity * [   ]
ApplName * [WebCI   ]
isValueBefore [Unset ▼]
[Commit] [Close]

   • Click **Modify** to modify properties.
   • Click **Delete** to delete an entry one by one.

4. Click **Commit** in the pop-up window when all the information has been entered.
   The system returns a confirmation message similar to `Entity entry was successfully committed.`

5. Click **OK**.

Provisioning Users

By default, the system pre-defines these users in the User table: user, operation, surveil, admin, batch and simprov. Each of these pre-defined users are associated with an application in the UserApplicationMap table.

Table 18: UserApplicationMap table

User	Applications associated to each user at installation (pre-defined)
User	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Operation	BlueCli, WebCI, LdapDataServer
Surveil (surveillance)	BlueCli, WebCI, LdapDataServer
Admin	BlueCli, WebCI, SOAP, CmdFileLoader, SNMP, LdapDataServer
Batch	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Simprov	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer

The administrator can display, add, or delete user-application combinations and modify their logging options. For an external application to be able to subscribe to notifications for specific applications, entities, or attributes, it must have a user account defined by the SDM system administrator with a username, password (in the User[ ] entity) and application name (user-application association defined in the UserApplicationMap[ ] entity). For the defined user accounts (in User[ ] entity), the SDM system administrator must associate them with applications by provisioning the UserApplicationMap[ ] entity.

Note: The application must already be defined in the ApplicationIdentity[ ] entity (see previous sub-sections).

These procedures define users and associate applications to them by provisioning the UserApplicationMap table. Users can create and display the User table, modify user passwords, and assign a group to each user.

For details on the User table, refer to the "Notification Security Management through CLI" section of the *SDM System Configuration - Reference Manual*.

WebCI	CLI
Creating user	Provisioning users
Modifying user	
Deleting user	

Provisioning user/application combinations from the WebCI
This procedure creates user/application combinations in the UserAppMap entity.

The user must have been defined in the User[ ] entity, and the applications must have been defined in the ApplicationIdentity[ ] entity.

1. From the main menu, navigate to **Oamp** > **NotificationManager**.
    The Notification Manager window displays with the UserAppMap table.

2. Perform one of the following operations:

   • Click **Add UserAppMap** to add a new user/application combination.

     The UserAppMap Provisioning pop-up window opens.

   • Click Modify to change the Log Option.
   • Click **Delete** to delete the UserAppMap entry.

3. Click **Commit** in the pop-up window when all information has been entered.
   The system returns a confirmation message similar to `Entity entry was successfully committed`.

4. Click **OK**.

Provisioning Users

By default, the system pre-defines these users in the User table: user, operation, surveil, admin, batch and simprov. Each of these pre-defined users are associated with an application in the UserApplicationMap table.

Table 19: UserApplicationMap table

User	Applications associated to each user at installation (pre-defined)

User	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Operation	BlueCli, WebCI, LdapDataServer
Surveil (surveillance)	BlueCli, WebCI, LdapDataServer
Admin	BlueCli, WebCI, SOAP, CmdFileLoader, SNMP, LdapDataServer
Batch	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer
Simprov	BlueCli, WebCI, SOAP, CmdFileLoader, LdapDataServer

The administrator can display, add, or delete user-application combinations and modify their logging options. For an external application to be able to subscribe to notifications for specific applications, entities, or attributes, it must have a user account defined by the SDM system administrator with a username, password (in the User[ ] entity) and application name (user-application association defined in the UserApplicationMap[ ] entity). For the defined user accounts (in User[ ] entity), the SDM system administrator must associate them with applications by provisioning the UserApplicationMap[ ] entity.

Note: The application must already be defined in the ApplicationIdentity[ ] entity (see previous sub-sections).

These procedures define users and associate applications to them by provisioning the UserApplicationMap table. Users can create and display the User table, modify user passwords, and assign a group to each user.

For details on the User table, refer to the "Notification Security Management through CLI" section of the *SDM System Configuration - Reference Manual*.

WebCI	CLI
Creating user	Provisioning users
Modifying user	
Deleting user	

Provisioning user/application combinations from the WebCI
This procedure creates user/application combinations in the UserAppMap entity.

The user must have been defined in the User[ ] entity, and the applications must have been defined in the ApplicationIdentity[ ] entity.

1. From the main menu, navigate to **Oamp** > **NotificationManager**.
    The Notification Manager window displays with the UserAppMap table.

2. Perform one of the following operations:

   • Click **Add UserAppMap** to add a new user/application combination.

   The UserAppMap Provisioning pop-up window opens.

   • Click Modify to change the Log Option.
   • Click **Delete** to delete the UserAppMap entry.

3. Click **Commit** in the pop-up window when all information has been entered.
   The system returns a confirmation message similar to `Entity entry was successfully committed`.

4. Click **OK**.

Chapter

4

Viewing and editing subscriber profiles using WebCI

Topics:

This chapter contains information used to manage profiles within the Subscriber Data Management system

Viewing/editing SIM cards, MSISDNs, IMSIs, and HLR subscriber profiles

View all data or modify editable data related to a SubscriptionId with an HLR subscriber profile for troubleshooting purposes.

The current release supports one single HLR Subscriber Profile with one single Service Profile for each SubscriptionID. Once a SubscriptionID along with its Sim card(s), IMSI(s) (SimImsiMap), MSISDN(s) (MsIsdnImsiProfileAssociation) and HLR subscriber profile (including its Service Profile) have been provisioned through XML scripts, this data can be edited:

- MSISDNs
- Sim cards
- SimImsiMap
- MsIsdnImsiProfileAssociation
- Service Profile

1. *Access Subscriber Provisioning submenu*

2. From the submenu, go to **HLR** > **Display/Modify**.

   The Subscriber Provisioning window contains all related HLR subscriber information for the SubscriptionID.

MsIsdnImsiProfileAssociation

Imsi	MsIsdn	HlrServiceProfileID	Displayed	Deferred	Priority	Reachable	Action
310910421000101	15634210101	HlrId-00000002	On	Off	0	Off	Modify Delete
310910421000101	15634210200	HlrId-00000002	Off	Off	0	Off	Modify Delete

Add MsIsdnImsiProfileAssociation

ModifyDisplayedMSISDN   MakeMSISDNReachable   MakeMSISDNNotReachable

Service Profile

ServiceProfileId	Action
HlrId-00000002	Modify Delete

ServiceProfileID: [   ] Add

MsIsdn

MsIsdn	BearerCapName	DefaultBsg	BsgOverrride	Published	PortingStatus	Shared	ForceToSip	Action
15634210101		None	Off	On	NotPortedOut	On	Off	Modify Delete
15634210200		None	Off	On	NotPortedOut	Off	Off	Modify Delete

Add MSISDN

Sim

SimId	AlgoId	ManufacturerId	AlgorithmName	SimType	Ki32HexChar	PUK	Op32HexChar	Action
2344456666001	0		XOR	SIM	Provisioned	2345522333	NotProvisioned	Modify Delete

Add Sim

SimImsiMap

Attribute	Value
Imsi	310910421000101
PrimaryImsi	On
SimId	2344456666001

Modify Delete   Add SimImsiMap

Figure 14: HLR subscriber provisioning window

3. To edit data, click the desired button in the row of the identity to be edited.
   A pop-up window opens. It shows the editable data as an active field.

4. To view all SIM information specific to the subscription ID, click the SimID hyperlink to open the SIM Provisioning window.

Figure 15: Sim information for specific SubscriptionID

5. To view all MSISDN information specific to the subscription ID, click the MsIsdnId hyperlink to open the MSISDN Provisioning window.

Figure 16: MSISDN information for specific SubscriptionID

6. To view all Service Profile information specific to the subscription ID, click the ServiceProfileID hyperlink to open the Service Profile Provisioning window.

Figure 17: Service Profile information for specific SubscriptionID

Displaying the MSISDN/SIM/IMSI Provisioned in the Tekelec ngHLR

The WebCI allows the Network Operator to display the MSISDN/SIM/IMSI provisioned in the Tekelec ngHLR.

To display a MSISDN/SIM/IMSI provisioned in the Tekelec ngHLR, enter a MSISDN/SIM/IMSI number in its corresponding field in the Subscriber Provisioning window and click **Search**.

Figure 18: MSISDN Provisioned In The NgHLR

You can modify and/or delete a MsIsdn/SimId/Imsi entry. You can also provision (display, add, modify, delete) the data provisioned in the MsIsdnImsiProfileAssociation/SimImsiMap/ServiceProfile tables. To achieve this, click on the desired button.

Modifying Displayed MSISDN

Change the Display flag from one MSISDN to another MSISDN using the same IMSI.

Prerequisites:

- For more details on the 'Displayed' flag, refer to the "MSISDN-IMSI Profile Association" section of the *SDM Subscriber Provisioning-Reference Manual*. To achieve this, follow these steps:

1. *Access Subscriber Provisioning submenu*
2. Go to **HLR** > **display/modify**
   The Subscriber Provisioning window displays the HLR subscriber information for the specific SubscriptionID.
3. Click the **ModifyDisplayedMSISDN** button to enter the new Displayed MSISDN and other mandatory information identified by an asterisk (*).

   Note: Only one MSISDN entry can be 'Displayed' and hence have the Displayed flag set to '1'.
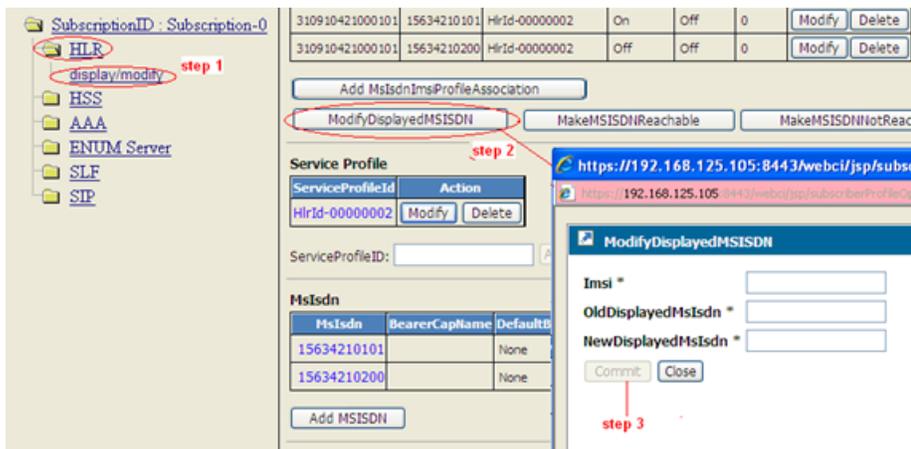
Figure 19: Modifying Display flag of an MSISDN

4. Click **Commit** to execute the operation.

Make a MSISDN-IMSI Profile Association Reachable/Not Reachable

This procedure configures the MSISDN/IMSI Profile Association to enable or disable an MSISDN from receiving calls.

Prerequisites: *Access Subscriber Provisioning submenu*

All mobiles/SIMs that share an MSISDN are able to make outgoing calls but only one mobile/SIM that uses a shared MSISDN shall receive incoming calls. Therefore, each MSISDN-IMSI profile association must be defined as "reachable" or "not reachable" so that the Tekelec ngHLR can choose the correct MSISDN-IMSI profile association to reach the SIM. These rules apply:

- All MSISDN-IMSI profile associations defined for one single SIM with the same MSISDN must all have the 'Reachable' flag set to the same value.
- Only one SIM can be reachable among the ones that have MSISDN-IMSI associations that use the same shared MSISDN.

  - A SIM is reachable if the MSISDN 'Published' flag and the MSISDN-IMSI association's 'Reachable' flag are both set to '1' (default). For an MSISDN, if one of its MSISDN-IMSI associations is not set to 1, all MSISDN-based messages will fail for this MSISDN.
  - To change the reachable flag of many IMSI-MSISDN associations of the same SIM, use the MakeMsisdnNotReachable() or MakeMsisdnReachable() operations.
  - The MakeMsisdnNotReachable() operation changes the 'Reachable' flag to '0' (not reachable) for all MSISDN-IMSI associations of the MsIsdn provided.
  - The MakeMsisdnReachable() operation changes the 'Reachable' flag to '1' (reachable) for all the MSISDN-IMSI associations of the MsIsdn provided, and of the IMSIs that are part of the SimId provided or found by the Tekelec ngHLR (if IMSI is provided instead of SimId).
  - For more details on the 'Reachable' flag, refer to the "MSISDN-IMSI Profile Association" section of the *SDM Subscriber Provisioning-Reference Manual*.

- When an MSISDN is defined as 'Shared', other mobile/SIMs within the same subscription (SubscriptionID) or belonging to different subscriptions (different SubscriptionIDs) can use that same MSISDN.

1. Go to **HLR > display/modify**
   The Subscriber Provisioning window displays the HLR subscriber information for the specific SubscriptionID.

2. Perform one of these operations:

   • Click the **MakeMsisdnNotReachable** button to enter the MSISDN that shall not receive calls.
   • Click the **MakeMsisdnReachable** button to enter the MSISDN and the SimId to enable the MSISDN to receive calls.
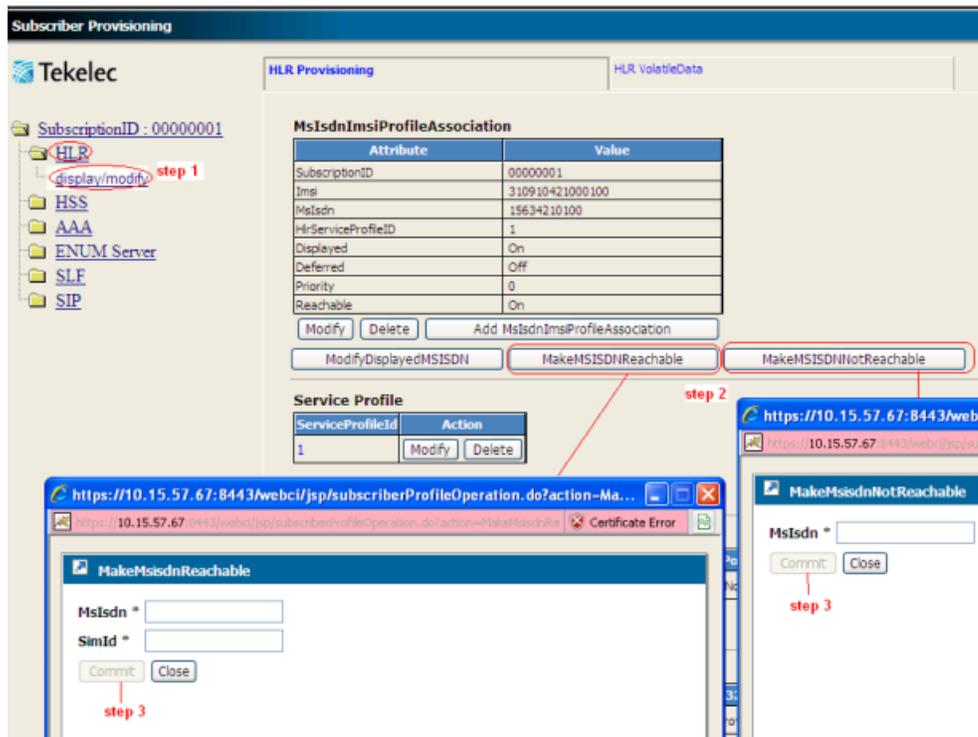
Figure 20: Making an MSISDN 'Reachable' or 'Not Reachable'

3. Click **Commit** to execute the operation.

Assigning/unassigning a SubscriptionID to a provisioned SIM card

The SDM interfaces allow the Network Operator to provision through XML scripts SIM cards with a SubscriptionID assigned to each of them or unused SIM cards without any SubscriptionID assigned to them. Refer to the *SDM Subscriber Provisioning Reference Manual and User Guide* for further information on SIM card provisioning.

The WebCI offers a way to assign a provisioned unused SIM card data to a SubscriptionID and a way to unassign a SIM card (SimId) from a SubscriptionID.

1. From the main menu, navigate to **Subscription Management** > **Subscriber Provisioning**.

2. Click **Subscriber Provisioning**.
   The Subscriber Provisioning window displays.

3. Click **Assign** or **Unassign** and enter all the mandatory fields.

For details on each parameter and their value and meaning, refer to the AssignSIM() and UnassignSIM() operations described in the "HLR Operations" section of the *SDM Subscriber Provisioning – Reference Manual*.

4. Click **Commit**.
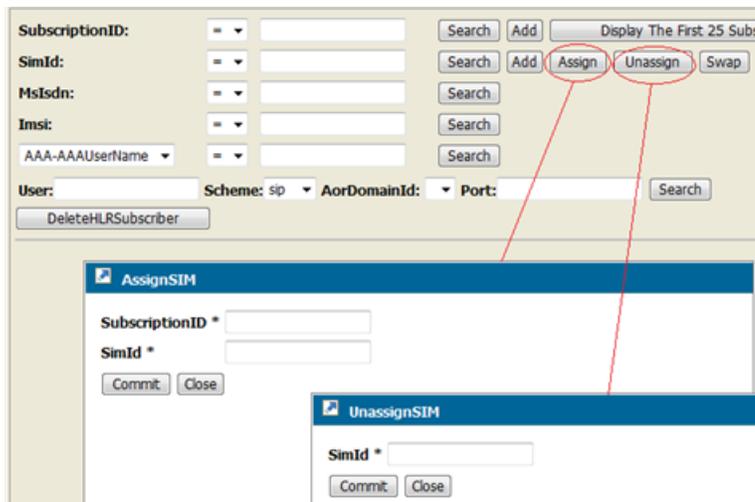
Figure 21: Assigning/unassigning a SIM card

Swapping SIM cards

The WebCI offers the ability for the Network Operator to easily swap SIM cards for a subscriber.

The Network Operator can change a provisioned SIM card already assigned to a SubscriptionID with an unused SIM card that has been already provisioned in the Tekelec ngHLR but that is unassigned to any SubscriptionID.

1. From the main menu, navigate to **Subscription Management** > **Subscriber Provisioning**.
2. Click **Swap SIM** and enter all the mandatory information identified by an asterisk (*).

For details on each parameter and their value and meaning, refer to the SwapSIM() operation described in the "HLR Operations" section of the *SDM Subscriber Provisioning – Reference Manual.*

3. Click **Commit** to execute the operation.
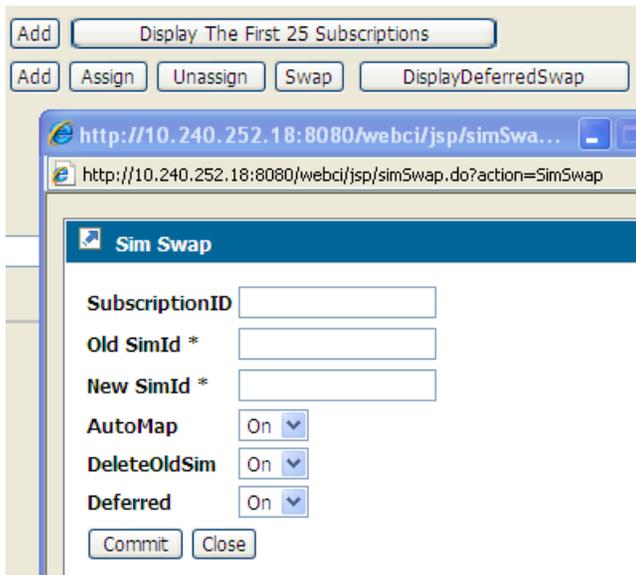
Figure 22: SIM swap operation

Deleting HLR subscriber

Clean up the entries provisioned in all HLR entities specifically for a subscriber (SubscriptionID).

1. From the WebCI main menu, go to **Subscription Management** > **Subscriber Provisioning**

2. Click the **DeleteHLRSubscriber** button to perform the desired operation and enter all the mandatory information identified by a '*'.
   The Subscriber Provisioning pop-up window opens.

3. Enter the information in the available fields

   For details on each parameter and their value and meaning, refer to the "HLR Operations" section of the *SDM Subscriber Provisioning – Reference Manual.*

4. Click on **Commit** to execute the operation.
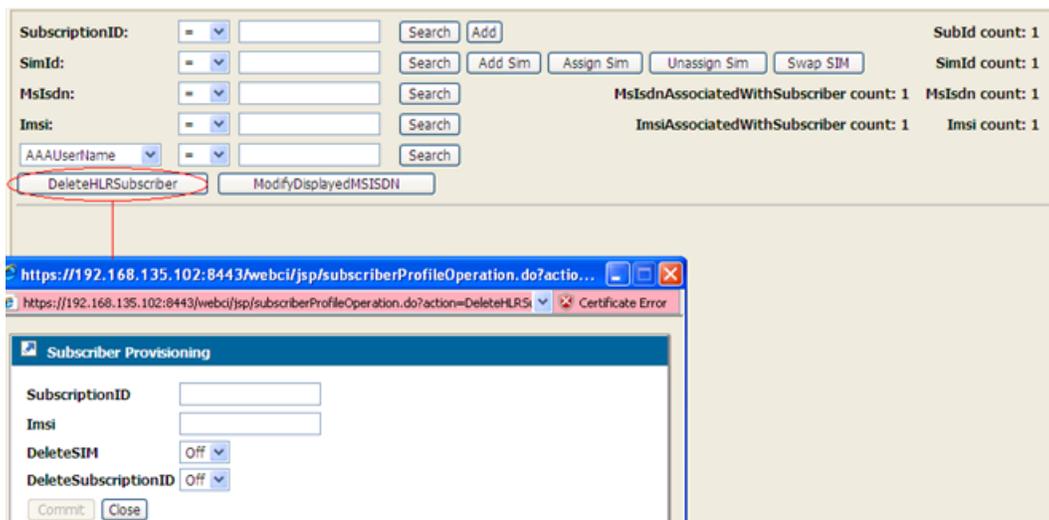
Figure 23: Delete HLR Subscriber

Viewing/Editing HLR Service Profile

The Service Provisioning screen provides access to provisioning windows to configure additional basic services and supplementary services.

The Service Provisioning screen provides access to provisioning windows that allow the network operator to provision HLR services profiles with the following:

- Templates/rules that must be followed for this subscriber concerning functionalities, such as:
  - XML Notifications (SubsRoamingMsgOn and SubsVlrMsgNotificationOn)
  - MT-SMS Routing (SmsTemplateName)
  - Forward-To-Number (FTNRule)
  - Access Restriction Data
  - Operator Controlled Roaming Controls (OCPlmnTemplateName)
  - ATI Subscriber Information Level
  - Enable/Disable Subscriber state
- Additional basic services and supplementary services

Provisioning a subscriber HLR service profile

Use this procedure to provision an HLR Service Profile for a subscriber.

The operator must have already provisioned the *Viewing/editing SIM cards, MSISDNs, IMSIs, and HLR subscriber profiles* and must have created a ServiceProfileID.

Use this procedure to

- edit subscriber-specific settings, templates, and rules for ngHLR functionalities; for example,

- XML Notifications (SubsRoamingMsgOn and SubsVlrMsgNotificationOn)
- MT-SMS Routing (SmsTemplateName)
- Forward-To-Number (FTNRule)
- Access Restriction Data
- Operator Controlled Roaming Controls (OCPlmnTemplateName)
- ATI Subscriber Information Level
- Enable/Disable Subscriber state

- provision the services outlined in *Table 20: Subscriber services provisioned with WebCI*.

For details on these options, refer to the HLR entities in the *SDM Subscriber Provisioning - Reference Manual*.

Table 20: Subscriber services provisioned with WebCI

Service	Provisionable items	Description
Call Forward	Type	Call Forward Unconditional (CFU), Call Forwarding on Mobile Subscriber Busy (CFB), Call Forwarding on No Reply (CFNRY), and Call Forwarding on Mobile Subscriber Not Reachable (CFNRC).
	Basic Service Group	Speech, Fax, All Data Asynchronous, All Data Synchronous, Voice Group, Provision, Forward To Number, Default Forward To Number, No Reply Condition Timer.
Call Barring	Supplementary Services	Outgoing Calls (BAOC), Outgoing International Calls (BOIC), Outgoing International Calls Except to the Home PLMN (BOICEXHC), Incoming Calls (BAIC), and Incoming Calls when Roaming outside home PLMN country (BICROAM).
	Basic Service Group	Speech, Short Message Service, Fax, All Data Asynchronous, All Data Synchronous, Voice Group, Provision
	Subscription options	Password change option, password, Number of wrong attempts.
Closed User Group	Basic Service	CUG Teleservice, CUG Bearer Services.
	Subscription	Group Id, Index, Options, BsgList.
	Features	BsgId (Speech, Fax, All Data Asynchronous, All Data Synchronous, Voice Group), Inter CUG Restriction, Preferential Index.
Number Id	Supplementary Services	Calling Line Identification Presentation (CLIP), CLIP Override, Calling Line Identification Restriction (CLIR).Connected Line Identification Presentation (COLP), COLP Override, Connected Line Identification Restriction (COLR), CLIR presentation mode
Charge Service	Supplementary Services	AOCC, AOCI

Call Completion	Supplementary Services	Call Wait, Call Hold, MultiParty, Call Wait Activation (BsgID).
Camel	Subscriber Info	Provision states (OCsi, TCsi, VTCsi, SsCsi, DCsi, UCsi, MCsi, OSMSCsi, GPRSCsi), Csi Types, Camel Phases and Trigger Detection Points for each Camel CSI Type.
LCS	Subscriber Info	LCSPrivacyExceptionList, SRILCSAllowed

1. *Access Subscriber Provisioning submenu*.
2. Go to **HLR** > **display/modify**.
   The HLR provisioning window displays.
3. Locate the Service Profile table and click the **Modify** button of the Service Profile to be edited.

The Subscriber Provisioning window displays with its main page and the Edit Subscriber Profile menu.
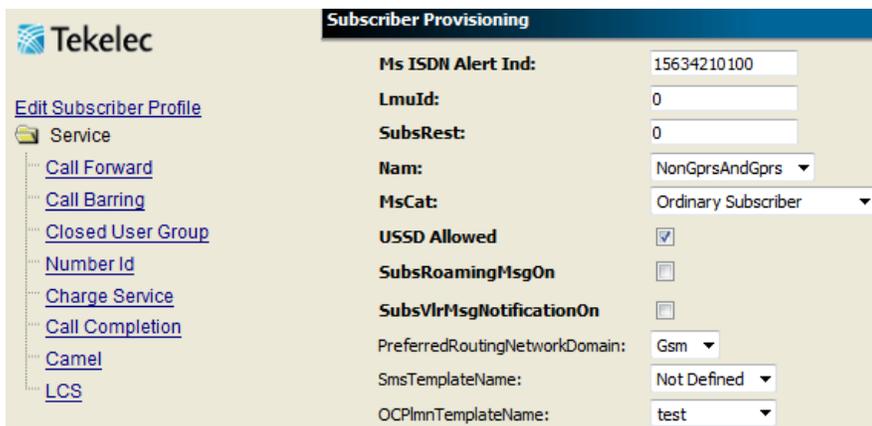
4. From the Subscriber Provision main page, provision subscriber-specific settings, templates, and rules for ngHLR functionalities.
5. From the Edit Subscriber Profile menu, click the hyperlink of the service to be modified.

   Clicking a checkbox to enable a feature may provide additional parameters to provision. Changes take effect by clicking the **Commit** button.

   Perform one or more of these steps:

- In the *Call Forward Provisioning* window, click a checkbox to enable or disable Call Forwarding features.

  By default, none of the services are selected and basic service group parameters are unprovisioned. Once a service is selected, the provisioning options become selectable.

Call Forwarding Unconditional (CFU)
- ☑ Provision State
- ☑ NotifyToCgParty
- ☑ PresentMsIsdn
- ☑ NotifyToForwardingParty
- ☐ CFDefaultEnabled
- CFDefaultFtn [   ]

Bsg ID	Bsg State	Forward To Number	Ftn Override	Default Ftn	FtnSubAddr
Speech	Provision ▾		☐	15634213333	
FacsimileServices	Provision ▾		☐	15634213333	
AllDataCircuitAsynchronous	Unprovision ▾		☐		
AllDataCircuitSynchronous	Unprovision ▾		☐		
VoiceGroupServices	Unprovision ▾		☐		

Call Forwarding on Mobile Subscriber Busy (CFB)
- ☑ Provision State
- ☑ NotifyToCgParty
- ☑ PresentMsIsdn
- ☑ NotifyToForwardingParty
- ☐ CFDefaultEnabled
- CFDefaultFtn [   ]

Bsg ID	Bsg State	Forward To Number	Ftn Override	Default Ftn	FtnSubAddr
Speech	Provision ▾		☐	15634213333	
FacsimileServices	Provision ▾		☐	15634213333	
AllDataCircuitAsynchronous	Unprovision ▾		☐		
AllDataCircuitSynchronous	Unprovision ▾		☐		
VoiceGroupServices	Unprovision ▾		☐		

Call Forwarding on No Reply (CFNRY)
- ☑ Provision State
- ☑ NotifyToCgParty
- ☑ PresentMsIsdn
- ☑ NotifyToForwardingParty
- ☐ CFDefaultEnabled
- CFDefaultFtn [   ]

Bsg ID	Bsg State	Forward To Number	Ftn Override	Default Ftn	NoReplyCondTimer	FtnSubAddr
Speech	Provision ▾		☐	15634213333	15	
FacsimileServices	Provision ▾		☐	15634213333	15	
AllDataCircuitAsynchronous	Unprovision ▾		☐			
AllDataCircuitSynchronous	Unprovision ▾		☐			
VoiceGroupServices	Unprovision ▾		☐			

- In the *Provisioning Call Barring* window, click a checkbox to enable or disable Call Barring features.

  By default, none of the services are selected and basic service group parameters are unprovisioned. Once a service is selected, the provisioning options become selectable.

- In the *Provisioning Closed User Group* window, click a checkbox to enable or disable Closed User Group features.

  By default, none of the services are selected and basic service group parameters are unprovisioned. Once a service is selected, the provisioning options become selectable.

  When the Enable Closed User Group Services box is selected, the services are displayed and become selectable.
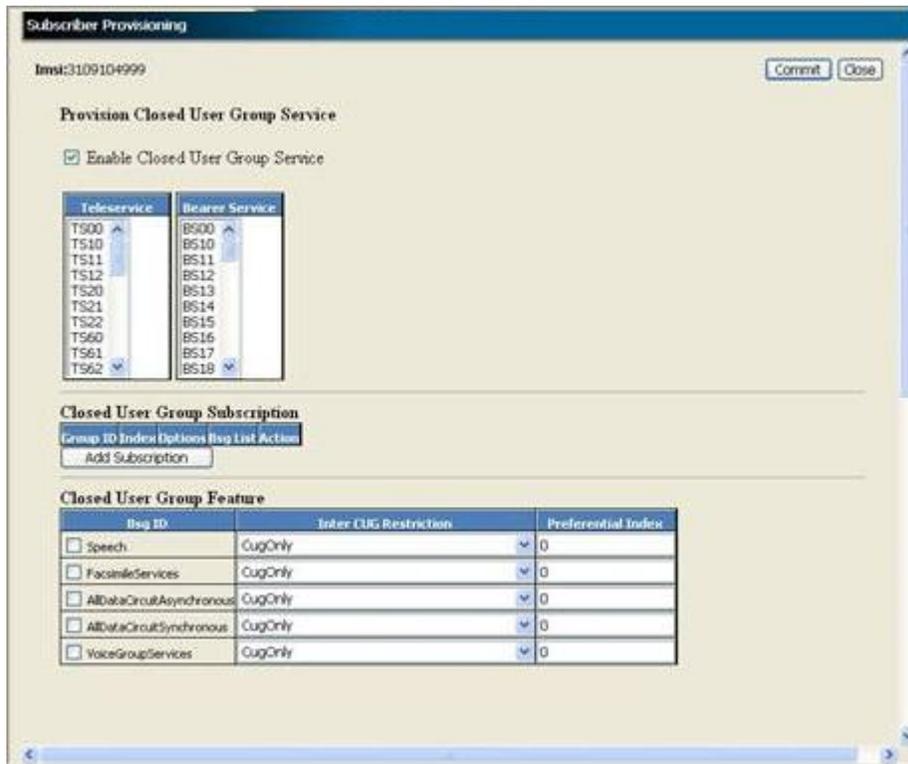
- In the *Provisioning Number Id Service* window, click a checkbox to enable or disable Number Id features.
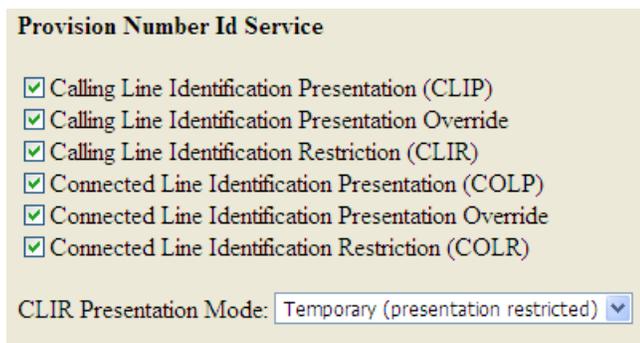
- In the *Provisioning Charge Service* window, click a checkbox to enable or disable the Charge Service features.
- In the *Provisioning Call Completion* window, click a checkbox to enable or disable Call Completion features.

- In the *Provisioning Camel* window, click a checkbox to provision Camel features.

Figure 24: Camel Provisioning Screen

- Click the **Add CamelData** button.

Figure 25: Camel Data Screen

- In the *Provisioning LCS* window

Note: The **Add GMLCList, Add MOLRList, Add ExternalClientList and Add ServiceTypeList** options are not implemented in this release and an error will be returned if those tables are provisioned.

Figure 26: LCS Provisioning Screen

- Click the **Add LCSPrivacyExceptionList** button.

Figure 27: LCSPrivacyExceptionList Screen

- (Required) Enter the **appropriate information** in screen fields.

  Note: If universalClass is selected as the SSCode, then the InternalClient must be set to NULL. If PLMN Operator Class is used, then an InternalClient option must be selected.

  Note: This parameter only applies to the PLMN operator privacy class and gives the identities of the internal PLMN operator clients allowed to locate a target MS for an N1-LR or MT-LR.

  Note: Up to five internal clients are supported.

- Click **Commit** button to save changes.
- Click **Close** button.

6. Click **Commit** in the Subscriber Provisioning window when all the services have been added. The system returns a confirmation message.

```
All changes were successfully committed
```

7. Click **OK**

Provision Camel services for a subscriber

Provision CAMEL services for a subscriber.

Important Notes:

- O-CSI is considered as provisioned only if the O-CSI is provisioned with the ProvisionState ON and there is one Detection Point (camel phase 1 and 2 must have the CollectedInfo DP) provision for O-CSI and the ProvisionState of the Detection point is ON.
- T-CSI is considered as provisioned only if the T-CSI is provisioned with the ProvisionState ON and there is one Detection Point provision for T-CSI and the ProvisionState of one of the Detection point is ON.

1. *Access Subscriber Provisioning submenu*.

2. Go to **HLR** > **display/modify**.
   The HLR provisioning window displays.

3. Locate the Service Profile table and click the **Modify** button next to the ServiceProfileID
   The Subscriber Provisioning window with the Edit Subscriber Profile menu opens.

4. Go to **Service** > **Camel**

5. Use the Camel table to provision CAMEL subscription data such as Provision State or Camel Subscription Information Notification Criterias. Perform one of these operations:

   - Click the **Add CamelData** button to add another entry.
   - Click the **Modify** button to change the Camel entry.
   - Click the **Delete** button to delete a Camel entry one at a time.

Figure 28: Camel and CamelCSIData provisioning

6. Provision the CSI types in the CamelCsiData table. Perform one of these operations:

- Click the **Add CamelCsiData** button to add another entry.

  Note: For each definition entered in this table, the related tables that provision Trigger Detection Points (Tdps) for that CSI type become visible and provisionable.

- Click the **Modify** button to change Camel CSI data for one entry at a time.
- Click the **Delete** button to delete a CamelCsiData entry one at a time.

  Note: This field is mandatory.

  Note: Deleting an entry in the CamelCsiData table will automatically delete the TDPs that were provisioned for that entry (CSI Type and Camel Phase).

  Note:

- For O-CSI and T-CSI only, multiple different Camel Phases can be provisioned by provisioning multiple entries with the same CsiType (O-CSI or T-CSI) and a different CamelPhase.
- For each CSI type, the Active State, Camel Phase, Notification flag, and the ActionOnUnsCamelPh (only for O-CSI) can be defined.
- For each definition entered in this table, the related tables that allow the provisioning of Trigger Detection Points (TDPs) for that CSI type become visible and provisionable.

7. Provision the Trigger Detection Points (TDPs) in the O-CSI or T-CSI tables using the **Add**, **Modify**, or **Delete** button.

   Note:

- The Gsm Scf Addresses must have already been defined (GsmScfId must exist) before a service code can be linked to it, refer to the "Provisioning Camel" section of the *SDM System Configuration – User Guide* for instructions on how to define Gsm Scf Addresses.
- The HLR Camel Service Mask Template entity must be provisioned for the Enhanced Camel handling behavior to take place when the parameter ActionOnUnsCamelPh (in the CamelCsiData table) is set to 'Apply Mask' for Camel O-CSI.

   a) For the O-CSI tables, configure *Collected Info* and *Route Select Failure*
   b) For T-CSI tables, configure Terminating Attempt Authorized, Terminating Busy, or Terminating NoAnswer (as applicable).

Figure 29: Camel O-CSI and T-CSI table provisioning

Delete services for a subscriber

This procedure describes how to delete services from a subscriber profile.

1. Follow the instructions described in *Viewing/editing SIM cards, MSISDNs, IMSIs, and HLR subscriber profiles*.

2. Click the **Modify** button located in the same row as the subscriber's HlrServiceProfileID value.

   The Subscriber Provisioning window will open.

3. When the Subscriber Provisioning screen appears, select the link (Call Forward, Call Barring, Closed User Group, Number Id, Charge Service, Call Completion, and Camel) of the service to be deleted.

4. When the screen of the selected service appears, deselect or uncheck the service that is no longer needed.

   Note: To withdraw the Call Forward service for a subscriber, simply uncheck the Provision State box.

5. Click **Commit** for the changes to take effect.

6. When the confirmation window "

```
All changes were successfully committed
```

" appears, click **OK**.

Display the Services for a Subscriber

This procedure is used to display a subscriber's profile and its provisioned services.

1. Follow the instructions described in *Viewing/editing SIM cards, MSISDNs, IMSIs, and HLR subscriber profiles*

2. Click on the HlrServiceProfileID's value.

   The Subscriber Provisioning window will open.

3. Select a service tab (along the top of the window) to view details of other services (Subscriber Profile, Call Forward, Call Barring, CUG Service, Camel Service, and Other Service) assigned to this subscriber.

Viewing/Editing MNP-SRF Subscribers

This procedure provisions MNP-SRF subscribers.

The MNP-SRF is one of the Tekelec ngHLR's multiple functionalities. The Tekelec ngHLR supports Mobile Number Portability (MNP), which allows mobile subscribers to change their subscription from one service provider to another without changing their mobile phone number (MSISDN). For a detailed description of this feature, refer to the "Support of MNP-SRF" section in the *SDM Product Description*.

The MNP-SRF functionality can be enabled/disabled on the Tekelec ngHLR by the Tekelec Network Support Team and from the WebCI's HLR Configuration window, its activation status can be viewed with the MobileNumberPortabilityState parameter in the Hlr Config table. The Network Operator can activate/deactivate the MNP feature by clicking on the **Activate MNP/Deactivate MNP** buttons available from the HLR Configuration window's MNP tab. Refer to the "Activating/Deactivating the Mobile Network Portability (MNP)" section of the *SDM System Configuration – User Guide* for more details on the HLR Configuration window's MNP tab. Note that this can be done even if the SSR is not authorized yet. The activation/deactivation of the MNP can be done dynamically at any time during running time of the system and won't require the restart of the HLR.

This section describes how to provision MNP-SRF subscribers. Note that deactivating the MNP will not remove the data provisioned for the MNP subscribers.

The operator can provision the Number Portability database (NPDB) with MSISDNs, their portability status and the necessary portability information needed for the Tekelec ngHLR to be able to take one of the following actions:

- Continue normal HLR processing
- Relay query towards the recipient network
- Redirect interrogating node towards the recipient network

It is very important to note that the Tekelec NPDB is managed independently from the Tekelec ngHLR subscriber profiles and that the information contained in this database supersedes the one contained in the "regular" subscriber profile, if any.

1. From the WebCI main menu, go to **HLR** > **Mobile Number Portability**

   The Mobile Number Portability window opens.
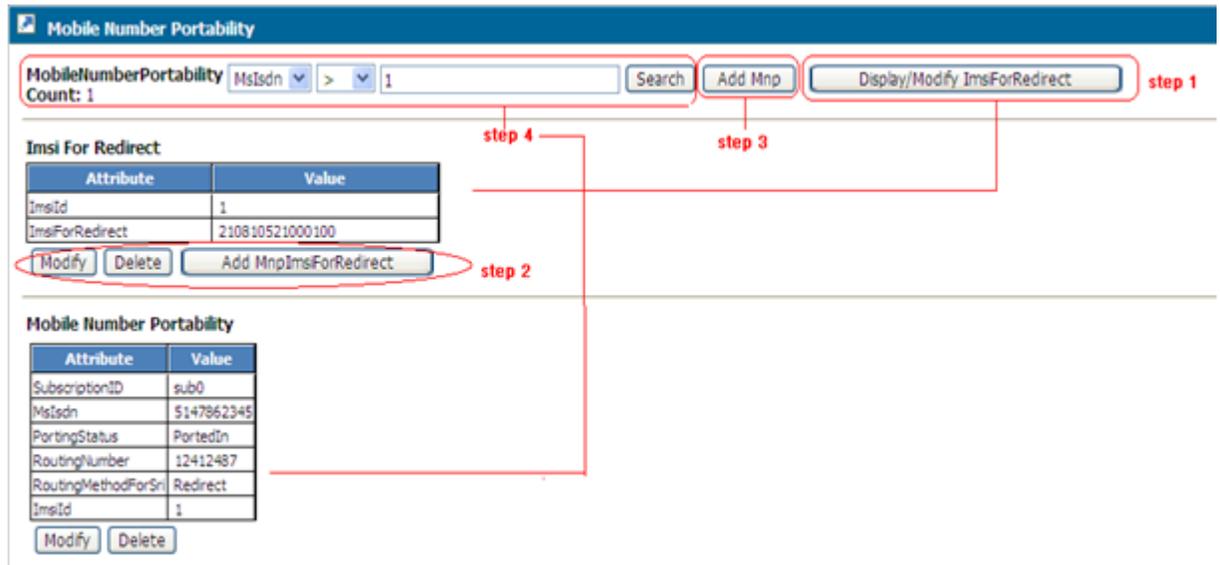
2. To define IMSIs that will be returned in the SRI_ack message when the Tekelec ngHLR will redirect the interrogating node to the recipient's network, perform these steps:

   a) Click the **Display/Modify ImsiForRedirect** button to display the ImsiForRedirect table.

   b) Then perform one of these operations:

   - To add an IMSI for Redirect, click the **Add MnpImsiForRedirect** button.
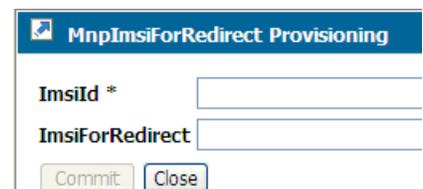
     The MnpImsiForRedirect Provisioning window opens.

     Type the IMSI for Redirect.

   - To modify the IMSI for Redirect, click the **Modify** button.

     All entries can be modified.

   - To delete the IMSI for Redirect, click the **Delete** button.

     Note: If one or several MNP entries refer to the ImsiForRedirect to be deleted, the MNP entries must first be deleted, or the ImsiId value of these MNP entries must be changed to another existent value provisioned in the ImsiForRedirect table.

     Delete one entry at a time.

3. To provision ported-out MSISDNs with the relay routing method, perform one of these operations:

- To add a new entry to the MNP table, click the **Add Mnp** button .

   The MNP Provisioning window opens.
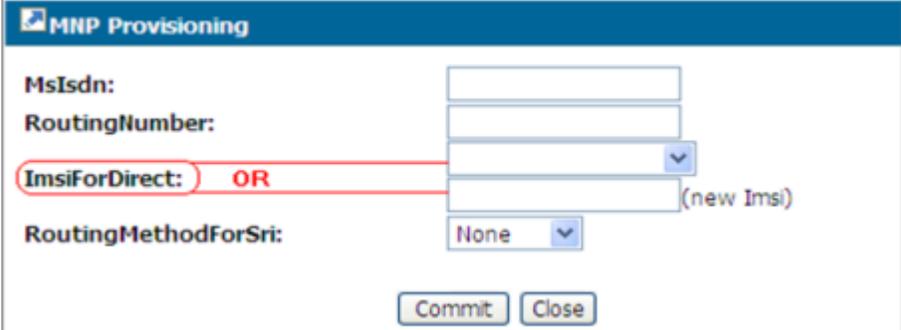
   The Mobile Number Portability table defines MSISDNs and their portability status, routing number, IMSI for redirection or routing method on SRI queries.

   Note: The IMSI for redirection must only be provisioned if the routing method is set to 'Redirect'. Moreover, this operation allows you to either select an IMSI for redirection among the ones that are already provisioned in the ImsiForRedirect table or either enter a new IMSI for redirection value.

   Select the routing method.

- Search for the MNP table by typing a specific ImsiId or a range of MSISDN entries into the Search field.

a) Then perform one of these operations:

- Click the **Modify** button to modify an entry in the Mobile Number Portability table.
- Click the **Delete** button to delete one entry one at a time in the Mobile Number Portability table.

Other Operations

In addition to provisioning the ImsiForRedirect and Mobile Number Portability tables with new entries, the following operations are also available:

- **Delete.** The following can be deleted:

One entry at a time in the Imsi For Redirect table.

Prerequisite: If one or several Mobile Number Portability entries refer to the ImsiForRedirect entry you wish to delete, the Mobile Number Portability entries must first be deleted or at least the ImsiId value of these Mobile Number Portability entries must be changed to another existent value provisioned in the Imsi For Redirect table.

One entry at a time in the Mnp table.

- **Modify.** Each entry in the Imsi For Redirect and Mobile Number Portability tables can be modified.

Viewing/Editing SIP Subscriber Profiles (Address Of Records)

This procedure describes how to display and provision SIP Address of Records (AoRs) for a subscriber (SubscriptionID), related Registration Bindings, as well as SIP permanent Redirection contact URIs.

Prerequisites: The Subscription (SubscriptionID) to be provisioned or troubleshooted must already exist in the database.

Once a SubscriptionIDs and SIP subscriber profiles have been provisioned through XML scripts, the Network Operator can use the WebCI to troubleshoot subscriber profiles by viewing SIP subscriber profiles and editing selected data in the AoR table.

1. *Access Subscriber Provisioning submenu*.
2. Go to **SIP** > **display/modify**.
   The Subscriber Provisioning window opens to display the AddressofRecord table.
3. Define an Address Of Record by provisioning the AddressOfRecord table, using these operations:

   - Click the **Add** button to add a new address of record.
   - Click the **Modify** button to modify the data provisioned for a specific AoR entry.

     Note: Modify/Update operation on SIP AddressOfRecord is only permitted to update one record at a time. Update of multiple records is not permitted.

   - Click the **Delete** button to delete a specific AoR entry. Delete operation on SIP AddressOfRecord is only permitted to delete one record at a time

     Note: When an AOR associated with a Sip subscriber profile is deleted, if there is an associated SipUa registration binding, the AOR is deregistered and deleted, and a GSM CancelLocation is performed for the associated Imsi. (This is in addition to deleting associated entries in the Registrar's RegistrationBinding, if the Registrar is enabled.)

     Deleting a SIP AOR record automatically deletes all associated contacts (entries in the Registrar's Registration bindings, if the Registrar is enabled) currently registered against this AOR. When an AOR associated with a Sip subscriber profile is deleted, if there is an associated SipUa registration binding, the AOR is deregistered and deleted, and a GSM CancelLocation is performed for the associated Imsi.

   - Click the **Registration Binding** button to display the Registration Binding for a specific AoR.
   - Click the **Ua Registration Binding** button to display the User Agent Registration Binding for a specific AoR.
   - Click the **Redirection Override** button to provision (display, add, delete) SIP Permanent Redirection contact URIs for a specific AoR.

Figure 30: SIP tab for SubscriptionID

Viewing/Editing HSS Subscriber Profiles

Once SubscriptionIDs and HSS subscriber profiles have been provisioned through XML scripts (refer to the *SDM Subscriber Provisioning Reference Manual and User Guide*), the Network Operator can view and edit, from the WebCI, some of the data provisioned for these HSS subscriber profiles. For subscriber data, the WebCI is mainly helpful for troubleshooting purposes.

For details on HSS Subscriber Provisioning parameters, refer to the "HSS" chapter of the *SDM Subscriber Provisioning - Reference Manual.*

This section describes how to troubleshoot a HSS Subscriber Profile, as follows:

- Display/Delete an entire HSS Subscriber Profile
- Add/Modify/Delete a Private Identity.
- Modify the ChargingID the HSS Subscriber Profile refers to.
- Display the Registration Status
- Add/Modify/Delete a Service Profile
- Add/Modify/Delete a Public Identity
- Link a Public Identity to a Private Identity
- Remove the link between a Public Identity and a Private Identity
- Display HSS Volatile Data
- Add/Modify/Delete HSS Initial Filtering Criterias
- Linking(Adding) DSAI to a HSS Initial Filtering Criteria
- Modify/Deleting DSAI
- Add/Modify/Delete HSS Service Point Trigger
- Link HSS Shared Initial Filtering Criteria
- Remove Link to HSS Shared Initial Filtering Criteria

To provision a HSS Subscriber profile from the WebCI, the operator must follow these steps:

Prerequisite: It is important to note that a Subscription (SubscriptionID) and its HSS Subscriber Profile must already be created before being able to troubleshoot it (display, edit, delete) from the WebCI. You can do this by running XML scripts that provision Subscriptions and HSS Subscriber Profiles. Refer to the *SDM Subscriber Provisioning – User Guide* for examples of XML scripts. Moreover, the HSS System Features must already be configured, refer to the "HSS System Features" section of the SDM System Configuration – User Guide.

1. *Access Subscriber Provisioning submenu*.

2. From the Subscriber Provisioning submenu, go to **HSS** > **Display/Modify**.

The Subscriber Provisioning window contains all related HSS subscriber information for the SubscriptionID.
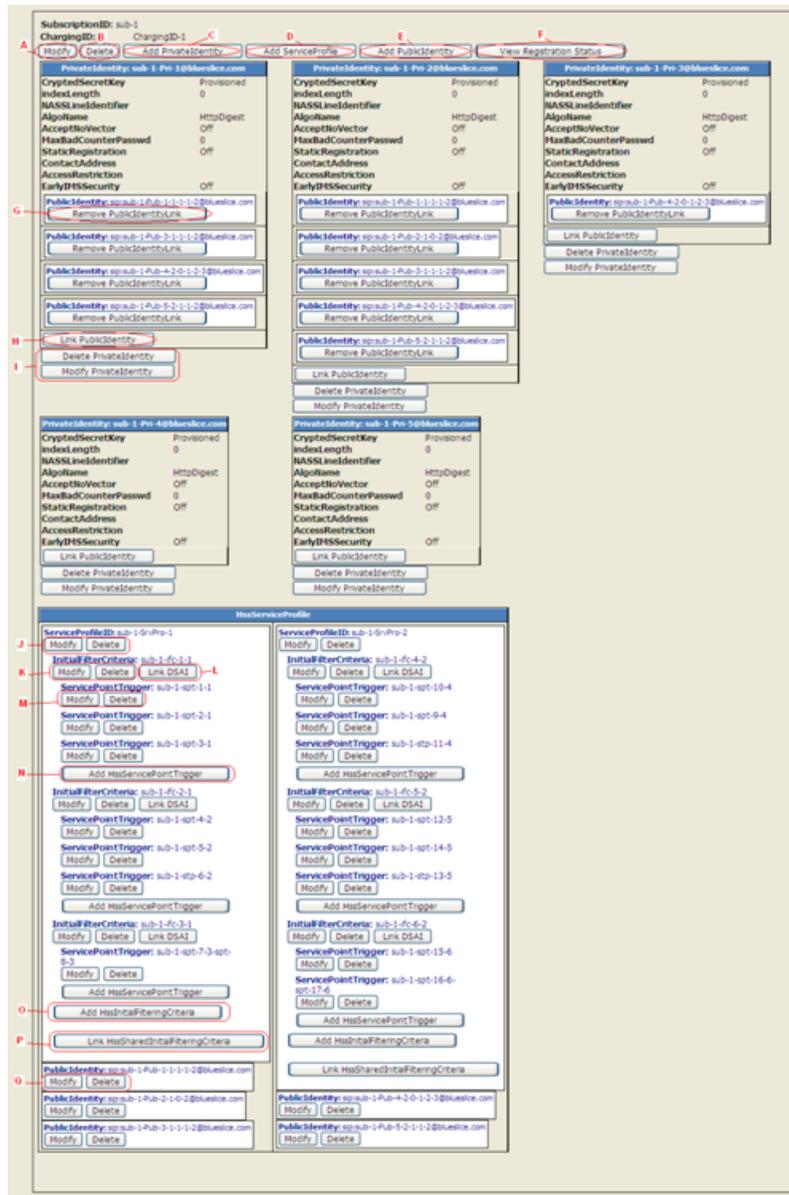
Figure 31: HSS subscriber provisioning window

3. Edit the HSS Subscriber Profile by clicking on the buttons available from this window.

The table presents the different provisioning operations that can be performed for the HSS subscriber profile and the buttons displayed in the WebCI that allow to execute these operations.

Table 21: Provisioning Operations

Location in WebCI window	WebCI button(s) available	Operation description
A	Modify	This button allows to modify the ChargingID the Subscription's HSS subscriber profile refers to.
B	Delete	This button allows to delete the entire HSS Subscriber Profile.
C	Add Private Identity	This button allows to add a Private Identity to the HSS subscriber profile. Multiple Private Identities can be provisioned for one single HSS Subscriber Profile. Simply repeat this operation as many times as the number of Private Identities you wish to have provisioned.
D	Add Service Profile	This button allows to add a Service Profile to the HSS subscriber profile. Multiple Private Identities can be provisioned for one single HSS Subscriber Profile. Simply repeat this operation as many times as the number of Service Profiles you wish to have provisioned.
E	Add Public Identity	This button allows to add a Public Identity to the HSS subscriber profile. Multiple Public Identities can be provisioned for one single HSS Subscriber Profile. Simply repeat this operation as many times as the number of Service Profiles you wish to have provisioned. Prerequisite: At least one Service Profile must be provisioned prior to being able to add a Public Identity.
F	View Registration Status	This button allows to display the Registration Status data for the HSS Subscriber profile.
G	Remove PublicIdentity Link	This button is available for each Private Identity and allows to remove the link between a Private Identity and a Public Identity. Prerequisite: This operation can only be executed for a Private Identity that has already been linked to a Public Identity.
H	Link Public Identity	This button is available for each Private Identity and allows to link a Public Identity to a Private Identity. Prerequisite: At least one Public Identity and Private Identity must be provisioned.
I	Delete Private Identity Modify Private Identity	These two buttons are independent and available for each Private Identity. They respectively allow to delete a Private Identity and modify a Private Identity. Prerequisite: You can only delete a Private Identity once its linked Public Identities have been deleted (refer to the Remove PublicIdentityLink button to achieve this).

Location in WebCI window	WebCI button(s) available	Operation description
		Note: Beware that deleting the last Private Identity of a HSS Subscriber Profile results in the deletion of the entire HSS Subscriber Profile itself.
J	**Modify** **Delete**	These two buttons are independent and available for each Service Profile. They respectively allow to modify a Service Profile and delete a Service Profile.
K	**Modify** **Delete**	These two buttons are independent and available for each HSS Initial Filtering Criteria. They respectively allow to modify a HSS Initial Filtering Criteria and delete a HSS Initial Filtering Criteria.
L	**Link DSAI**	This button is available for each HSS Initial Filtering Criteria and allows to link a DSAI to a HSS Initial Filtering Criteria. For details on the HssIFCToDSAI entity, refer to the "Subscription Management-HSS application" section of the "HSS Entities" chapter in the *SDM Subscriber Provisioning - Reference Manual.*
M	**Modify** **Delete**	These two buttons are independent and available for each HSS Service Point Trigger. They respectively allow to modify a HSS Service Point Trigger and delete a HSS Service Point Trigger.
N	**Add HssService PointTrigger**	This button is available for each HSS Initial Filtering Criteria (iFC) and allows to add a HSS Service Point Trigger for a HSS iFC. Prerequisite: At least one Service Profile must have already been provisioned with at least one HSS Initial Filtering Criteria.
O	**Add HssInitial FilteringCriteria**	This button is available for each HSS Service Profile and allows to add a HSS Initial Filtering Criteria (iFC) for a HSS Service Profile. Prerequisite: At least one Service Profile must have already been provisioned.
P	**Link HssShared InitialFiltering Criteria**	This button is available for each HSS Service Profile and allows to link a Shared Initial Filtering Criteria (Shared iFC) for a HSS Service Profile. Prerequisite:Shared iFCs must already be provisioned in the database. Refer to the "Configuring Shared Initial Filtering Criterias" section of the SDM System Configuration – User Guide for instructions on how to provision Shared iFCs.

Location in WebCI window	WebCI button(s) available	Operation description
Q	**Modify** **Delete**	These two buttons are independent and available for each Public Identity. They respectively allow to modify a Public Identity and delete a Public Identity.

Displaying the Service Profile, HSS Initial Filtering Criteria and HSS Service Point Trigger Data

This procedure shows how to display all information related to Service Profile, HSS Initial Filtering Criteria, and HSS Service Point Trigger.

1. *Access Subscriber Provisioning submenu*

2. Go to **HSS** > **display/modify**.
   The Subscriber Provisioning window and all associated information is displayed, see *Figure 32: HssServiceProfile table displaying all service profile information*.

3.
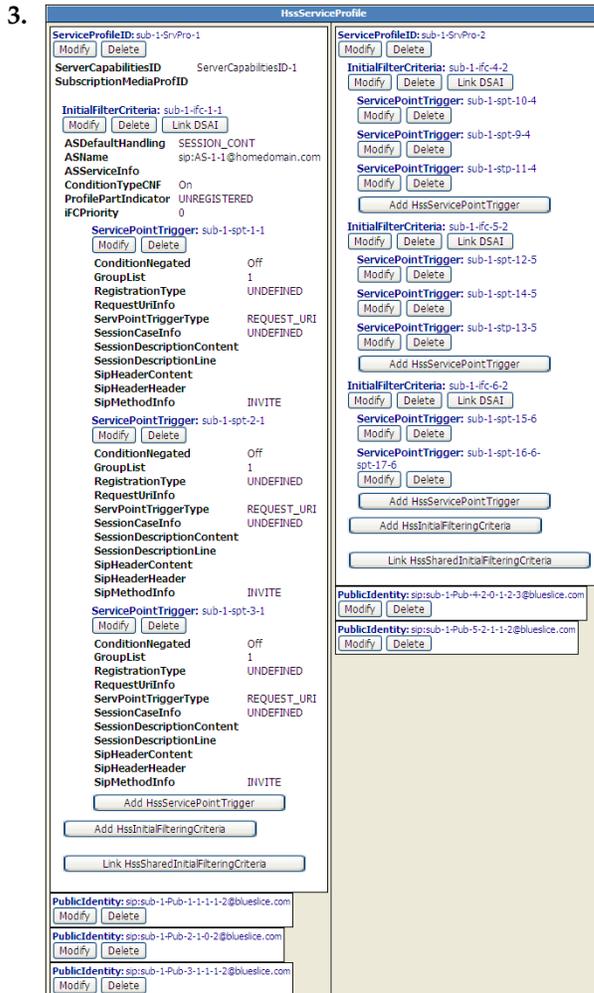
Figure 32: HssServiceProfile table displaying all service profile information

Displaying Subscriber Volatile Data

Use this procedure to display subscriber volatile data from the HlrVolatileData table through the WebCI.

Note: Volatile data cannot be provisioned, it can only be displayed.

1. *Access Subscriber Provisioning submenu*
2. Go to **HLR** > **display/modify**.
   The Subscriber Provisioning window opens to the HLR Provisioning tab.
3. Click the HLR Volatile Data tab.
   The HlrVolatileData table displays the volatile subscriber values configured in the HSS system.

Viewing/editing SLF Redirect host mapping

Prerequisites:

A subscription (SubscriptionID) and its SLF redirect host mapping (Public Identities - Hss host pairs) must already be created before being able to troubleshoot it (display, add, delete) from the WebCI. You can do this by running XML scripts that provision Subscriptions and HSS Subscriber Profiles. Refer to the *SDM Subscriber Provisioning – User Guide* for examples of XML scripts. Moreover, the SLF must already be configured, refer to the "Configuring the HSS/SLF" section of the *SDM System Configuration – User Guide*.

The Network Operator can define the mapping of the SLF Redirect Hosts for each Public Identity, which means that a HSS host can be defined for each of the subscribers' Public Identities. This indicates to the SLF to which HSS it must redirect the messages for a specific Public Identity.

Once SubscriptionIDs and the SLF redirect host mapping have been provisioned in bulk through XML scripts (refer to the *SDM Subscriber Provisioning Reference Manual and User Guide*), the Network Operator can view and edit, from the WebCI, some of the data provisioned for these SLF redirect host mapping. For subscriber related data, the WebCI is mainly helpful for troubleshooting purposes.

For details on SLF redirect host mapping parameters, refer to the "SLF Entities" section of the *SDM Subscriber Provisioning - Reference Manual.*

This section describes how to troubleshoot the SLF redirect host mapping, as follows:

- Display/Add/Delete the SLF redirect host mapping

To provision the SLF redirect host mapping from the WebCI, the operator must follow these steps:

1. *Access Subscriber Provisioning submenu*
2. Go to **SDL** > **display/modify**.
   The Subscriber Provisioning window opens to the HssSlfPublic2HssName tab.
3. Perform one of these operations:

   - Click the `Add HssSlfPublic2HssName` button to define an SLF entry ((Public Identity-HssName pair) by provisioning the 'HssSlfPublic2HssName' table.
   - Click the **Delete** button to delete an SLF entry.
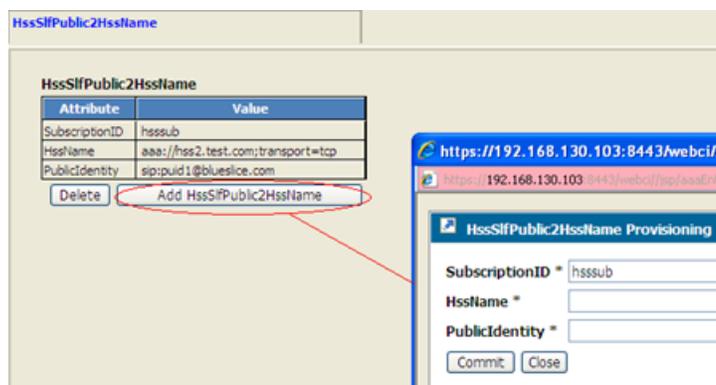
Figure 33: HssSlfPublic2HssName provisioning window

Viewing/Editing AAA Subscriber Profiles

Prerequisites:

1. Subscription (SubscriptionID) and its AAA Subscriber Profile must already be created

2. AAA and AAA Address Allocation Policies must already be configured

Once SubscriptionIDs and AAA subscriber profiles have been provisioned through XML scripts, the Network Operator can use the WebCI to troubleshoot subscriber profiles by viewing AAA subscriber profiles and editing selected data.

This section describes how to troubleshoot a AAA Subscriber Profile, as follows:

- Add/Display/Modify/Delete AAA subscriber profiles (AAAUserId)
- Display User IP Address.
- Add/Display/Modify/Delete AAA User Vendor Attributes
- Add/Display/Modify/Delete AAA User Address Allocation Policies
- Assign/Release IP Addresses
- Display User Status
- Display/Modify
- Display Assigned IP Addresses
- Disconnect User
- Enable User

1. *Access Subscriber Provisioning submenu*

2. Go to **AAA** > **display/modify**.
   The Subscriber Provisioning window opens to the AAAUserId tab. Each AAA user ID has its own table.

3. Edit the AAA Subscriber Profile by clicking on the buttons available from this window.

   The following presents the buttons displayed in the WebCI that allow to execute the different provisioning operations that can be performed to edit the AAA subscriber profile:

   a) **Modify**.

      This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to modify it.

   b) **Delete.**

      This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to delete it.

   c) **Modify/Display AAAUserVendorAttribute.**

      This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to display/add/modify/delete AAA User Vendor Attributes for the AAA subscriber profile.

   d) **Modify/Display AAAUserAddressAllocationPolicies.**

      This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to display/modify/delete or to assign a AAA Address Allocation Policy to the AAA subscriber profile.

e) Prerequisite: A minimum of one AllocationPolicyName must already exist and have been configured in the AAAAddressAllocationPolicy entity (refer to the "AAA Provisioning Configuring- Provisioning AAA Address Allocation Policies and IP Address Pools" of the *SDM System Configuration – User Guide* for instructions on how to add a AAAAddressAllocationPolicy entry).

f) **Display UserStatus.**

This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to display a AAA subscriber's dynamic IP Addresses information. The IP Address (es) dynamically allocated to that AAA subscriber are displayed, as well as the NAS IP Address and the CallingStationID. With the IP Address allocation based on Calling-Station-Id attribute feature, multiple entries are allowed in this table, each with a different Calling Station ID (MSISDN in 3GPP Gi interworking).

g) **Display AssignedIPAddress.**

This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to display the static IP Addresses that the AAA server has already assigned to the AAA subscriber.

h) **Disconnect User.**

This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to send a Disconnect-Request packet in order to terminate a user session on a NAS and discard all associated session context.

Note: Disconnecting a AAA user will disable it.

Note: In the case where a AAA user has IP addresses allocated to multiple MSISDNs, disconnecting the AAA user will disconnect all of the IP connections.

i) **Enable User.**

This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to enable an existing AAA user that was disabled. This operation can be performed to enable a AAA user after it was disconnected using the Disconnect User operation.

j) **Assign IP Address.**

This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows a static IP Address to be associated to a specific Called Station (APN) or Realm. If desired, a Calling Station (MSISDN) can also be added, in order to identify the subscriber. When executing this operation for a subscriber, the Called Station must be specified in the indicated field; the realm, on the other hand, doesn't need to be entered, it is extracted from the AAAUserName. With this information, the AAA server associates an IP Address to the Called Station or Realm from the configured IP Address pools. This IP Address is said to be static and becomes unavailable for allocation by the AAA server when performing dynamic allocation of an IP Address. For a single subscriber, a different static IP Address can be assigned for each Called Station (APN) or Realm. Moreover, for a subscriber's specific Calling Station (MSISDN), different static IP addresses can be assigned for different Called Stations (APNs).

The following are the four cases in which a static IP address can be assigned for a AAA user:

k) **Case 1:** The subscriber's AAAUserName doesn't include the realm and is defined in a format such as aaauser1.

In this case, the operator can assign a static address to the subscriber by providing a called station, which is associated with an address pool. The address is selected from the pool associated

with the called station. On receiving an access-req from the subscriber for this called station the assigned static address is returned.

l) **Case 2:** The subscriber's AAAUserName includes the realm and is defined in the following format: user@realm.

In this case, the operator can assign a static address to the subscriber, without providing a called station. An address is selected from the address pool associated with the user's realm. The assigned address will be provided for all access requests for the user with this realm, regardless of called station.

m) **Case 3:** The subscriber's AAAUserName includes the realm and is defined in the following format: user@realm.

In this case, the operator can assign a static address to the subscriber by specifying a called station, which is associated with an address pool. Since a called station is specified, the user's realm is not considered. An address is assigned based on the called station. Access-requests for the this user to the specified called station will be provided with the assigned address.

n) **Case 4:** The subscriber's AAAUserName doesn't include the realm and is defined in a format such as aaauser1.

In this case, the operator can assign a static address the subscriber, with no realm and no called station or a realm or called station that aren't associated with an address pool. In this case, an address is assigned from the system default pool and the address is allocated for any access-requests for the user, regardless of called station.

Requirements:

o) Case 1: The called station, for which the operator wishes to assign a static IP address, must be associated with an address pool.

For instructions on how to make the association between an address pool and the Called Station Id, refer to the "AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address pools" section of the *SDM System Configuration – User Guide*. When executing this procedure, set the AssociationType parameter to '2' (CALLED_STATION_ID). Moreover, you have to make sure that IP addresses are assigned to that pool, by setting an IP address range (refer to the "AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address pools" section of the *SDM System Configuration – User Guide*).

p) Case 2: The AAA user must have a AAAUserName defined in the following format: user@realm. The realm, for which the operator wishes to assign a static IP address, must be associated with an address pool.

For instructions on how to make the association between an address pool and the Realm, refer to the "AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address pools" section of the *SDM System Configuration – User Guide*. When executing this procedure, set the AssociationType parameter to '1' (REALM). Moreover, you have to make sure that IP addresses are assigned to that pool, by setting an IP address range (refer to the "AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address pools" section of the *SDM System Configuration – User Guide*).

q) Case 3: The AAA user must have a AAAUserName defined in the following format: user@realm.

The called station, for which the operator wishes to assign a static IP address, must be associated with an address pool. For instructions on how to make the association between an address pool and the Called Station Id, refer to the "AAA Provisioning Configuration – Provisioning AAA

Address Allocation Policies and IP Address pools" section of the SDM System Configuration – User Guide. When executing this procedure, set the AssociationType parameter to '2' (CALLED_STATION_ID). Moreover, you have to make sure that IP addresses are assigned to that pool, by setting an IP address range (refer to the "AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address pools" section of the *SDM System Configuration – User Guide*).

r) Case 4: In this case, the static IP address is assigned from the system default pool.

In this case, a default pool must already be defined and must be associated to the system. Refer to "Add AAA Address Allocation Policy" in the *SDM System Configuration – User Guide* in order to define a default Address Allocation Policy and "Add the AAA Address Pool Association" in order to associate the default Address Allocation Policy to an Association Type set to '0' (SYSTEM). Moreover, you have to make sure that IP addresses are assigned to the default pool, by setting an Address Allocation range (refer to the "AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address pools" section of the *SDM System Configuration – User Guide*).

Follow either one of these steps, depending on the case in which you wish to assign a static IP address for a user:

s) For Case 1 and Case 3 described above, enter the Called Station Id next to the Called Station field, at the bottom of the AAAUserId table of the AAA user for which you wish to assign a static IP address.

Click on the **Assign IP Address** button. Please note that the Called Station you enter here must have already been associated to an Address Allocation Policy when adding a AAA Address Allocation Association (refer to *step 3* in the " AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address Pools" section of the *SDM System Configuration – User Guide*).

t) For the Case 2 and Case 4 described above, simply click on the **Assign IP Address** button.

u) **Release IP Address.**

This button is available for each AAA User Id (AAA subscriber profile) provisioned and allows to release a static IP Address. When executing this operation for a Called Station (and optionally Calling Station) of a subscriber, the AAA server releases the static IP Address that was assigned for that subscriber's Called Station (and Calling Station). This means that this IP Address is now available in the pool for dynamic IP allocation and is no longer reserved uniquely for that subscriber's Called Station (and Calling Station).

v) Prior to clicking on the **Release IP Address** button, the following parameters can be specified:

4. CalledStation: optional parameter that represents the Called-Station-Id (e.g., APN) to which the static IP address is associated.

Whenever an Access-Request with this Called-Station-Id arrives, the corresponding static IP address will be allocated. The value supported for this parameter is 'string'. If no CalledStation is indicated and the AAAUserName contains a Realm (i.e., the AAAUserName is in the format *user@realm*), the static IP address is released from its association with the user's realm.

5. CallingStation: optional parameter that represents the Calling-Station-Id (e.g., MSISDN) that identifies the subscriber to which the static IP address is assigned.

The value supported for this parameter is 'string'.

Simply click on one of these buttons to execute the corresponding operation. Refer to *Web Craft Interface (WebCI)* for instructions on how to provision a table through the WebCI.

For details on the different AAA Operations, refer to the "AAA Operations" section of the *SDM System Configuration - Reference Manual*.

Figure 34: AAAUserId Window

Viewing/Editing DNS ENUM Users

This section describes how to provision DNS ENUM Users from the WebCI.

Multiple DNS Enum Users can be provisioned for one single Subscription.

1. *Access Subscriber Provisioning submenu.*
2. Go to **ENUM Server** > **display/modify**.
   The Subscriber Provisioning window opens to the Enum User tab.
3. Click the **SubscriptionId** for which you wish to provision a DNS Enum User.
4. When the Subscriber Provisioning window pops up, extend the ENUM Server sub-folder and click on display/modify.
5. The DNS Enum User table will appear and allow you to view the already provisioned users or and/or allow you to add, edit, delete entries. For details on the parameters needed to provision ENUM Users, refer to the ENUM chapter of the *SDM Subscriber Provisioning - Reference Manual.*
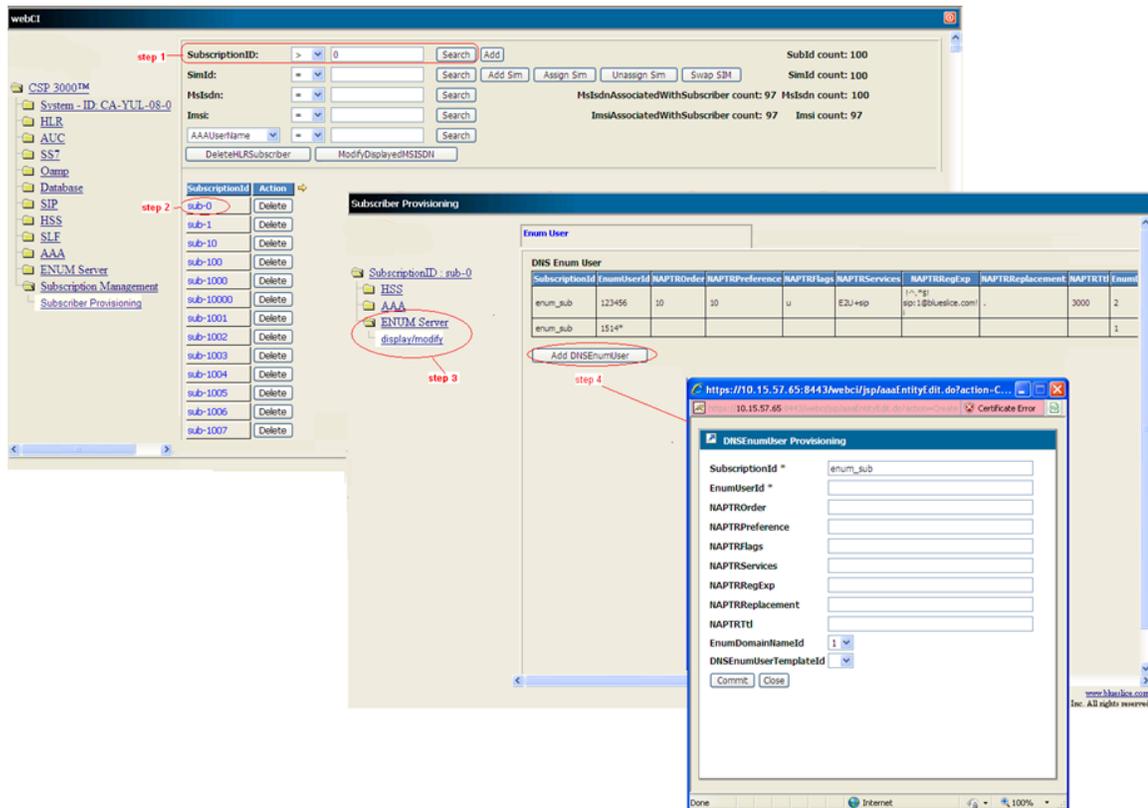
Figure 35: Provisioning DNS Enum Users

Provisioning LTE-HSS Subscriber Profiles

This procedures describes how to provision view, edit, add) LTE-HSS profiles from the WebCI. This can be achieved within the HLR Subscriber Profile.

Prerequisites:

- A subscription must already be created for the subscriber with the SIM/MSISDN/SimImsiMap/MsIsdnImsiProfileAssociation and HLR Subscriber profile (with service profile) already defined. Note that when defining a SIM with a SimType='Offboard', an AlgorithName must still be provided. The AlgorithName can be any of the ones already configured in the system's AuC. See *Viewing/editing SIM cards, MSISDNs, IMSIs, and HLR subscriber profiles*
- HLR-Proxy functionality has been configured through the CLI (see *HLR Proxy functionality*" in the *SDM System Configuration – Reference Manual*.
- PDN Context Templates must already have been configured in the system. See "PDN Context Templates Configuration" section of the *SDM System Configuration – User Guide*.

1. *Access Subscriber Provisioning submenu*.
2. Go to **HLR** > **display/modify**.
   The HLR provisioning window displays.

3. Locate the Service Profile ID table and click **Modify** next to the Service ProfileID.

Service Profile

ServiceProfileId	Action
1	Modify Delete

ServiceProfileID: [_____] Add

The Subscriber Provisioning window displays.

4. Provision the following fields: DefaultPdnContextId, SpPdnChargingCharacteristics, HlrProxyMode, AMBRUL , AMBRDL, APNOIReplacement, RFSPId. For a description of these parameters, their values supported and their default values, refer to the "Subscriber Profile (Bearer Services, Teleservices, Call Barring, PreferredRoutingNetworkDomain)" sub-section of the *SDM Subscriber Provisioning-Reference Manual's* "HLR Subscriber Provisioning" chapter.

DefaultPdnContextId:	2
SpPdnChargingCharacteristics:	HotBilling / FlatRate / Prepaid / Normal
HLRProxyMode:	☑
AMBRUL:	4000
AMBRDL:	2000
APNOIReplacement:	
RFSPId:	

5. Click the HLRProxyMode checkbox.

6. Define PDN Context by provisioning the PDN Context, PDN MipAgentInfo, and CSG Subscription Data tables.

PDN Context

CSG Subscription Data

PDN ContextId	PDN Type	PDN Address1	PDN Address2	PDN TemplateId	Action	CSG Id	CSG Expiration Date	Action
1	IPv4	192.168.20.12		1	Delete	1	2012-03-14 01:00:54	Delete
2	IPv4	192.168.20.13		1	Delete		Add CSG SubscriptionData	
3	IPv4_OR_IPv6	192.168.20.15		1	Delete			

Add PDN Context

PDN MipAgentInfo

PdnContextId	AccessPointName	MipHaAddress1	MipHaAddress2	MipHaDestHost	MipHaDestRealm	Mip6HomeLinkPrefix	Action

Add PDN MipAgentInfo

For details on these tables, their parameters and supported values, refer to the "LTE-HSS profile – PDN Context/CSG" section of the *SDM Subscriber Provisioning – Reference Manual*.

Viewing/editing Subscriber (Policy) profiles

This procedure describes how to provision or troubleshoot a subscriber profile using WebCI.

The Network Operator can troubleshoot subscriber profiles by viewing and editing some of the subscriber data, for example:

- Display user data/quota/state
- Modify or delete the following subscriber profile data:

  - AccountId
  - MSISDN
  - IMSI
  - Entitlement
  - NAI,
  - PublicIdentity
  - BillingDay
  - Custom1 through Custom20
  - Tier

1. Go to **Subscription Management** > **Subscriber Provisioning**.

   The Subscriber Provisioning window displays.

2. To create an SPR subscriber, click **AddSPRProfile**.

   The Policy Subscriber pop-up window displays.

   a) Enter the subscriber identities.

      Enter all identities to support multi-key network access.
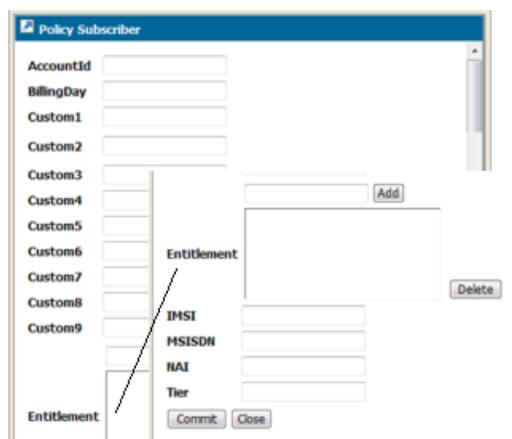
   b) Add entitlements by entering the data in the field to the left of the **Add** button, then click **Add**.

      The entitlement displays in the Entitlement field.

   c) Remove an entitlement by selecting the entitlement in the Entitlement field and click **Delete**.

   d) Enter the values for the remaining fields.

      Note: Entitlement values can be added or deleted. All other values can be only added.

     e) Click **Commit.**

3. To edit an existing subscriber profile, retrieve the subscriber profile:

     a) Select one of its mandatory primary key types from the identity drop down list.
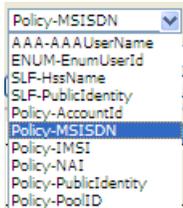
     b) Enter the key value in the right field and click **Search**.

     The Subscriber Profile table displays the profile matching the key value as well as a Quota table if quota is defined.
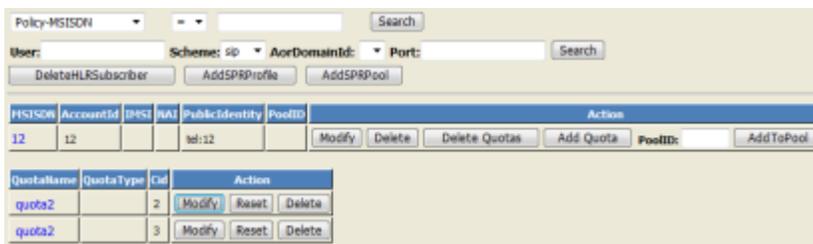
     Note: If multiple quotas exist with the same name then each will be displayed on a separate line along with their associated Quota type and Cid value.

4. Perform one or more of these actions from the subscriber table:

- To modify a quota entity select the appropriate row and **Modify**. The following table is
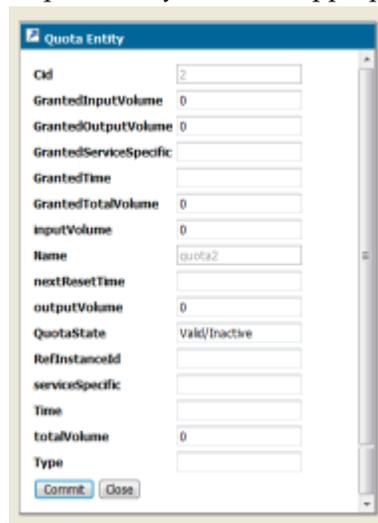
displayed.

For more information about the attributes please refer to section *Subscriber Quota* in the *Subscriber Provisioning Reference Manual*.

Note: State data is opaque data. It can be edited as fields through XML interfaces only.

- Click **Delete** to delete profile data.

- Click **Delete Quotas** to delete all quotas of a subscriber.

  Note: This operation deletes all values, names, and even the database entry in the SPR volatile data.

- Click **Add Quota** to add a quota to the subscriber profile.

  Note: Multiple quotas can be defined for a subscriber profile.

- Click **DeleteFromPool** to delete the subscriber from the pool.
- Click **AddToPool** to add the subscriber to the pool.

Viewing/editing SPR subscriber quota (WebCI)

This procedure describes how to provision the subscriber quota using the WebCI.

The subscriber quota represents the subscriber usage of managed resources. Use this procedure to adjust the subscriber quota to maximize resource usage.

1. Go to **Subscription Management** > **Subscriber Provisioning**.
   The Subscriber Provisioning window displays.

2. Retrieve the existing SPR subscriber by selecting one of its mandatory primary key types from the identity drop-down list.

   a) Enter the key value in the right field.
   b) Click **Search**.

   The Subscriber Profile table displays the profile matching the key value as well as a Quota table if quota is defined.

3. In the subscriber profile table, click **Add Quota** to add a new quota to the subscriber profile. Enter a quota name and the quota data and commit.

Unspecified fields are set to their default values.

4. Click **Delete Quotas** to delete all quotas of a subscriber.

Note: This operation deletes all values, names, and even the database entry in the SPR volatile data.

5. To edit quota data from the Subscriber Quota table, perform one of these steps:

- Click **Modify** to change quota data.

Note: When editing the NextResetTime field, the timestamp format must follow this convention: `[-]CCYY-MM-DDThh:mm:ss[Z|(+|-)hh:mm]`

For example:

`2012-05-07T00:00:00Z` (UTC) or

`2012-05-07T00:00:00-05:00` (UTC minus 5 hours = US Eastern Standard Time)

- Click **Reset** to reset the quota usage to the default values assigned to the Subscriber Quota table.
- Click **Delete** to delete a quota from the subscriber profile.

Viewing/editing SPR Pool information (WebCI)

This procedure describes how to display pool information, create an SPR pool, adding a subscriber to a pool, and editing existing pool information using the WebCI.

Each subscriber can be a member of only one pool.

1. Go to **Tekelec SDM** > **Subscription Management** > **Subscriber Provisioning**. The Subscriber Provisioning window displays.

2. To create an SPR pool, click **AddSPRPool** and enter pool identity and pool data, then commit.

3. To manipulate any pool data, retrieve the pool information by selecting Policy-PoolID from the drop-down menu, enter the PoolD to the right, and click **Search**.

The Pool table displays with the actions that can be performed on the pool.

4. To display Pool data, click the hyperlink of the PoolID.

5. To display all members of a pool, to add a subscriber to a pool, or to delete a subscriber from a pool, click **Manage Subscribers**.

The Subscriber List displays.

a) To add a subscriber to the pool, enter the PublicIdentity and click **Add Subscriber**.
b) To delete the subscriber from the pool, click **DeleteSubscriber**.

Confirm that you want to delete the subscriber.

6. To modify pool data, click**Modify** in the pool table.

Chapter

5

Monitoring the system

Topics:

This chapter contains information used to monitor the Subscriber Data Management system for alarms and other errors.

Viewing and Managing Alarms

Active Alarm View

The Active Alarm window provides a listing of all active alarms existing on the shelf. The alarms can be viewed according to Sequence Id number, Alarm Id number, Severity accompanied with its corresponding color, Description, Shelf Id number, Slot Id number, Alarm Set Time, Alarm Set Last Time, Alarm set by which application, Alarm Count, Acknowledge time, Alarm acknowledged by which user and there is a last option that permits the operator to acknowledge and clear the alarm. The operator can not only view all the active alarms, but he can also acknowledge and clear each active alarm. It is important to note that each alarm must be acknowledged before being cleared. The following task list shows the different tasks the operator can perform in the Active Alarm View.

Table 22: Active Alarm Procedures

TASK	PROCEDURE
Active alarms	
1. View active alarms	*View Active Alarms*
2. Acknowledge active alarms	*Acknowledge Active Alarms*
3. Clear active alarms	*Clear Active Alarms*

View Active Alarms

This procedure describes the steps to view active alarms. For details on the alarm window attributes, refer to the "System entities" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. By default, the alarms are sorted by Sequence Id in ascending order. Oldest alarms are displayed at the top.

1. Open the `System folder` by clicking it.
2. Click on **Active Alarm View**.
3. The Active Alarms window appears (as follows) displaying all the active alarms.

Figure 36: Active Alarm Window

Acknowledge Active Alarms

This procedure describes the steps to acknowledge active alarms. For details on the alarm window attributes, refer to the "System entities" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual.*

1. Open the **System folder** by clicking it.
2. Click on **Active Alarm View**.
3. The Active Alarms window appears as shown in *Figure 36: Active Alarm Window*.

    You will be able to notice that by default, the alarms are all checked with a green circle in the last column.

4. To acknowledge one specific active alarm:

    Click on the **green circle** corresponding to the active alarm you wish to acknowledge.

5. This will result in the display of the date and time in the Acknowledge Time column for the specific alarm you just acknowledged and in the display of the user that acknowledged the alarm in the Ack By column.

    In the example shown in the figure below, the acknowledged alarm is the Alarm Id:7012.

Figure 37: Active Alarm Window With An Active Alarm Acknowledged

6. An acknowledge notification will be recorded in the Alarm History.

    More precisely, the acknowledge date and time will be registered and appear in the Acknowledge time column and the user that acknowledged the alarm will be displayed in the Ack By column. In the example shown in the figure below, the acknowledged alarm is the Alarm Id: 7012.

Figure 38: History Alarm Window With An Active Alarm Acknowledged

Acknowledge All Alarms

You can also acknowledge all the alarms at once. To acknowledge all the alarms, click the **Acknowledge all** action button located at the top right corner of the Active Alarm window.

The operator can use this operation to acknowledge all the active alarms. This will result in the Acknowledge Time column of the Active Alarms window to display the date and time of the acknowledgement of each alarm and in the Ack By column to display the user that acknowledged the alarm. An acknowledge notification will be recorded in the Alarm History. More precisely, for each acknowledged active alarm, the acknowledge date and time will be registered and appear in the Acknowledge time column and the user that acknowledged the alarm will appear in the Ack By column.

Note: The acknowledge operation does not clear the alarm condition that generated the alarm.

Clear Active Alarms

The Network Operator can manually clear individual active alarms, one at a time, under the following conditions:

* The alarm has already been acknowledged.(See previous procedure for instructions on how to *Acknowledge All Alarms*)
* The alarm is defined as an alarm that can be manually cleared.
* The required action to rectify the condition for which the alarm was raised has been taken

    When all of these conditions have been met for an alarm, the WebCI displays a **x** button in the last column of the Active alarm table. This indicates that the Network Operator can clear the alarm.

    This procedure describes the steps to clear an active alarm from the WebCI. For details on the alarm window attributes, refer to the "System entities" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual.*

1. Open the **System folder** by clicking it.
2. Click on **Active Alarm View**.
3. At this point, the alarms that can be cleared are the ones that have already been acknowledged (acknowledged alarms have an acknowledge time and acknowledged by (Ack By) name displayed) and that have a **x** button available in the last column of the table.

Figure 39: Active Alarm Window With Alarm That Can Be Manually Cleared

4. To clear one specific active alarm:

    a) Click on the **x** corresponding to the active alarm you wish to clear.

5. A window will automatically appear and display the following message (i.e., Sequence ID of the active alarm to be cleared: 936):

    Clear Alarm with Sequence ID: 936

6. If you are certain that you want to clear this specific active alarm:

    a) Click **OK.** Otherwise: Click **Cancel**

7. This will result in the removal of the active alarm in the Active Alarms window and in the addition of a "Cleared" alarm entry in the History Alarms.

    You will be able to identify this new entry by the Alarm Id and you will also be able to verify its status, which displays "Cleared" in the last column Set/Clear. For a cleared alarm, the WebCI also displays the username of the user (in the case where the alarm can be manually cleared) or the name of the application that cleared the alarm.

    The figure below displays the History Alarm window with several cleared alarms. In order to allow you to easily identify them, the 'Set/Clear' state and 'Clear By' name have been manually circled.

Figure 40: History Alarm Window With Cleared Alarms

Auto Refresh

The Active Alarm window provides a snapshot listing of the alarms currently active on the system. The window is refreshed every 15 seconds.

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 .

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

Sorting Alarms

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).

View History Alarms

This procedure describes how to view the alarm history. The History Alarm window provides a chronological listing of all the alarms that have been set (i.e., raised) as well as those that have been cleared on the system. The alarms are listed in descending order according to the Sequence Id. This will list the most recent alarm events at the top. For details on the alarm history window attributes, refer to the "System entities" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*.

1. Open the **System** folder by clicking it.
2. Click on **History Alarm View**.

3. The History Alarms window appears (as follows) displaying all the alarms that occurred and when they have been created.

Figure 41: Alarm History Window

The History Alarm window displays the 50 most recent history alarm events at a time.

To view the Previous 50 events, click on the **left arrow** .

To view the Next 50 events in the list, click on the **right arrow** .

The Active Alarm and History Alarm windows also offer another feature that helps you identify more quickly the degree of severity of each alarm. The severity description for each alarm is accompanied with a color. The following table presents each of the severity degree and its corresponding color displayed.

Table 23: Alarm Severities and Colors

Severity description	Color
Warning	Turquoise
Minor	Yellow
Major	Orange
Critical	Red

Viewing Logs

Accessing log files

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 on the active System Controller can be viewed from the CLI.

The current day logs are stored in an XML file called *current.xml*. This file is located in the directory /blue/var/log.

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

Accessing Log Files

This procedure outlines the steps to view the current system log messages.

Requirements: Log in to your SSH client to access the system with your username and password. It is important to note that only the users part of the Operation and Admin User Groups can do the following procedure.

1. Access the log directory by typing,

    admin@p0s2 # cd /blue/var/log

2. List the logs in the directory by typing,

    admin@p0s2 # ls

3. View the logs by specifying the filename and typing,

    admin@p0s2 # more current.xml

    The items in the log are shown below:

Table 24: Accessing Log Files

Item	Description	
type	the type of system log	
code	an error message identifier which is a unique value	
severity	Trace	indicates function calling sequence
	Debug	debugging information
	Info	information normally used when debugging a problem

Item	Description	
	Notice	non-error conditions that may require special handling
	Warning	warning
	Error	error
	Alarm Warning	warning alarm
	Alarm Minor	minor alarm
	Alarm Major	major alarm
	Alarm Critical	critical alarm
eventType	Log or Trace	
description	additional information describing the log event	
timeStamp	in GMT format (YYYY-MM-DDThh:mm:ss)	
fileName	module file name	
lineNumber	module file line number	
SequenceNumber	log sequence number generated by client application	
slotId	slot where the event was generated	

Configuring and Enabling/Disabling Audit Logging

This section describes how to configure the following Audit log files management options:

- 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.

  Moreover, it describes how to enable/disable the audit logging for a specific audit component. In the current release, only the AaaIp audit component is supported for the AAA Logging of IP address allocation feature.

  For a detailed description of the AAA Logging of IP address allocation feature, refer to the "AAA address allocation" section of the *SDM Product Description*.

  In order to configure the system to enable the AAA Logging IP address feature, the audit logging mechanism must first be enabled as follows:

1. Configure audit options (format, history, debug information) by provisioning the AuditManager[] entity.

   For all the information on this entity, its CLI navigation path and attribute values, refer to the "Audit log file Management" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. For instructions on how to get around in the CLI or WebCI, refer to *Command Line Interface (CLI)* and *Web Craft Interface (WebCI)*.

2. Enable/Disable the audit logging per audit component by provisioning the AuditInfo[] entity.

   For all the information on this entity, its CLI navigation path and attribute values, refer to the "Audit log file Management" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. For instructions on how to get around in the CLI or WebCI, refer to *Command Line Interface (CLI)* and *Web Craft Interface (WebCI)*.

3. Execute the StartAudit() operation.

   Refer to the "Audit Log file Management" section of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual* for more details on the StartAudit() operation.
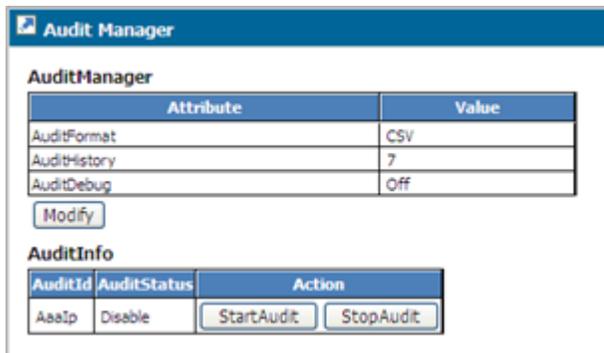
Figure 42: Audit Manager Window

4. Enable/Disable the audit logging per AAA Address Allocation policy by setting the AuditLoggingEnabled parameter in the AAAAddressAllocationPolicy entity.

   In order to configure the system to disable the AAA Logging IP address feature, the audit logging mechanism must be disabled, as follows:

5. Disable the audit logging for each AAA address allocation policy, by setting the AuditLoggingEnabled parameter to 'Disable' in the AAAAddressAllocationPolicy entity.

   Refer to the "AAA Provisioning Configuration – Provisioning AAA Address allocation Policies and IP address pools" section of the *SDM System Configuration – User Guide* for instructions on how to modify the AuditLoggingEnabled parameter to the 'Disable' value in the AAAAddressAllocationPolicy entity. Note that by default, the AuditLoggingEnabled value is set to 'Disable'.

6. Execute the StopAudit() operation.

   Refer to the "Audit Log file Management" section of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual* for more details on the StopAudit() operation.

Display Event Logs with WebCI

1. Open the System folder by clicking on it.
2. Click **Event Log View**. The Event Log View screen displays.
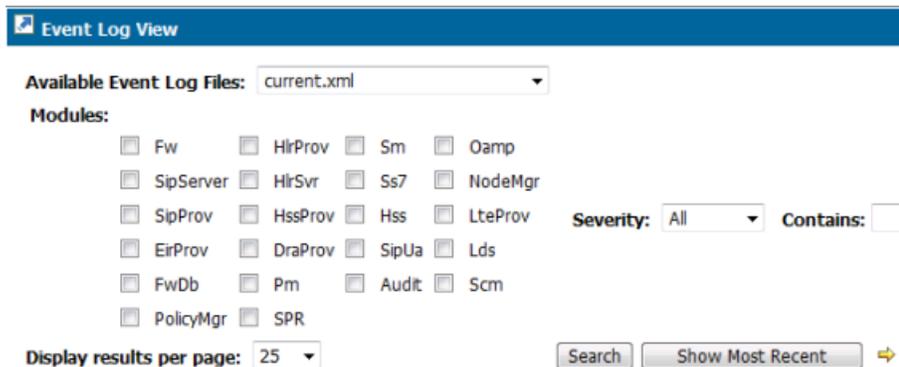
Figure 43: Event Log View

3. Select the Event Log File from the dropdown list.
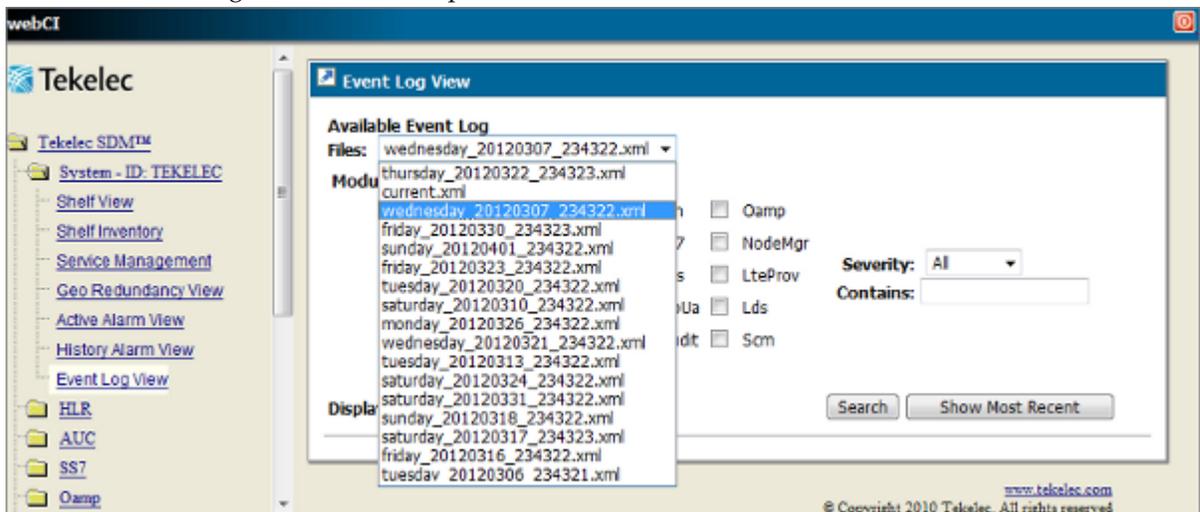
Figure 44: Available Event Logs

4. Search the Event Log File using the following criteria:

Modules

- All
- Fw
- HlrProv
- Sm
- Oamp
- SipServer
- HlrSvr
- Ss7
- NodeMgr
- SipProv
- Hssprov
- Hss
- LteProv

- EirProv
- DraProv
- SipUA
- Lds
- FwDb
- Pm
- Audit
- Scm
- PolicyMgr
- SPR

Severity

- All
- Warning
- Critical
- Major
- Minor

Contains - search using text that describes the log event.

Display results per page - 25, 50, 100

5. Click **Search** or **Show Most Recent**. Event Logs are displayed in a table as shown below. Search displays the Event Logs in ascending chronological order and Show Most Recent displays the Event Logs in descending chronological order.

Type	Code	Category	Severity	eventType	Description	TimeStamp	FileName	LineNumber	SequenceNumber	SlotId
Oamp	7010	OampManager	ALARM_CRITICAL	LOG	Active subscribers license violation. (clear-0)	2012-02-22T2:0:16Z	OampManagerLicenseHandler.cpp	184	70	3
Oamp	7009	OampManager	ALARM_WARNING	LOG	Active subscribers license warning. (clear-0)	2012-02-22T2:0:16Z	OampManagerLicenseHandler.cpp	184	71	3
SPR	70111	DataAccessServer	WARNING	LOG	Subscriber field not found for key/value NAI/test999.com	2012-02-22T11:54:41Z	Select.cpp	90	12	4
SPR	70111	DataAccessServer	WARNING	LOG	Subscriber field not found for key/value AccountId/123	2012-02-22T11:57:43Z	Select.cpp	90	12	3
SPR	70210	DataAccessServer	WARNING	LOG	Quota not found for key/value MSISDN/1234567890	2012-02-22T11:59:26Z	Select.cpp	150	13	3
SPR	70210	DataAccessServer	WARNING	LOG	Quota not found for key/value MSISDN/1234567890	2012-02-22T11:59:26Z	Select.cpp	150	14	3

Figure 45: Event Log Display

Accessing VLR Message Notification Logs

This procedure outlines the steps to be taken in order to view the VLR Message Notification logs.

Requirements: Log in to your SSH client to access the system with your username and password. All users have read only access. Use the following procedure to access VLR Message Notification Logs.

1. Access the log directory by typing

   cd /blue/var/log/csv

2. List the logs in the directory by typing

   ls

3. View the logs in the directory by typing

   more VlrMessageNotification.csv

4. There is a line for each VLR message notification in the log file. The line displays the data in the following order:

Item	Description
MSISDN	The "displayed" MSISDN of the subscriber
IMSI	The registered IMSI of the subscriber
Source Gtt	The global title (e.164) address of the node that sent the message (VLR or SGSN)
Message Type	The type of message received (UL, UL_GPRS, SAI, ReadySM, PurgeMS, ISD, DSD)
Time Stamp	The local timestamp (format: YYYY-MM-DD HH:MM:SS)
MSC address	The MSC e164 address
Alert Reason	The Alert Reason
Result Notify	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
SourceSSN	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)
Retry Number	The number of retries that have taken place for Dialogue Re-initiation upon Failure

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

5. Here is an example of a VLR Message Notification Log:

```
15634210001,310910421000001,15634110002,UL,2013-09-25 16:07:32,15634110004,,0,7,
15634210001,310910421000001,15634110002,UL,2013-09-25 16:08:26,15634110004,,0,7,
15634210001,310910421000001,15634110002,UL,2013-09-25 16:08:30,15634110004,,0,7,
,310910421000001,15634110002,CL,2013-09-25 16:08:40,,,0,7,
15634210001,310910421000001,15634110002,UL,2013-09-25 16:08:47,15634110004,,0,7,
,310910421000001,15634110002,ISD,2013-09-25 16:09:45,,,6,7,1
,310910421000001,15634110002,ISD,2013-09-25 16:10:20,,,6,7,2
,310910421000001,15634110002,ISD,2013-09-25 16:10:28,,,0,7,2
,310910421000001,15634110002,DSD,2013-09-25 16:11:17,,,6,7,1
,310910421000001,15634110002,ISD,2013-09-25 16:11:17,,,6,7,1
```

```
,310910421000001,15634110002,DSD,2013-09-25 16:11:52,,,6,7,2
,310910421000001,15634110002,ISD,2013-09-25 16:11:52,,,6,7,2
,310910421000001,15634110002,ISD,2013-09-25 16:12:30,,,6,7,3
,310910421000001,15634110002,DSD,2013-09-25 16:12:30,,,6,7,3
```

Adding a header to the VLR Message Notification Logs

By default the VLR Message Notification Log has no header. If you wish to add a header to the VLR Message Notification Log please contact the Tekelec *My Oracle Support (MOS)*.

Removing a header from the VLR Message Notification Logs

By default the VLR Message Notification Log has no header. If you have added a header and wish to remove it please contact the Tekelec *My Oracle Support (MOS)*.

VLR Message Notification Log File retention

By default the VLR Message Notification Logs are stored for 7 days in `blue/var/log/csv`. If you wish to change the number of days please contact the Tekelec *My Oracle Support (MOS)*.

Accessing LTE-HSS Logs

This procedure outlines the steps to be taken in order to view the LTE-HSS logs.

Requirements: Log in to your SSH client to access the system with your username and password. All users have read only access. Use the following procedure to access LTE-HSS Logs.

1. Access the log directory by typing

    cd /blue/var/log/csv

2. List the logs in the directory by typing

    ls

3. View the logs in the directory by typing

    more lteHSSCaleaLog.csv

4. There is a line for each LTE-HSS event in the log file. The line displays the data in the following order:

Item	Description
Time Stamp	The local timestamp (format: YYYY-MM-DD HH:MM:SS)
Request Type Code	The request type code
MME/SGSN HostName	The host name
Diameter Result Code Number	The diameter result code
IMSI	The registered IMSI of the subscriber

Item	Description
Visited PLMN ID	The identification of the visited PLMN
Alert Reason	The alert reason
Cancellation Type	The cancellation type
MSISDN	The "displayed" MSISDN of the subscriber
Requested Authentication	The authentication request
IMEI	The IMEI

Empty parameters are represented by a null character between two commas. (,,). The content of each line in the LTE-HSS log differs based on the type of diameter message query received by the LTE-HSS.

5. Here is an example of an LTE-HSS Log:

```
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
```

Accessing SPR provisioning logs

This procedure describes how to access and view an SPR provisioning log.

Requirements: Log in to your SSH client to access the system with your username and password. All users have read-only access.

1. Access the log directory by typing

   cd /blue/var/log/csv

2. List the logs in the directory by typing

   ls

3. Retrieve one of the logs:

   • To retrieve the current log file, type: **more provlog.csv**
   • To retrieve an older log file, type: **provlog.<date_time>.csv**, for example,
     provlog.20131024_15h54m30s.csv

The log contains a line for each provisioning event. The line displays the data in the following order:

Item	Description
Time Stamp	Local timestamp (format: YYYY-MM-DD HH:MM:SS)

Item	Description
Source	IP address (XML-REST operations) or subscriber name (CLI, WebCI, XML operations) that originated the request
Request Type Code	Action requested (create/modify/delete/retrieve), for example, INSERT, UPDATE, DELETE, SELECT
Primary Key	Key of the affected subscriber (MSISDN, IMSI, or NAI)
Command Parameters	All values to be created, modified, deleted, or retrieved
Result Code	Success/failure, other error codes

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

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 subscriber 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
```

All log files can also be retrieved to an external server using the SCP/SFTP protocol .

Using traces

The system generates Traces for each system module for debugging purposes and to provide information on the actions that have been executed on the system and their sequence. Traces provide the Tekelec *My Oracle Support (MOS)* and the operator with an additional level of information and allow them to verify correct operation of the SDM.

⚠️
WARNING

Warning: Traces are only useful for debugging purposes and should not be managed by the operator. Before troubleshooting, the operator must contact the Tekelec *My Oracle Support (MOS)*, who will help you debug by using the system traces.

Unlike all other log events in the system, traces are stored locally where they are produced. They are stored locally on the blade (under the `/blue/var/trace` directory) where the application concerned is running. Hence, trace files can be viewed from the blade which produced it through the CLI.

Note:

System events with the following levels are all called traces:

- Trace

- Trace Error

All of the events of Trace Error level are by default always activated, which means that they can always be viewed and accessed.

However, events of Trace level are by default all deactivated. Some events of Trace level may have been activated by Tekelec and can only be managed (activated/deactivated) by the Tekelec *My Oracle Support (MOS)* during troubleshooting. In addition to activating or deactivating the necessary traces, the Tekelec *My Oracle Support (MOS)* will be able to filter some events of Trace level on a per component basis for each process.

Accessing Traces

Warning: You must contact the Tekelec *My Oracle Support (MOS)* prior to performing this operation.

This procedure outlines the steps to view the system's traces. If no traces were activated by Tekelec prior to performing this operation, then only events of Trace Error level will be displayed and accessed. On the other hand, if some traces were previously activated, all events of Trace Error level will be displayed as well as the events with Trace level that were activated. When contacting Tekelec's Technical Support team, the proper necessary traces will be activated/deactivated and/or filtered in order to allow access to all the needed traces to be able to proceed with the correct debugging of the system.

Requirements: Log in to your SSH client to access the system with your username and password. It is important to note that only the users part of the Operation and Admin User Groups can do the following procedure as per instructed and only when requested by the Tekelec's Technical Support team.

1. Access the trace directory by typing,

   admin@p0s2 # cd /blue/var/trace

2. List the trace files in the directory by typing,

   admin@p0s2 # ls

3. View the traces of one of the listed trace files by specifying its filename and typing:

   admin@p0s2 # more HlrServer.xml

4. Traces will be displayed.

   If the file contained a long list of traces, only sections will be displayed at a time. To see the next section, press **ENTER** on your keyboard.

5. Here is a section of the traces that will be displayed, as per an example:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type='text/xsl' href='logs.xslt'?>
[Fri Dec 19 2008 16:36:31:103862][Slot:5][bHlrSS7Main.cc(128)][HlrServer(HLR_INF
O)][Tid:4115138240][DEBUG]
->HlrSS7 main : app name = HlrServer instance = 5
[Fri Dec 19 2008 16:36:31:106534][Slot:5][bHlrSS7Main.cc(130)][HlrServer(HLR_INF
O)][Tid:4115138240][DEBUG]
```

```
->HlrSS7 main : Instantiating HlrSS7Mng
[Fri Dec 19 2008 16:36:31:106708][Slot:5][bHlrSS7Mgr.cc(46)][HlrServer(HLR_INFO)
][Tid:4115138240][DEBUG]
->HlrSS7Mgr::HlrSS7Mgr()
[Fri Dec 19 2008 16:36:31:132175][Slot:5][bHlrSS7Mgr.cc(57)][HlrServer(HLR_INFO)
][Tid:4115138240][DEBUG]
->HlrSS7Mgr::HlrSS7Mgr(): started data provider
```

Viewing Information About the Activation Status of the SS7 and SIGTRAN Links

The CONFIG window is used to display the SS7 configuration information. For a description of each of these configuration parameters, refer to the "CONFIG" section in the "SS7 entities" chapter of the *SDM System Configuration Reference Manual*.

Requirements: Log in to a WebCI session with a valid username and password.

1. From the main menu, navigate to **SS7 > CONFIG**

2. This will open a SS7 configuration window (as shown in the figure below) which displays the SS7 configuration information.

SS7 Configuration Window

Monitoring SS7 Links and Performing a Line Test

To help troubleshoot SS7 physical link problems, the following sequence of events should be followed to help isolate the cause.

1. Check the line status with the iphlinestat tool.
2. Test the line with the iphlinetest tool.
3. If a link is down, check step 1, the signalling link status, and configuration.
4. If a linkset is down, check steps 1, 2, the linkset status, and configuration.
5. If a Destination Point Code (DPC) is down, check steps 1, 2, and 3.

    The iphlinetest and iphlinestat are testing and monitoring tools to help troubleshoot SS7 physical line problems. Both utility tools are found in the following directory on a blade: */opt/iphwan/tools*

    To determine the device name, run the iphDumpCardList tool. This will display a list of detected devices with their type, serial number, and device node name.

    Log onto the blade desired (you must be part of the operation or admin User Group) and type:
    admin@t0s3 / # opt/iphwan/tools/iphDumpCardList

Line Status

Iphlinestat

The iphlinestat tool enables the user to view the status of the lines handled by a communications controller.

View the line status

To view the status of the lines handled by communications controller #2 (iph_wan_2), type:

admin@t0s3 / # /opt/iphwan/tools/iphlinestat /dev/iph_wan_2

To view the status of the lines handled by communications controller #0 (iph_wan_0) and communications controller #3 (iph_wan_3), type:

admin@t0s3 / # /opt/iphwan/tools/iphlinestat /dev/iph_wan_0 /dev/iph_wan_3

To view the status of the lines handled by all the communication controllers plugged in the host, type:

admin@t0s3 / # /opt/iphwan/tools/iphlinestat /dev/iph_wan_*

Information similar to the following will be shown:

Press **I** to get secondary information, **H** for help, and **Q** to quit.

```
------------------------------------------------------------------------
time      adapter          port loopback alarms                   errors
15:36:23 /dev/iph_wan_0  p0   none     LOS-- LOF-- AIS-- RAI-- BPV-- PCV-- CS--
15:36:23 /dev/iph_wan_0  p1   none     LOS++ LOF++ AIS-- RAI-- BPV-- PCV-- CS--
15:36:23 /dev/iph_wan_0  p2   none     LOS++ LOF++ AIS-- RAI-- BPV-- PCV-- CS--
15:36:23 /dev/iph_wan_0  p3   none     LOS++ LOF++ AIS-- RAI-- BPV-- PCV-- CS--
```

The description for the alarm states are given below.

Table 25: State definitions

State	Error	Description
loopback	Line	The signal restored to the source of the loopback command consists of the full signal.
	Payload	The signal restored to the source of the loopback command consists of the payload of the received signal (with bit sequence integrity maintained) and newly-generated ESF framing.
	None	The port is not in loopback mode.
Alarms	LOS	Loss Of Signal. No electrical signal is detected. Verify the line is plugged into the communications controller and into the network interface.
	LOF	Loss Of Frame. Frames are lost due to framing errors. The terminal is unable to synchronize on the DS1 signal.
	AIS	Alarm Indication Signal. A signal transmitted instead of the normal signal to maintain transmission continuity. This signal notifies the receiving equipment that a transmission interruption occurred either on the equipment creating the AIS signal or by the receiving equipment.
	RAI	Remote Alarm Indication. A signal transmitted in the outgoing direction when a terminal detects a loss of the incoming signal.
Errors	BPV	BiPolar Violation. A BPV error event for an AMI-coded signal is the occurrence of a pulse with the same polarity as the previous pulse.
	PCV	Path Code Violation. A PCV error event is a frame synchronization bit error (in D4 and E1-no CRC formats) or a CRC error in the ESF and E1-CRC formats.
	CS	Controlled Slip. A CS error results from the replication or deletion of the payload bits of the DS1 frame. A CS may occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.

Each time one of the above states changes on a line (i.e., if loop back state has changed or an alarm occurred or new errors were detected), a new line of text is displayed for that port. Alarms and errors occurrences are explained in the table below.

Table 26: Alarm Symbols

Symbol	Alarm	Error
- -	No alarm of that type has occurred.	No other errors of that type have occurred.

Symbol	Alarm	Error
- +	An alarm of that type has occurred.	Other errors of that type have occurred.
+ +	That alarm is always present for the line.	Other errors of that type have occurred.
+ -	The alarm has just disappeared.	No other errors of that type have occurred.

The secondary information that can be obtained by pressing **I**, provides detailed information such as:

1. Type: line type (`E1, T1,` ...).
2. CSU availability: indicates if a CSU facility data link is used or not.
3. Uptime: length of time interface has been on-line.
4. Unavailable Seconds: number of seconds during which the interface was unavailable.
5. Errored Seconds: number of seconds during which any of the following occurred: PCV, one or more LOFs, one or more CSs, or a detected AI defect).
6. Severely Errored Seconds: number of seconds during which one of the following occurred: 320 or more PCVs, one or more LOFs, or a detected AIS defect).

Line Test

Iphlinetest

Caution: The iphlinetest should be used only in case of trouble at installation time and only with Telco agreement.

This utility enables the user to test a line connected on any port of a communications controller by selecting one of the following:

1. **Loopback** mode: A transmission state in which the signal received by the port is returned to the sender.

   Use this mode when the remote end (i.e., the Telco) is testing your line. All information sent is returned to the remote end according to the following sub-configurations:

   a) **Line**loopback mode: Signal returned to the source of the loopback command contains the full signal with bit sequence integrity maintained, no change in framing, and no removal of bipolar violations.
   b) **Payload**loopback mode: Signal returned to the source of the loopback command contains the received signal's payload.

      This signal also includes newly generated ESF framing.

2. **Pseudo-Random Bit Sequences** test: Causes a port to generate and transmit Pseudo Random Bit sequences online, while it tries to synchronize on the received signal.

   This mode should only be used with Telco agreement. Remote equipment should also be set to loopback mode. As soon as this test is selected, this application notifies the user of the evolution of the test by displaying one of the following messages:

Table 27: Error messages

Message	Description
Not synchronized	Port is unable to recognize the sequence of bits it has sent.
X bits in error/sec	Port compares the received bit sequences with sent bit sequences. Each erroneous bit found is added and the sum is displayed every second.
No error	Receiving bit sequences completed; Port found no errors when comparing sent and received bit sequences.

Testing the line

To test the line plugged on port#0 (default port =0) of communications controller #2 (iph_wan_2), type:

admin@t0s3 / # /opt/iphwan/tools/iphlinetest /dev/iph_wan_2

To test the line plugged on port#1 of communication controller #0, type:

admin@t0s3 / # /opt/iphwan/tools/iphlinetest /dev/iph_wan_0 1

After tests have been completed and the application closed, the tested port is automatically restored to its operational mode in order to handle incoming and outgoing calls.

CLI Operations to Monitor SS7 Activity

The following operations can be used to monitor SS7 activity and status on the system.

1. View Active MTP2 Saps
   a) To display the active MTP2 Service Access Points, run the following operation.

      Command syntax:

      SS7[]:MTP2[] GetActiveMTP2Saps()

2. View Active MTP3 Links
   a) To display the active MTP3 Links, run the following operation.

      When the state = up it indicates the link is active.

   b) Command syntax:
   c) SS7[]:MTP3[]> GetActiveLinks()

3. View Active MTP3 LinkSets
   a) To display the active MTP3 Link Sets, run the following operation.
   b) Command syntax:
   c) SS7[]:MTP3[]> GetActiveLinkSets()

4. View Active MTP3 Saps

   a) To display the active MTP3 Service Access Points, run the following operation.

   b) Command syntax:

   c) SS7[]:MTP3[]> GetActiveMTP3Saps()

5. View Active SCCP NSaps

   a) To display the active SCCP Network Service Access Points, run the following operation.

   b) Command syntax:

   c) SS7[]:SCCP[]> GetActiveSccpNSaps()

6. View Active SCCP USaps

   a) To display the active SCCP User Service Access Points, run the following operation.

   b) Command syntax:

   c) SS7[]:SCCP[]> GetActiveSccpUSaps()

Monitoring the System Through SNMP

The Tekelec SDM provides the end user the capability to monitor the alarms and system behaviour using a standard Network Manager. Detailed SNMP information can be found in the "SNMP" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*.

UDP Port designation

SNMP requests from the Network Manager are sent to UDP port 161 of the Tekelec SNMP agent. The Tekelec SNMP agent will also send SNMP responses from UDP port 161 to the Network Manager.

Trap messages from the Tekelec SNMP agent are sent to UDP port 162 of the Network Manager.

Configure/Edit SNMP Server Host (Network Manager)

The configuration of the Tekelec SNMP agent can be edited and the SNMP trap hosts can be configured by the Network Operator, through the system's interfaces, such as the WebCI or CLI.

The following SNMP configuration parameters can be edited from the Shelf entity, through the CLI or WebCI:

• SnmpRwCommunity
• SnmpAgentPort
• SnmpHeartbeatEnabled
• SnmpHeartbeatTime

In addition to this, the Network Operator can configure SNMP trap hosts by executing the following operations through the CLI or WebCI:

• AddSnmpTrapConfig()
• RemoveSnmpTrapConfig()

Note: that by default no SNMP trap hosts are configured in the system.

Refer to *Viewing/Editing SNMP Configuration* of this document for instructions on how to view/edit the SNMP configuration parameters and on how to add/delete SNMP trap hosts from the WebCI. For detailed information on these parameters and their value range, refer to the "Shelf" and "SNMP trap host configuration" sections of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual*. For more information on the AddSnmpTrapConfig() and RemoveSnmpTrapConfig()

operations, refer to the "Shelf Operations" section of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual*.

MIB access

The Tekelec proprietary MIBs are shipped with every SDM system.

The MIBs can be accessed from the following directory: *blue/usr/local/snmp/share/snmp/mibs*

There are two MIB files:

```
TEKELEC-SMI-ROOT.txt
```

and

```
TEKELEC-SYS-MIB.txt
```

Synchronization

Requirement: a SNMP v3 user with user name, an MD5 password, and DES password. The user should have read/write access.

To synchronize the alarm information between the Tekelec alarm table and the Network Manager, access the Tekelec SNMP agent through the SNMP V3 user.

The Network Manager can initiate a synchronization request by issuing a SNMP SET with the following information:

Table 28: SNMP SET

SNMP SET information	Value
SNMP version	**v3**
User name	*(user_name)*
Authentication protocol	**MD5**
Authentication password	*(my_password1)*
Privacy protocol	**DES**
Privacy password	*(my_password2)*
OID name	**bsNmSynchroTrigger**
OID type	*(type)*
OID value	*(value)*

This request will trigger the Tekelec agent to retrieve all active alarms in the Alarm table. Any existing alarms in the Alarm table will be sent as traps to the Network Manager.

Network Manager Implementation

Implementation required at the Network Manager.

1. Define the parameters required for the SNMP V3 access (see previous **Synchronization** section).

2. Perform the synchronization request (see previous **Synchronization** section).

3. Build and update the alarm table.

   a) Use the Sequence ID as the unique key to determine duplicated, cleared, and acknowledged alarms.

   b) Remove the duplicated alarms from the alarm table.

   c) Remove the cleared alarms from the alarm table.

Chapter

6

Maintenance

Topics:

The chapter contains information used to perform maintenance on the Subscriber Data Management system.

Maintenance

Viewing System Resource Data

The purpose of this feature is to collect system resource data. This includes CPU, I/O and network usage. Two new files ,dstat and resourcemonit.pl, have been added under `/blue/bin`. Under `/etc/init.d/blue` , blue has been updated.

Running the System resource Data script

amount of disk space available on a blade should be monitored on a frequent basis. If the disk space capacity used is 60 percent or higher, it is recommended some files be deleted from the disk drive to free up space.

The df (disk free) command is used to display the amount of free disk space. The disk space used should be checked on all blades. To check the available disk space, perform the following steps:

1. Log into the blade using a valid Id and password.

2. Type: **df**

   Screen information similar to the one below will be displayed.

```
Filesystem            1K-blocks      Used Available Use% Mounted on
/dev/hda3             72690908   7271808  62465068  11% /
/dev/hda1               101089     14818     81052  16% /boot
```

Viewing the CPU and Memory Usage

The administrators of the system can keep track of which users and processes are consuming the most system resources at any given time. To do so, the system administrator can log in the system (please refer to *Accessing the System*) and execute the following command: top.

This command is a standard Unix command that produces a frequently-updated list of processes (refreshed every 5 seconds). The top command shows how much processing power and memory are being used, as well as other information about the running processes. The processes are ordered by amount CPU usage, with only the "top" CPU consumers shown.

Viewing System Resource Data

The purpose of this feature is to collect system resource data. This includes CPU, I/O and network usage. Two new files, dstat and resourcemonit.pl, have been added under `/blue/bin`. Under `/etc/init.d/blue` , blue has been updated.

When the service is started on the blade the script starts automatically by default and runs in the background. It can also be started and stopped manually.

To start a new script type "service blue start" at the command line. The script starts and uses the following component default values:

- **interval** is the number of seconds between each run. The default is 5.
- **nothres** is the bypass resource threshold checking. The default is threshold check. To ensure threshold checks take place do not enter a value in the script for nothres. If the value nothres is present in the script then threshold values are not checked.
- **outdir** is the name of the directory to save the output data. The default is /export/resource_monit.
- **ttl** is the time to live (the number of days) for the output log files. The default is 10 days.

To check if a script is running already use the ps command on resourcemonit.pl. Stop the script by typing "service blue stop" at the command line. Multiple instances of the script can run concurrently.

Running the System resource Data script manually

1. To run the script with values other than the default type the following:
   `/blue/bin/resourcemonit.pl -interval <integer> -nothres -outdir <string>`
   `-ttl <integer>`. Example: `/blue/bin/resourcemonit.pl -interval 10 -nothres`
   `-outdir /export/resource_monit -ttl 8`
2. To stop the script type the following at the system prompt: `pkill -KILL -f resourcemonit`

When the system resource monitoring script is run certain data is collected. A snapshot of the overall system utilization. Three samples are collected. A comparison is made between current usage and pre-defined thresholds. If a single threshold has been exceeded then the following resource data is collected: CPU usage using 'top', I/O usage using 'iostat' and network usage using 'dstat'.

Once the script is started it can take up to 6 seconds for data collection to take place. If the interval specified is 5 seconds then there is 11 seconds between each run.

The data that was gathered is stored in a directory name provided by the user. If the user does not provide a directory name then the default directory name is used: `export/resource_monit`. The filename of the data file is resource_data.txt. All the data collected during a day, 24 hour period, is stored in the same data file. At the end of the 24 hours the file is renamed to resource_data_<YYYYMMDD>.txt.

The data files are saved in the system for the number of days specified (ttl) when the script was started. If no ttl value is provided then the default value is used. It is important to set the ttl value carefully as the data file consumes disk space.

This is an example of a resource_data.txt file. It contains the following: Date and time, Top data, IOStat and Dstat data.

```
----- 2014-09-23 09:39:55 -----
--TOP--
top - 09:39:56 up 3 days, 21:43,  3 users,  load average: 0.03, 0.05, 0.07
Tasks: 261 total,   1 running, 260 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  49322868k total,  4239484k used, 45083384k free,   355816k buffers
Swap:        0k total,        0k used,        0k free,  3226960k cached
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      15   0 10364  692  580 S  0.0  0.0   0:02.89 init
    2 root      RT  -5     0    0    0 S  0.0  0.0   0:00.01 migration/0
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S  0.0  0.0   0:00.08 migration/1
    6 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/1
    7 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/1
    8 root      RT  -5     0    0    0 S  0.0  0.0   0:00.01 migration/2
    9 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/2
   10 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/2
   11 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/3
```

```
   12 root      34  19     0     0     0 S  0.0  0.0  0:00.00 ksoftirqd/3
   13 root      RT  -5     0     0     0 S  0.0  0.0  0:00.00 watchdog/3
   14 root      RT  -5     0     0     0 S  0.0  0.0  0:00.00 migration/4
   15 root      34  19     0     0     0 S  0.0  0.0  0:00.00 ksoftirqd/4
   16 root      RT  -5     0     0     0 S  0.0  0.0  0:00.00 watchdog/4
   17 root      RT  -5     0     0     0 S  0.0  0.0  0:00.00 migration/5
   18 root      34  19     0     0     0 S  0.0  0.0  0:00.00 ksoftirqd/5
top - 09:39:56 up 3 days, 21:43,  3 users,  load average: 0.03, 0.05, 0.07
Tasks: 261 total,   1 running, 260 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  49322868k total,  4239988k used, 45082880k free,   355816k buffers
Swap:        0k total,        0k used,        0k free,  3226960k cached
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      15   0 10364  692  580 S  0.0  0.0  0:02.89 init
    2 root      RT  -5     0    0    0 S  0.0  0.0  0:00.01 migration/0
    3 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S  0.0  0.0  0:00.08 migration/1
    6 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/1
    7 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/1
    8 root      RT  -5     0    0    0 S  0.0  0.0  0:00.01 migration/2
    9 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/2
   10 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/2
   11 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 migration/3
   12 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/3
   13 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/3
   14 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 migration/4
   15 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/4
   16 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/4
   17 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 migration/5
   18 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/5
top - 09:39:57 up 3 days, 21:43,  3 users,  load average: 0.03, 0.05, 0.07
Tasks: 261 total,   1 running, 260 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  49322868k total,  4239864k used, 45083004k free,   355816k buffers
Swap:        0k total,        0k used,        0k free,  3226964k cached
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      15   0 10364  692  580 S  0.0  0.0  0:02.89 init
    2 root      RT  -5     0    0    0 S  0.0  0.0  0:00.01 migration/0
    3 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S  0.0  0.0  0:00.08 migration/1
    6 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/1
    7 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/1
    8 root      RT  -5     0    0    0 S  0.0  0.0  0:00.01 migration/2
    9 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/2
   10 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/2
   11 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 migration/3
   12 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/3
   13 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/3
   14 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 migration/4
   15 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/4
   16 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 watchdog/4
   17 root      RT  -5     0    0    0 S  0.0  0.0  0:00.00 migration/5
   18 root      34  19     0    0    0 S  0.0  0.0  0:00.00 ksoftirqd/5
--IOSTAT--
Linux 2.6.18-308.11.1.el5prerel5.1.1_73.5.4 (SDM1-A)    23/09/14
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.03    0.04    0.01    0.00    0.00   99.91
Device:        rrqm/s   wrqm/s   r/s   w/s    rkB/s    wkB/s avgrq-sz avgqu-sz
   await  svctm  %util
cciss/c0d0       0.05     6.77  0.16  2.21     6.26    35.90    35.66     0.01
    4.42   0.23   0.05
cciss/c0d0p1     0.00     0.00  0.00  0.00     0.00     0.00     0.00     0.00
```

```
   1.96   1.64   0.00
cciss/c0d0p2      0.05      6.77 0.16 2.21      0.00      0.00      0.00      0.01
   4.42   0.23   0.05
dm-0              0.00      0.00 0.04 1.40      0.65      5.62      8.71      0.00
   0.31   0.04   0.01
dm-1              0.00      0.00 0.09 1.60      0.90      6.38      8.66      0.00
   0.46   0.15   0.02
dm-2              0.00      0.00 0.01 0.33      0.10      1.31      8.39      0.00
   0.48   0.16   0.01
dm-3              0.00      0.00 0.00 0.02      0.00      0.08      8.00      0.00
   0.38   0.08   0.00
dm-4              0.00      0.00 0.04 2.89      3.57     11.58     10.31      0.00
   0.53   0.07   0.02
dm-5              0.00      0.00 0.03 2.73      1.01     10.93      8.64      0.93
 338.26   0.04   0.01
avg-cpu:  %user   %nice %system %iowait   %steal    %idle
          0.00    0.00    0.00    0.00     0.00  100.00
Device:          rrqm/s   wrqm/s   r/s   w/s    rkB/s     wkB/s avgrq-sz avgqu-sz
   await  svctm  %util
cciss/c0d0        0.00      4.00 0.00 3.00      0.00     28.00     18.67      0.00
   0.00   0.00   0.00
cciss/c0d0p1      0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
cciss/c0d0p2      0.00      4.00 0.00 3.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-0              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-1              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-2              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-3              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-4              0.00      0.00 0.00 7.00      0.00     28.00      8.00      0.00
   0.00   0.00   0.00
dm-5              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
avg-cpu:  %user   %nice %system %iowait   %steal    %idle
          0.00    0.00    0.00    0.00     0.00  100.00
Device:          rrqm/s   wrqm/s   r/s   w/s    rkB/s     wkB/s avgrq-sz avgqu-sz
   await  svctm  %util
cciss/c0d0        0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
cciss/c0d0p1      0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
cciss/c0d0p2      0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-0              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-1              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-2              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-3              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-4              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00
dm-5              0.00      0.00 0.00 0.00      0.00      0.00      0.00      0.00
   0.00   0.00   0.00

--DSTAT--
^[[7l----system---- ----total-cpu-usage---- -dsk/total- ---procs--- -net/total-
 --io/total-
    time     |usr sys idl wai hiq siq| read  writ|run blk new| recv  send| read
```

```
  writ
23-09 09:39:59|  0   0 100   0   0   0|6407B   36k|0.0   0 0.7|   0     0 |0.31
  4.41
23-09 09:40:00|  0   0 100   0   0   0|  0     0 | 0   0 1.0| 204B    0 |   0
  0
23-09 09:40:01|  0   0 100   0   0   0|  0    460k| 0   0 2.0| 624B  170B|   0
  42.0
23-09 09:40:02|  0   0 100   0   0   0|  0     0 | 0   0   0| 204B    0 |   0
  0
```

This table displays SPR system resource threshold values with the maximum TPS:

Resource	Threshold Value
CPU idle	<50%
CPU I/O wait	>3%
Disk write	>50MB/s
Disk read	>2MB/s
Network transmit	>70MB/s
Network received	>70MB/s

Chapter

7

Troubleshooting

Topics:

This chapter contains information used to troubleshoot the Subscriber Data Management system.

What Is Troubleshooting?

Troubleshooting generally consists of the following:

1. Define the specific symptoms.

   a. What caused the problem?

2. Determine the cause of the symptoms by using various Troubleshooting tools and techniques.

3. Correct the problem.

4. Once the problem has been identified, fix it by implementing a series of actions.

Before you start Troubleshooting

During troubleshooting, it may be necessary to change some files (i.e., configuration files). Once troubleshooting has been completed, some changes may need to be undone. The process of restoring files is easier to do when the files are saved before troubleshooting has started.

The operator should consider each of the following:

1. Save the network configuration.
2. Save the log files.
   a) Log files are kept for a period of seven days.

      Logs generated by a troubleshooting session will eventually overwrite the logs that are stored.

3. Do not erase the log files unless they have been saved.
4. If there are going to be several troubleshooting sessions, consider saving the logs after each troubleshooting session (otherwise it may be overwritten by normal system activity logs).
5. When the troubleshooting session is finished, remember to restore the system to the state it was in before the troubleshooting session started.
6. If necessary, restore any configuration changes, restore any files that were changed, etc.
7. If special cabling was wired for troubleshooting (for example, for loopback tests), restore the cabling to its original state.

   Troubleshooting may affect system behavior

   Before beginning troubleshooting, consider the following:

   When it is necessary to troubleshoot on a live system, it is best to perform troubleshooting procedures when the traffic is low.

Troubleshooting Tools

The following section describes the tools that can be used to help troubleshoot problems on the system.

If the problem still exists after using these tools, please contact the Tekelec *My Oracle Support (MOS)* to help resolve the problem.

Troubleshooting Using Alarms

The system alarms can be used to determine the state of the system. The operator is able to:

1. View all active alarms
2. View details of specific alarm(s)
3. View alarm history
4. Acknowledge alarms
5. Clear alarms

View Active Alarms

To view active alarms on the system, type:

```
System[]>
display Alarm[]
```

View Alarm Details

To investigate details of a specific alarm, specify the SequenceId number and type:

```
System[]>display Alarm[SequenceId = 7]
```

Acknowledge Alarms

The acknowledge operation can be used to acknowledge a specific alarm. Note that it does not clear the conditions that raised the alarm. To acknowledge a specific alarm, enter the SequenceId number and type:

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

Clear Alarms

Caution: the operator must be careful with this operation.

CAUTION

Even though this clears all the alarms from the active alarm list, the conditions that caused these alarms still exist but will NOT be reported when these conditions no longer prevail.

The Acknowledge operation must be run first before running the Clear operation. To clear an alarm, specify the SequenceId number and type:

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

View Alarm History

To view the historical alarms type:

```
System[]>display AlarmHistory[]
```

Refer to *Viewing and Managing Alarms* for further details on how to view alarm information using the WebCI.

Each application running on the system raises alarm messages. These alarm messages can help for the troubleshooting of the system. For more information on each of these alarms, for a description of the effect they have on the system and for the recommended course of action to follow when they are raised, refer to the *SDM Alarm Dictionary*.

Troubleshooting with System Logs

The System logs can provide the operator with additional details on the symptoms on the system. 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*)
*
*   Requirement before viewing logs:

    The stored log files can be viewed by accessing the specific System Controller (SC) card. This means that since the logs are stored on the active and standby SystemController blade, the only way to view them is by accessing the files from the blade on which runs the SystemController service. Refer to *Viewing and Provisioning Services on Each Slot* to know on which blade runs the active SystemController service.

Viewing System Logs

To view system log messages, go to the log directory by typing:

```
admin@p0s2 # cd /blue/var/log
admin@p0s2 /blue/var/log # more current.xml
```

Viewing Stored System Logs

To view stored log files, list the files stored in the */blue/var/log directory* and type:

```
admin@p0s2 # cd /blue/var/log
admin@p0s2 /blue/var/log # more friday_20060616_115524
```

Understanding System Logs

The log messages generated provide information in the following format:

Table 29: Description of log fields

Item	Description	
Type	The type of system log	
Code	An error message identifier which is a unique value	
Category	module or event that generated the log	
Severity	Trace	indicates function calling sequence
	Debug	debugging information
	Info	information normally used when debugging a problem
	Notice	non-error conditions that may require special handling
	Warning	Warning
	Error	Error
	Alarm Warning	warning alarm
	Alarm Minor	minor alarm
	Alarm Major	major alarm
	Alarm Critical	critical alarm
eventType	Log or Trace	
Description	additional information describing the log event	
Timestamp	in GMT format (YYYY-MM-DDThh:mm:ss)	
Filename	module file name	
lineNumber	module file line number	
SequenceNumber	log sequence number generated by client application	
slotId	chassis slot where the event was generated	

Troubleshooting with Traces

The System traces can provide the operator with additional details on the symptoms of the system. Prior to using traces for troubleshooting, the Tekelec's *My Oracle Support (MOS)* must always be contacted. Tekelec technicians will be able to manage traces and analyse them properly to be able to debug the system.

Once you have contacted Tekelec's *My Oracle Support (MOS)*, a Tekelec Support Technician will perform all or some of the following operations:

- Access/View traces. See *Accessing Traces*.
- Save traces.
- Activate/Deactivate events of Trace level.
- Add/Remove Filter Component

The stored trace files can be viewed by accessing the blade on which runs the concerned application. This means that since the traces are stored locally, on the same blade on which runs the application that produced it, they cannot all be viewed at once under one single location. Only the traces produced by the applications running on a specific blade can be viewed when accessing the /blue/var/trace directory from that blade.

Refer to *Accessing Traces* for step-by-step instructions on how to access traces.

Performance Monitoring

The operator can also use Performance Monitoring counts to help view system activity and monitor system behavior. The operator is able to:

- View current PM counts
- View current PM historical

Refer to the *SDM Performance Measurements* document for a list of the different counters and for instructions on how to view these counters and modify some thresholds.

Restarting Processes

In the event it may be necessary to restart the software applications (i.e., after a power failure or to reboot the system), it is recommended to Stop the services on the system and once again Start them through the WebCI.

Stopping or starting applications, services, or slots

Applications, services, and slots can be stopped and started from the WebCI for troubleshooting purposes.

Applications

To stop an application, all the system services running the application must be stopped.

These services run the SDM applications:

- The Hlr service runs the HLR and SIP applications.
- The Hss service runs the HSS, SLF, AAA and DNS ENUM applications.
- The LteHss service runs the LTE HSS application.

Stopping these services will also stop the other applications that run on this service.

For example, to stop the AAA application on a slot, the HSS services on that slot must be stopped. Stopping the HSS services will then also stop the remaining applications such as HSS, SLF, and DNS ENUM.

After modifying the application, an application restart may be necessary.

Services

Each service can be stopped or started individually. In some situations, one single service or some specific services may need to be stopped or started. Stopping and restarting services may be required in the following cases:

- If the connections are down. For example, if the SS7 connections to an HLR service are down, that specific HLR service must be restarted. In this case, one single service needs to be stopped and may need to be started again later.
- After performing a restore of the database from a backup. In this case, all the services, except the CoreSystemController, Database and DataAccess services running on the slot on which the active Database service instance runs, must be stopped and then started. Each service of the slot must be stopped one at a time and then restarted again.

For a geo-redundant site where the VIP is to be modified, all the services running on a slot are stopped and then started again automatically.

Slots

To stop or start a slot, all services running on a slot must be stopped or started. Stopping and restarting a slot may be necessary when an SBC needs to be removed. Prior to removing the SBC, all services running on its slot must be stopped. Once the replacement SBC has been installed and configured, all the services on the slot can be started for the new SBC.

Note: When stopping slots, the front-end slots must be stopped before the back-end slots. When starting slots, the front-end slots must be started after at least one back-end slot is started.

Stop a service on a slot

Prerequisites:

The state of the service or all services must be at 'Started' prior to stop the service or all services.

1. Click the **System** folder.
2. Click **Shelf View**.
   The Shelf View window opens.

3. Perform one of these actions:

   - To stop all services, click the **Stop** button in the row of the slot identity.

     > ⚠️ **WARNING**
     > **Warning:** One slot with at least one service must remain running on the system. Stopping all services on the last slot will stop the system completely and no longer allow access to the system from the WebCI or CLI. Never stop all services on the last slot.

   - To stop an individual service, click the Plus symbol preceding the slot to view the individual services on the slot. Then click the **Stop** button of the service to be stopped.

   The service or services have stopped.

Start services on a slot

Prerequisites:

The state of the service or all services running on the slot must be in a **Stopped** state prior to starting the service or all services.

1. Click the **System** folder.
2. Click **Shelf View**.
   The Shelf View window opens.

3. Perform one of these actions:

   - To start all services, click the **Start** button in the row of the slot identity.

     Note: Use this option if all services on this slot need to be started. Do not attempt to start each service independently.

   - To start an individual service, click the Plus symbol preceding the slot to view the individual services on the slot. Then click the **Start** button of the service to be started.

⚠ WARNING

Warning: If a service is already running on a slot (i.e., CoreSystemController), starting the services on the slot will start the other services on the slot.

⚠ WARNING

Warning: If the **Stop** button was executed previously, wait 30 seconds before clicking the **Start** button.

The service or services have started.

Restart services on a slot

Prerequisites:

The state of the service or all services running on the slot must be in a **Started** state prior to restarting the service or all services.

1. Click the **System** folder.
2. Click **Shelf View**.
   The Shelf View window opens.

3. Perform one of these actions:

   • To restart all services, click the **Restart** button in the row of the slot identity.

     Note: Use this option if all services on this blade need to be restarted. Do not attempt to restart each service independently.

   • To restart an individual service, click the Plus symbol preceding the slot to view the individual services on the slot. Then click the **Start** button of the service to be restarted.

   ⚠ WARNING

   Warning: If a service is already running on a slot (i.e., CoreSystemController), starting the services on the slot will start the other services on the slot.

Warning: If the **Stop** button was executed previously, wait 30 seconds before clicking the **Start** button.

The service or services have restarted.

Start services on a System Controller blade

After a system start-up or a power failure it is possible to manually load data to memory on the active system controller blade. To do this these 2 steps must precede the steps in **Start services on a blade**.

Prerequisites:

The state of the service or all services running on the blade must be in a **Stopped** state prior to starting the service or all services.

1. At the command line type `service blue start` to access the SystemController blade.
2. Type `perl /blue/bin/load_db_tables_in_memory.pl localhost[username][password]` to run the script. After running the script :

   - Traffic can be run straight away. System capacity will not reach its full performance until all the data is loaded into memory.

   - Wait until all the data is loaded into memory and then run traffic at peak capacity. The system can handle traffic at its rated capacity at this point.

Remote Log In

When terminating a remote log in session, the session window may hang occasionally. This may occur after restarting a slot through a remote log in session.

Workaround: The session can be recovered by entering "`~.`".

Troubleshooting the System

Viewing the Software Version of the System

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.

Viewing the System's Host Name

Definition

The system host name should be configured according to the following definition:**xxxxxxxxxxxN1sN2** where **xxxxxxxxxx** can be any combination of characters. There is no maximum of characters but it must start with a letter.

The name must end with two numbers separated by the letter "**s**" e.g., **N1sN2**. Both numbers must be ≥ 1 and each number can be a maximum of 2 digits.

Generally, the first number, N1, refers to the System ID and the second number, N2, refers to the Slot Id.

Example.

```
TEKELEC_CA_HLR1s10
TEKELEC_CA_HLR99s5
```

Active Status

Active Host Name

To retrieve the name of the active host on the shelf, run the following operation by typing:

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

Viewing/Modifying the Information for a Geo-Redundant System

The Geo-Redundant feature can be provisioned through the WebCI.

With the SDM system running in a Geo-Redundant deployment, the OAMP Virtual IP address of the peer site and the state of the Geo-Redundant feature become important information to know.

The following procedures allow the administrator of the system, as well as users part of the Admin Group and Operation Group, to display and modify from the WebCI the Geo-Redundant configuration data.

The following information can be displayed:

- Enabled status of the Geo-Redundancy feature
- Local/Remote Virtual IP address of the geo-redundant sites
- Local Site Netmask
- Local/Remote Ports of the geo-redundant sites
- Activation status of the Geo-Redundancy deployment (started/stopped)

    The following information can be modified:

- Local/Remote Virtual IP address of the geo-redundant sites
- Local Site Netmask

Display Geo Redundancy View with WebCI

This procedure describes how to display the Geo Redundancy screen using the WebCI.

Open the System folder by clicking on it.
a) Click on **Geo Redundancy View**.
b) The Geo Redundancy screen will be displayed as shown below.
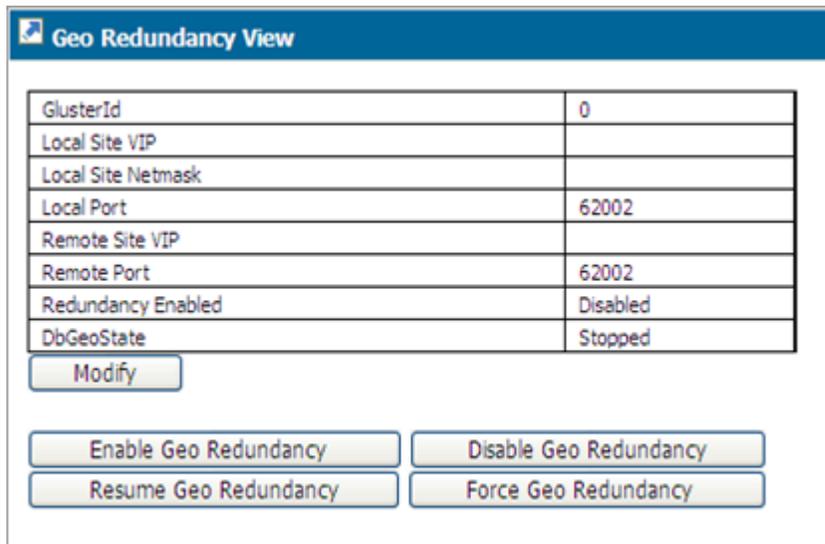
Figure 46: Geo Redundancy View

Modify the Geo Redundancy Information with WebCI

This procedure describes the steps to modify the Geo-Redundant configuration data.

1. Open the **System** folder by clicking it.
2. Click on **Geo Redundancy View**.
3. The Geo Redundancy window appears (as per *Figure 46: Geo Redundancy View*).
4. Click the **Modify** button.
5. When the Geo Redundancy Attributes window appears, enter the new values.
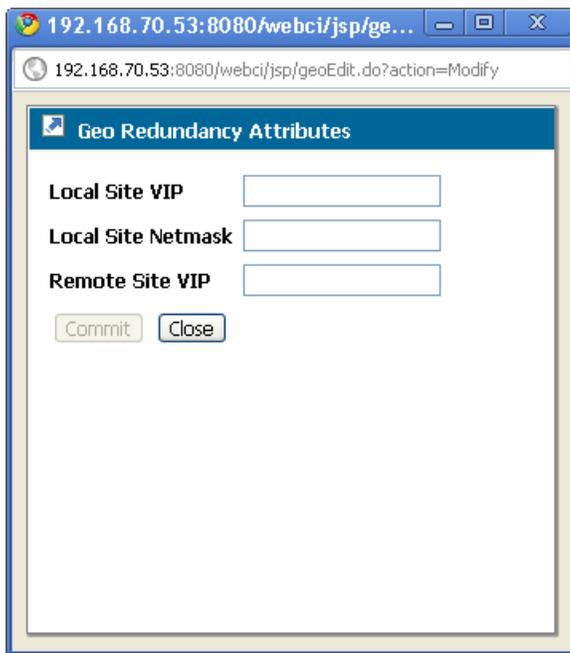
Figure 47: Geo Redundancy Attributes Screen

6. Click **Commit**.

7. When the confirmation message **"Entity entry was successfully committed"** appears, click **OK**.

   The WebCI's Geo-Redundancy View also allows to perform the following operations:

   a) Enable/Disable Geo Redundancy
   b) Resume Geo Redundancy
   c) Force Geo Redundancy

Enable/Disable the Geo Redundant Information with WebCI

This procedure describes the steps to enable/disable the Geo-redundant feature.

1. Open the **System** folder by clicking it.
2. Click on **Geo Redundancy View**.
3. The Geo Redundancy window appears (as per *Figure 46: Geo Redundancy View*).
4. Click the **Enable Geo Redundancy** button if the feature is disabled and you wish to enable it.
5. Click the **Disable Geo Redundancy** button if the feature is enabled and you wish to disable it.

   WARNING: The Geo-redundancy should never be disabled on both sites (ReferenceProtected and Replica). If it is done, one of the two sites will have to be completely shut down and restarted to recover geo-redundancy. In this case, contact Tekelec's *My Oracle Support (MOS)* in order to restart and recover geo-redundancy.

Resume Geo-Redundancy with WebCI

This procedure describes the steps to resume the synchronization process when it is in an unassigned state. Performing this operation forces the synchronization process to reenter the negotiating phase in order to identify which site has the reference database and which site has the replica database.

Requirement: The Geo-Redundancy feature must be enabled. Geo-Redundancy has not been disabled for more than 4 hours and DbGeoState must be unassigned and enabled. Tekelec support personnel must be contacted to resume Geo-Redundancy on a system where it was disabled for more than 4 hours.

1. Open the **System** folder by clicking it.
2. Click on **Geo Redundancy View**.
3. The Geo Redundancy window appears (as per *Figure 46: Geo Redundancy View*).
4. Click the **Resume Geo Redundancy** button.

Force the Geo Reference with WebCI

This procedure describes the steps to force the database to change from the PendingReference state to the Reference state, after which the database changed in the case where the connection between the two sites was lost, either due to the physical connection or the operational state of the other site.

Requirement: The Geo-Redundancy feature must be enabled and DbGeoState must be PendingReference.

1. Open the **System folder** by clicking it.
2. Click on **Geo Redundancy View**.
3. The Geo Redundancy window appears (as per *Figure 46: Geo Redundancy View*).
4. Click the **Force Geo Reference** button.

Viewing/Provisioning the System Shelf and Slots

This procedure describes how to display from the WebCI the configuration of the Shelf and of each of its slots.

The Shelf View displays all the slots on the system and the services running on each one and their status. It also provides in the form of buttons all the operations that might be necessary when troubleshooting the system. Please contact Tekelec's *My Oracle Support (MOS)* prior to executing these operations as they may impact the health of the system.

For further information on starting/stopping services, refer to *Stopping or starting applications, services, or slots*.

You will notice that the operational state of the slots is color coded as per the following legend:

Table 30: Operational Status Colors

Color	Operational status
Green	The shelf/slot/service are up and running.

Color	Operational status
Orange	The shelf/slot has some services that are not running.
Red	The shelf/slot/service is not running.
Grey	The slot doesn't have an identity bind to it. No processes are running on that slot.

1. Open the **System** folder by clicking on it.
2. Click on **Shelf View**.
   a) The Shelf View screen will be displayed as shown below.
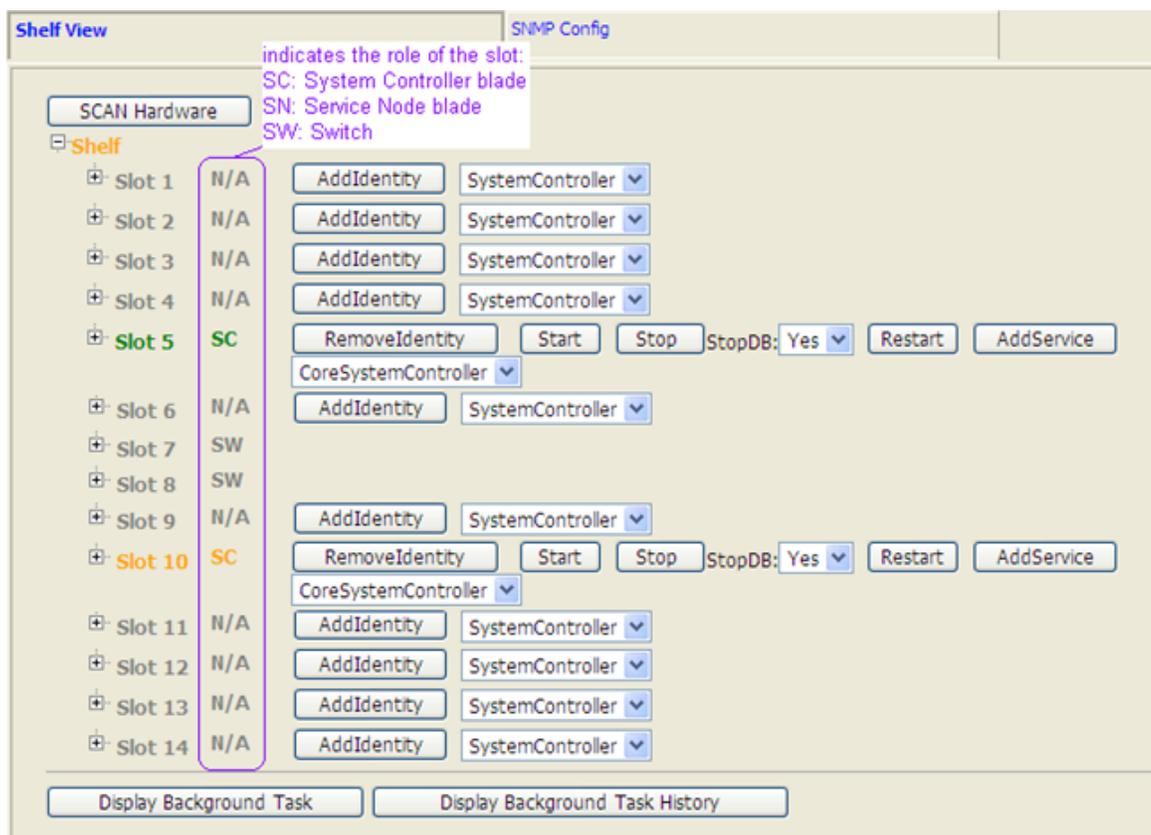
   Figure 48: Shelf View

3. Click on the **symbol** preceding the item for which you wish to see further information.
4. Click on the **Display Background Task or Display Background Task History** button to display the Background tasks currently in progress or all the Background tasks that have taken place on the system in a previous time (history of all Background tasks).
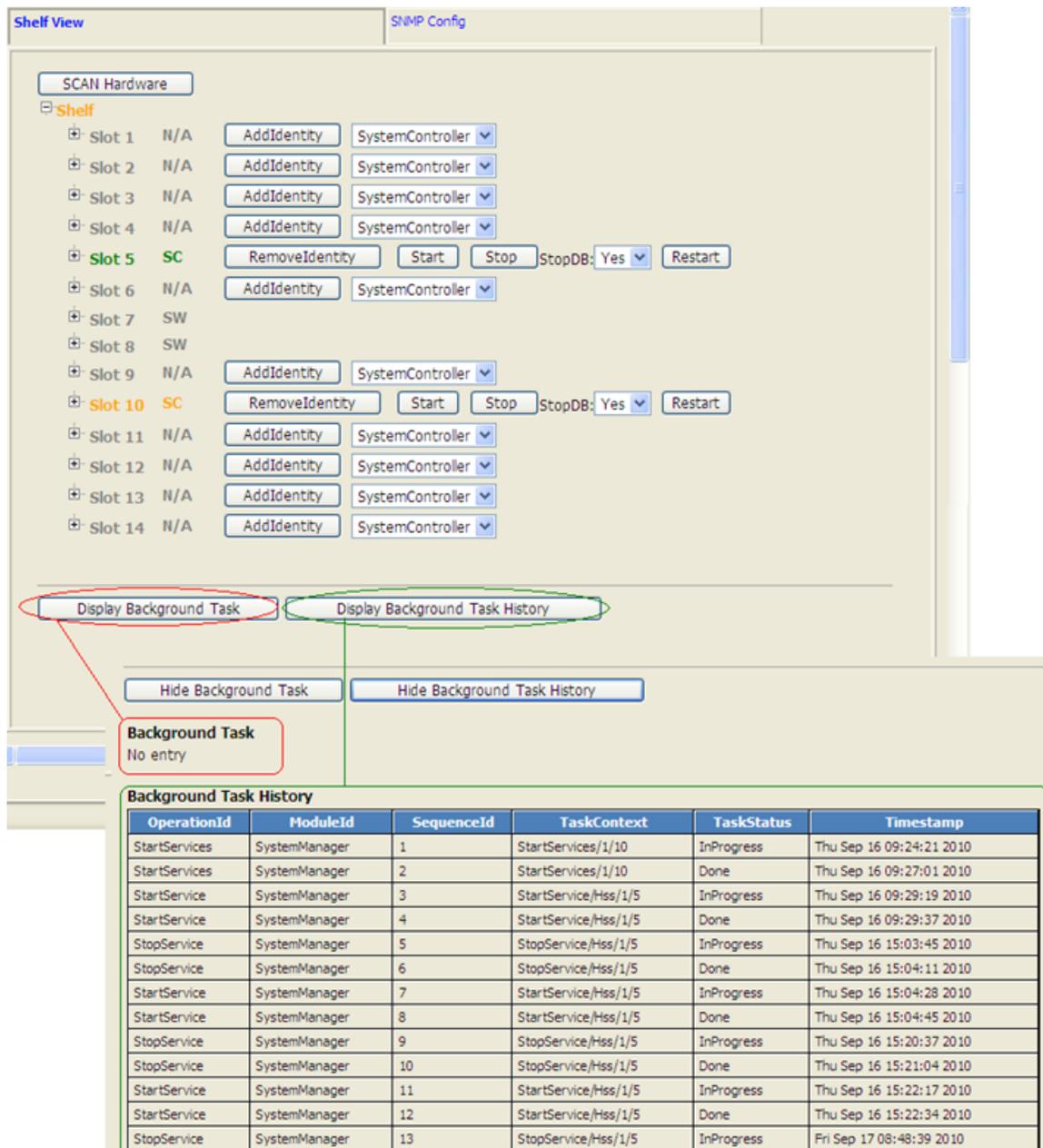
Figure 49: Displaying Background Tasks

5. In order to hide those tables, simply click on the **Hide Background Task** or **Hide Background Task History** button.

Viewing/Editing SNMP Configuration

The following configuration information for the Tekelec SNMP Agent can be displayed/edited via the WebCI, by accessing the Shelf View window's SNMP Config tab:

- SnmpAgentPort
- SnmpRwCommunity
- SnmpHeartbeatEnabled
- SnmpHeartbeatTime

The WebCI's SNMP Config window also allows to configure dynamically single/multiple SNMP trap host(s), by provisioning the lower table. Updates made through this table will automatically update the SNMP Agent configuration.
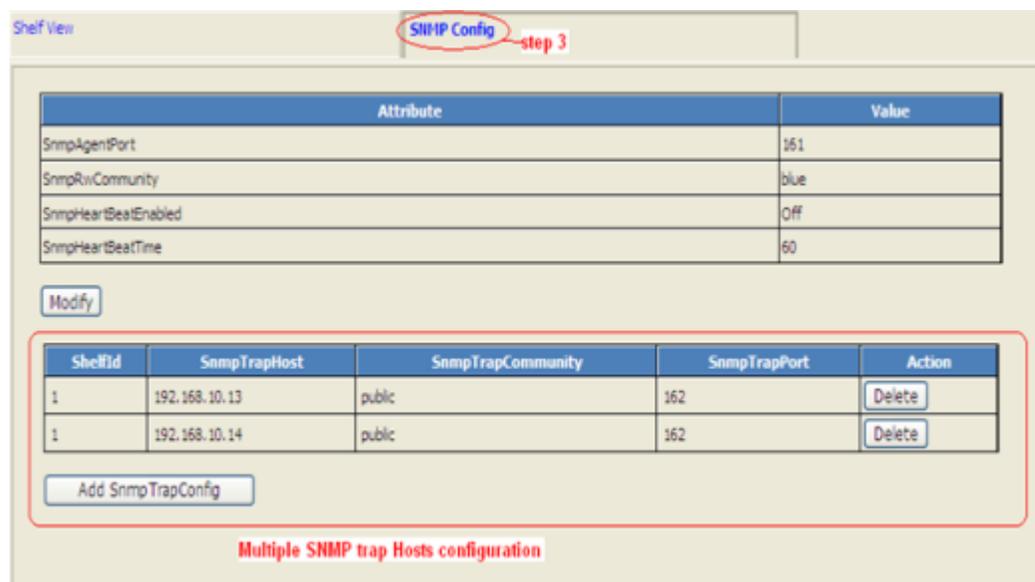
Figure 50: Displaying/editing SNMP configuration data and configuring SNMP trap hosts

Viewing and Provisioning Services on Each Slot

The System folder in the WebCI's menu can be expanded to provide access to the Service Management window, which displays information about the services running on the system and allows to perform operations on a per service basis.

Viewing Information for the Services Running on the System

In the Service Management window, all the services supported by the system are listed.

You will notice that the operational state of the services is color coded as per the following legend:

Table 31: Operation Status Colors

Color	Operational status
Green	The shelf/slot/service are up and running.
Orange	The shelf/slot has some services that are not running.
Red	The shelf/slot/service is not running.

Grey	The slot doesn't have an identity bind to it. No processes are running on that slot.

For each service, the following information can be displayed:

- The slot ID and state on which runs the service by clicking on the symbol preceding the slot.
- Each module (process) running within the service and its status by clicking on the symbol preceding the service:
- Resource State
- OpState (enabled, disabled)
- Slot Id
- HA Role (active, standby, unassigned)
- AdminState (locked, unlocked)
- The Service Option: WebServiceSecurity can be displayed by clicking on the **Option** button.
- The Service Instance Option can be displayed by clicking on the **ServiceInstanceOption** button. This displays the Service ID, Slot ID and Shelf ID on which the service runs. Moreover, for the HLR service, you can view which protocol is used with SS7 (MTP2, SAAL, SIGTRAN).

Provisioning New Services on a Slot

The Service Management window also allows you to provision new services on a specific slot, by displaying the following buttons for each service:

- Add
- Remove

   Please contact the Tekelec *My Oracle Support (MOS)* for assistance prior to performing these operations, which can impact traffic.

   Services can be started/stopped from this window as well. Refer to the next section for more details on these operations.

   Take note that the ServiceOption button also allows to enable/disable the Web Service Security in order to use the HTTPS protocol (port 8443) to access a secure web server or use the HTTP protocol (port 8080) to access the WebCI.

   The figure hereunder displays the Service Management window and circles where to find the different information described in this section as well as the operations that allow to provision new services.
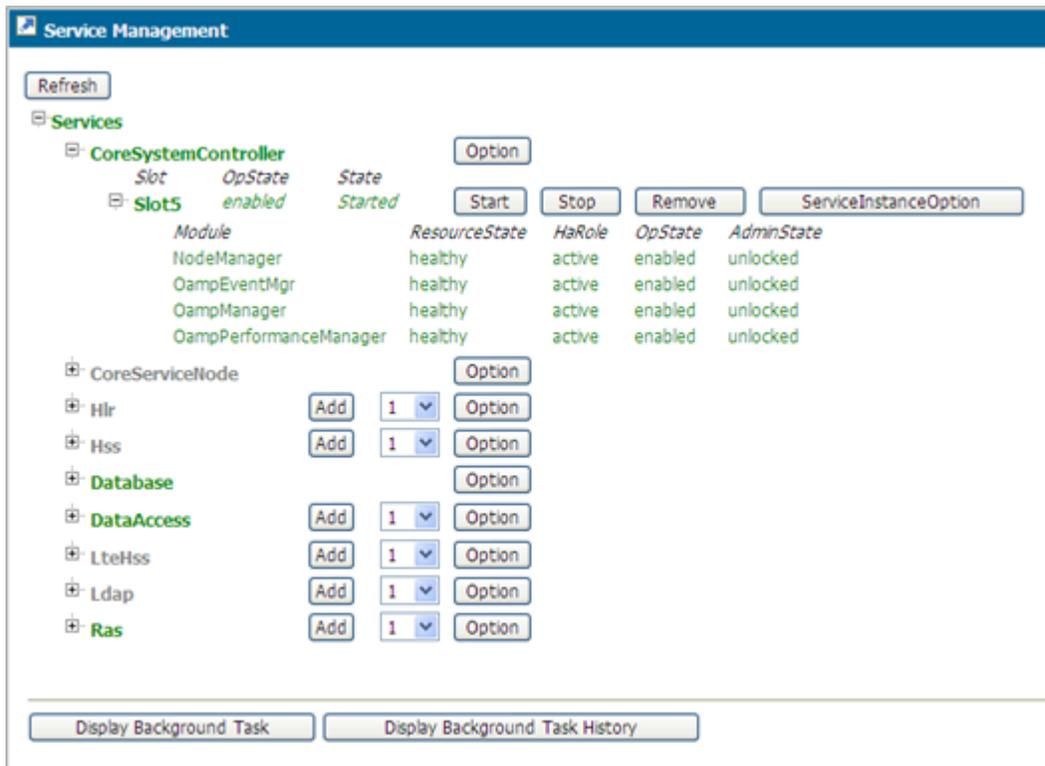
Figure 51: Service Management Window

Configuring the RAS server (XML-REST interface)

In order to be able to provision into the SPR the policy profiles and their user profile data using the XML-REST interface, the RAS Server must be configured properly. The latter can be configured from the WebCI's Service Management window, as follows:

☞   **Important:** The Ras server must be configured/modified at installation/reboot of the system. The configuration data cannot be changed during running-time of the system, the services must be stopped and the system must be rebooted afterwards. We strongly recommend you contact Tekelec's Customer Support Team if you wish any changes to be made to the Ras server.

Prerequisite: The Policy Schema must be loaded into the system prior to being able to add the Ras service. Contact Tekelec's Technical Support Team to achieve this.

1. Open the **System** folder by clicking on it.

   This will display the list of window names that can be accessed from this folder.

2. Click on the **Service Management** window name to display the window.

   The Service Management window will be displayed as shown below.

3. Click the **Option** button next to the Ras service.

   This will display the Service Option window. Enter all the necessary information. For more details on the fields and their value format, refer to the "Service Option" section of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual*.

4. Click the **Update** button to commit all the changes.

5. Click the **Close** button to close the window.
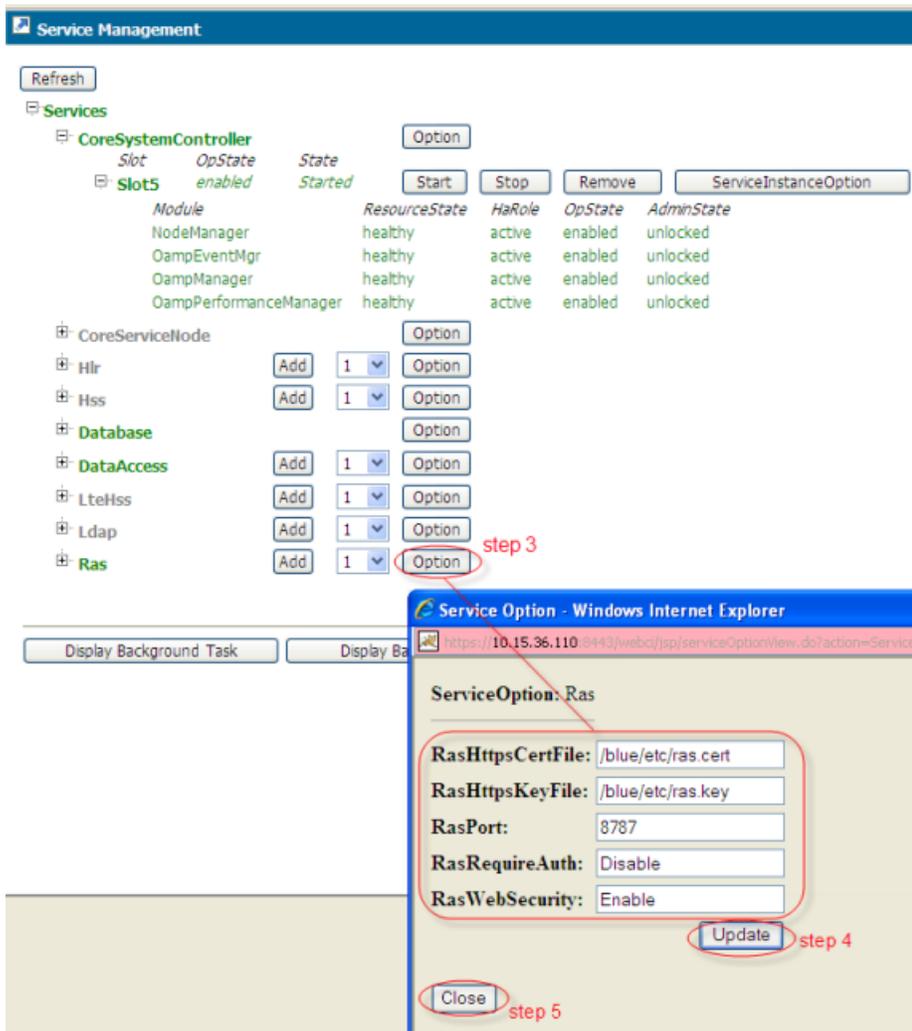
Figure 52: RAS Server Configuration

Stopping or starting applications, services, or slots

Applications, services, and slots can be stopped and started from the WebCI for troubleshooting purposes.

Applications

To stop an application, all the system services running the application must be stopped.

These services run the SDM applications:

- The Hlr service runs the HLR and SIP applications.
- The Hss service runs the HSS, SLF, AAA and DNS ENUM applications.
- The LteHss service runs the LTE HSS application.

Stopping these services will also stop the other applications that run on this service.

For example, to stop the AAA application on a slot, the HSS services on that slot must be stopped. Stopping the HSS services will then also stop the remaining applications such as HSS, SLF, and DNS ENUM.

After modifying the application, an application restart may be necessary.

Services

Each service can be stopped or started individually. In some situations, one single service or some specific services may need to be stopped or started. Stopping and restarting services may be required in the following cases:

- If the connections are down. For example, if the SS7 connections to an HLR service are down, that specific HLR service must be restarted. In this case, one single service needs to be stopped and may need to be started again later.
- After performing a restore of the database from a backup. In this case, all the services, except the CoreSystemController, Database and DataAccess services running on the slot on which the active Database service instance runs, must be stopped and then started. Each service of the slot must be stopped one at a time and then restarted again.

For a geo-redundant site where the VIP is to be modified, all the services running on a slot are stopped and then started again automatically.

Slots

To stop or start a slot, all services running on a slot must be stopped or started. Stopping and restarting a slot may be necessary when an SBC needs to be removed. Prior to removing the SBC, all services running on its slot must be stopped. Once the replacement SBC has been installed and configured, all the services on the slot can be started for the new SBC.

Note: When stopping slots, the front-end slots must be stopped before the back-end slots. When starting slots, the front-end slots must be started after at least one back-end slot is started.

Stop a service on a slot

Prerequisites:

The state of the service or all services must be at 'Started' prior to stop the service or all services.

1. Click the **System** folder.
2. Click **Shelf View**.
   The Shelf View window opens.

3. Perform one of these actions:

   - To stop all services, click the **Stop** button in the row of the slot identity.

     ⚠ **WARNING** **Warning:** One slot with at least one service must remain running on the system. Stopping all services on the last slot will stop the system completely and no longer allow access to the system from the WebCI or CLI. Never stop all services on the last slot.

   - To stop an individual service, click the Plus symbol preceding the slot to view the individual services on the slot. Then click the **Stop** button of the service to be stopped.

   The service or services have stopped.

Start services on a slot

Prerequisites:

The state of the service or all services running on the slot must be in a **Stopped** state prior to starting the service or all services.

1. Click the **System** folder.
2. Click **Shelf View**.
   The Shelf View window opens.

3. Perform one of these actions:

    • To start all services, click the **Start** button in the row of the slot identity.

        Note: Use this option if all services on this slot need to be started. Do not attempt to start each service independently.

    • To start an individual service, click the Plus symbol preceding the slot to view the individual services on the slot. Then click the **Start** button of the service to be started.

        Warning: If a service is already running on a slot (i.e., CoreSystemController), starting the services on the slot will start the other services on the slot.

        Warning: If the **Stop** button was executed previously, wait 30 seconds before clicking the **Start** button.

    The service or services have started.

Restart services on a slot

Prerequisites:

The state of the service or all services running on the slot must be in a **Started** state prior to restarting the service or all services.

1. Click the **System** folder.
2. Click **Shelf View**.
    The Shelf View window opens.

3. Perform one of these actions:

   • To restart all services, click the **Restart** button in the row of the slot identity.

      Note: Use this option if all services on this blade need to be restarted. Do not attempt to restart each service independently.

   • To restart an individual service, click the Plus symbol preceding the slot to view the individual services on the slot. Then click the **Start** button of the service to be restarted.

   Warning: If a service is already running on a slot (i.e., CoreSystemController), starting the services on the slot will start the other services on the slot.

   Warning: If the **Stop** button was executed previously, wait 30 seconds before clicking the **Start** button.

   The service or services have restarted.

Stop/Start One Single Service on a Blade

This procedure describes the steps to stop/start a specific service on a blade using the WebCI.

Prerequisite: The state of the service you wish to stop must be 'Started' prior to being able to stop it. The state of the service you wish to start must be 'Stopped' prior to being able to start it.

WARNING: If the Stop Service button was executed previously, a delay of 30 seconds must be taken into account before clicking on the Start Service button. The state of the service must be at 'Stopped' prior to being able to start the service.

1. Open the **System** folder by clicking on it.
2. Click on **Service Management**.

   The Service Management screen will appear, as shown below.

3. Click on the **symbol** preceding the service you wish to stop/start.
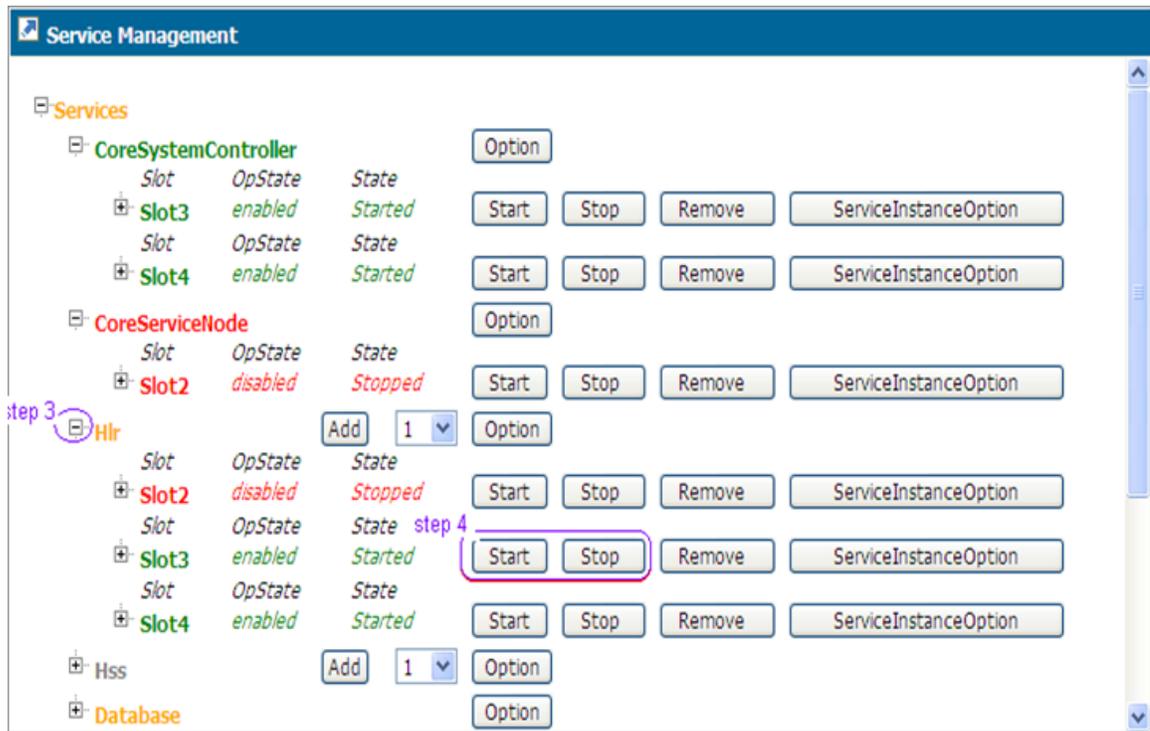
Figure 53: Service Management Screen

4. Click on the **Stop** or **Start** button located in the same row as the slot on which runs the service instance you wish to stop/start.

   In the example shown above, the Hlr service instance running on slot 3 will be stopped (if the Stop button is executed) or started (if the Start button is executed).

5. The following warning will appear:

```
This operation may be service affecting, Continue?
```

6. Click **OK** if you wish to Continue and **Stop** the service or **Cancel** if you don't.
7. You can verify that the service has been stopped by verifying the value of the State parameter of that service.

Creating a Backup of the System

Manual Backup

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
- Configuration
- 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 32: Manual Backup

Database file	Operation	Backup file extension	
All databases	Backup()	all.tar	
Subscribers	Backup()	Subscription.tar	
Configuration	Backup()	Configuration.tar	
Alarms	Backup()	bluealm.tar	
OamConfiguration	Backup()	blueoam.tar	
HlrConfiguration	Backup()	bluehlr.tar	
HssConfiguration	Backup()	bluehss.tar	

To manually initiate a backup, you must first access the system by entering a valid user ID and password to the System Controller (SC) (Please refer to *System login*) and subsequent procedures. Note that only users part of the Admin Group and Operation Group can perform a backup.

Perform Manual Backup of Database with WebCI

This procedure describes the steps to perform a database backup from the WebCI. For details on the database backup attributes, refer to section 4.2 "Database operations" in the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual.*

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

1. Open the **Database** folder by clicking it.
2. Click on **Backup/Restore/DRM**
3. The Backup/Restore window appears (as follows) displaying the backup view.
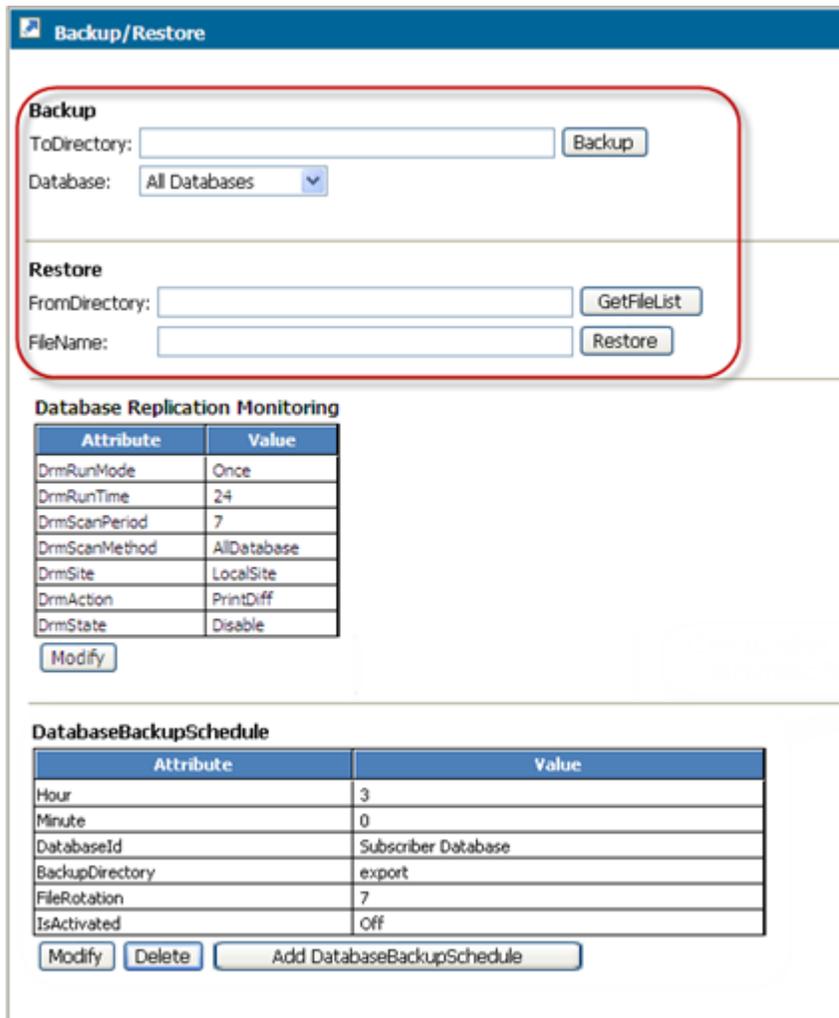
Figure 54: Backup/Restore Window

4. In the ToDirectory box, specify the directory (i.e., */export/backup*) to store the backup file.
5. In the Database box, select the segment of the database you wish to do a backup of: All databases, Subscribers, Configuration, alarms, OamConfiguration, HlrConfiguration, HssConfiguration.
6. Click on **Backup**.

   The following message will be displayed:

   ```
   asynchronous event currently executing.
   ```

7. Verify the backup has been completed by clicking on **System**
8. Click on **History Alarm View**
9. The Backup procedure is completed when the following message appears:

   ```
   Backup completed successfully
   ```

.

Automatic Backup

The following types of backup can be performed automatically on the active System Controller:

• a backup of all the subscriber profiles and of all the configuration data

  or

• a backup of all the subscriber profiles

  No automatic backups are executed by default, this function must be activated in order to start automatic backups. The operator can set a DatabaseBackupSchedule through the WebCI, which allows automatic backups to be executed at the time specified by the operator. In an automatic backup, a maximum of 10 files are 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. An automatic backup of Subscriber Profiles will be performed every time it has been scheduled to do so. When setting the schedule of the automatic backup, the IncludeConfiguration parameter can be set optionally to '1' in the case where you wish the automatic backup to back up all the configuration data in addition to all the subscriber profiles. By default, the IncludeConfiguration parameter is set to '0' and the automatic backup only backs up the subscriber profiles data.

  The following procedures show how to set a backup schedule and activate the automatic backup through the WebCI.

  First, you must access the system by entering a valid user ID and password to the System Controller (SC) and then you can follow the procedures below. (Please refer to *System login*).

  Note: Only users part of the Admin Group and Operation Group can set and activate an automatic backup.

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

Add Automatic Backup of Database with WebCI

This procedure describes the steps to add an automatic database backup from the WebCI. For details on the database backup attributes, refer to section 4.2 "Database operations" in the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual.*

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

1. Open the **Database** folder by clicking it.
2. Click on **Backup/Restore/DRM**. The Backup/Restore window will appear (as shown below).
3. Under DatabaseBackupSchedule, click the **Add DatabaseBackupSchedule** button.
4. When the DatabaseBackupSchedule Provisioning window appears, enter all the information. Note that the IncludeConfiguration parameter is optional and by default it is set to '0', which means that the automatic backup only backs up all the subscriber profiles data.
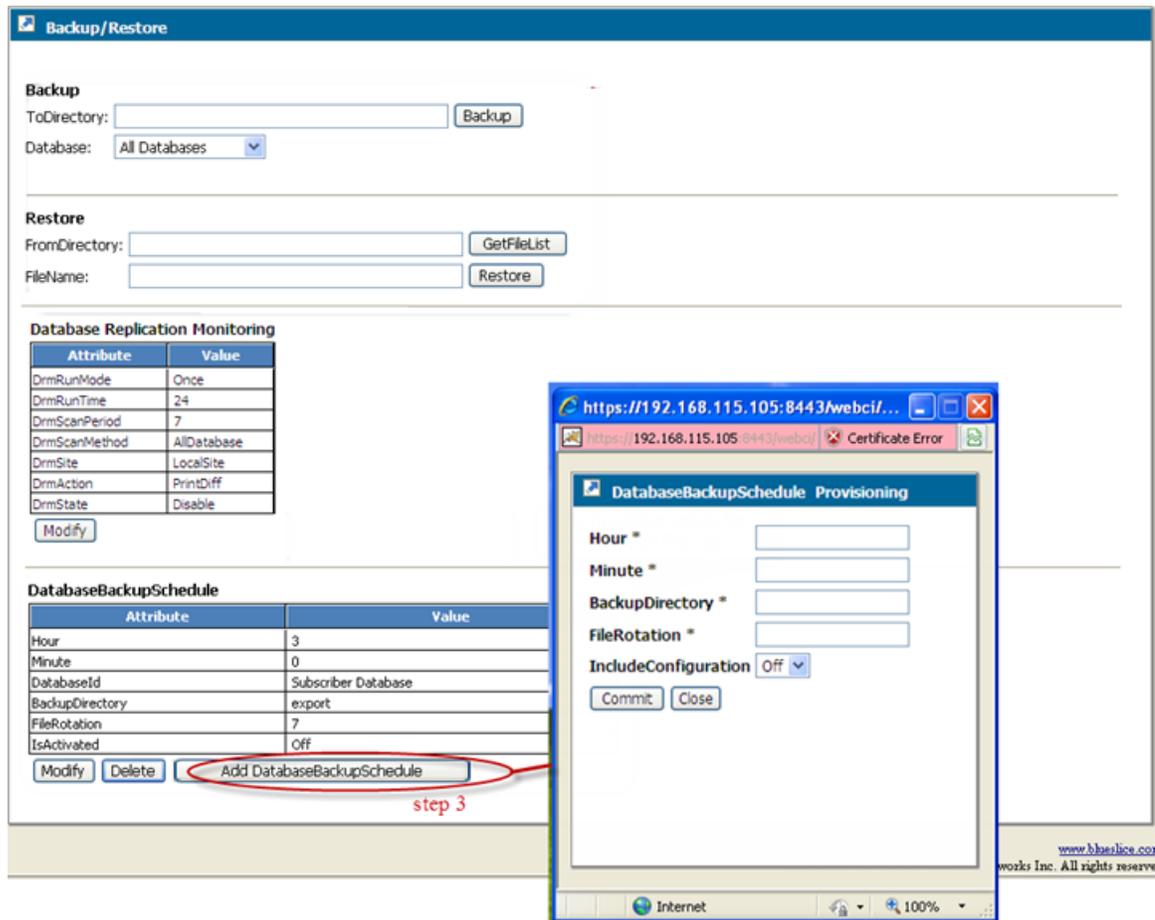
Figure 55: DatabaseBackupSchedule Provisioning Window

5. Click **Commit**.

6. When the confirmation message (**Entity entry was successfully committed**) appears, click **OK**.

Modify the Automatic Database Backup with WebCI

Modify an automatic database backup from the WebCI. For details on the database backup attributes, refer to section 4.2 "Database operations" in the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*.

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

CAUTION

1. Open the **Database** folder by clicking it.

2. Click on **Backup/Restore/DRM**.

3. The Backup/Restore window appears (as per *Figure 53: Service Management Screen*).

4. Under the DatabaseBackupSchedule table, click the **Modify** button.

5. When the DatabaseBackupSchedule Provisioning window appears, enter the new values of the parameters you wish to modify.

6. Click **Commit**.

7. When the confirmation message (**Entity entry was successfully committed**) appears, click **OK**.

Display the DatabaseBackupSchedule Entity with WebCI

This procedure describes the steps to display the automatic database backup information in the WebCI. For details on the database backup attributes, refer to section 4.2 "Database operations" in the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual.*

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

1. Open the **Database** folder by clicking it.

2. Click on **Backup/Restore/DRM**.

3. The DatabaseBackupSchedule entity will be displayed in the Backup/Restore window (as per *Figure 53: Service Management Screen*).

Activate and Disable the Automatic Backup with WebCI

This Procedure Describes The Steps To Activate And Disable The Automatic Database Backup In The WebCI For Details On The Database Backup Attributes, Refer To Section 42 "Database Operations" In The *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*

Caution: The Backup Operation Impacts The Performance Of The System Hence, The Backup Operation Must Be Done Only During Low Traffic Periods

1. Open the **Database** folder by clicking it.

2. Click on **Backup/Restore/DRM**.

3. The DatabaseBackupSchedule entity will be displayed in the Backup/Restore window (as per *Figure 53: Service Management Screen*).

4. Click on the **Activate** button to activate the automatic backup already set.

   (Before activating an automatic backup, you must set it. To do so, refer to procedure 7-19 Add Automatic Backup of Database with WebCI. By default, the automatic backup is not activated.

   a) If the automatic backup is activated, the attribute IsActivated will be On and the Activate button will not exist.

   In that case, there will be a `Disable` button that you can click on to deactivate the automatic backup.

Delete the Automatic Database Backup with WebCI

This Procedure Describes The Steps To Delete An Automatic Database Backup From The WebCI For Details On The Database Backup Attributes, Refer To Section 4.2 "Database Operations" In The *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*

Caution: The Backup Operation Impacts The Performance Of The System Hence, The Backup Operation Must Be Done Only During Low Traffic Periods

1. Open the **Database** folder by clicking it.

2. Click on **Backup/Restore/DRM**.

3. The Backup/Restore window appears (as per *Figure 53: Service Management Screen*).

4. Under the DatabaseBackupSchedule table, click the **Delete** button.

5. Click **Commit**.

6. When the delete confirmation window appears "

```
You are about to delete this DatabaseBackupSchedule entry, Continue?
```

   "

7. Click **OK**.

Restoring the database from a backup

This procedure describes the steps to perform a database restore from the WebCI.

The database information will be restored onto the active System Controller (SC) blade.

Caution: When restoring the database, on the active System Controller blade, all the services running on the system must be stopped except the active CoreSystemController, DataAccess and active Database services running on the active System Controller blade. In the case where the active CoreSystemController service instance is not running on the same blade as the active Database service instance, you must perform a manual switchover (see *Performing a manual switchover*) of the CoreSystemController service. This will make sure that the active CoreSystemController and the active database are running on the same blade, the active System Controller blade.

Note: 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 *Resume Geo-Redundancy with WebCI* for more information on Geo-Redundancy management.

To stop all services through WebCI, please follow these steps for each slot on the system except for the active System Controller slot:

1. In the WebCI, click on the **System** Folder.

2. Click on the **Shelf View**.

3. Click on the **symbol** preceding the slot on which you wish to stop all services.

4. Click on the **symbol** preceding the services which you wish to stop.

5. Click the **Stop** button located in the same row as the Slot ID.

   This will stop all the services on the slot.

   For the active System Controller slot, individually stop all the services on the blade except the active CoreSystemController service instance, the active Database service instance and the DataAccess service. Refer to *Stop/Start One Single Service on a Blade*.

Restoring the database

This procedure describes how to restore all segments of the database or only one of the following database segments from the WebCI:

• Subscribers

• Configuration

- Alarms

- OamConfiguration

- HlrConfiguration

- HssConfiguration

The database information will be restored onto the active System Controller (SC) blade.

Caution: When restoring the database, all the services running on the system must be stopped except the active CoreSystemController, DataAccess and active Database services running on the active System Controller blade. If the active CoreSystemController service instance is not running on the same blade as the active Database service instance, perform a *Resume Geo-Redundancy with WebCI* of the CoreSystemController service. This will make sure the active CoreSystemController and active Database are running on the active System Controller blade.

Warning: WARNING: When restoring the database on a Geo-Redundant system, this operation can lead to loss of subscriber provisioning activity on the system if geo-redundancy was disabled for more than 4 hours. Refer to *Resume Geo-Redundancy with WebCI* for more information on Geo-Redundancy management.

CAUTION: When restoring the database, all the services running on the system must be stopped except the active CoreSystemController, DataAccess and active Database services running on the active System Controller blade. If the active CoreSystemController service instance is not running on the same blade as the active Database service instance, perform a *Performing a manual switchover* of the CoreSystemController service. This will make sure that the active CoreSystemController and active Database are running on the same blade, the active System Controller blade.

1. For the active System Controller slot, individually stop all the services on the blade except the active CoreSystemController service instance, the active Database service instance, and the DataAccess service. Use procedure *Stop a service on a slot*.

2. In the WebCI main menu, click **Database Backup/Restore/DRM** to display the Backup/Restore window.

3. Type the directory path to the list of backup files into the *FromDirectory* field.

4. Click on 'GetFileList' button.
   A drop down list will appear.

5. Click the down arrow to display the backup files.

6. Select the backup file to restore.

7. Click **Restore**.

   The system returns this message:

   ```
   Restore operation in progress. Check log file for completion status.
   ```

8. Verify that the restore operation has been completed by checking the log file
   Refer to *Viewing System Logs*

9. Restart all services on the active System Controller slot.
   a) Log onto the active System Controller blade through SSH and start a session.
   b) In the SSH window, type **service blue stop all** to stop all services of the active System Controller node. Wait for all services to be stopped completely.
   c) In the SSH window, type **service blue start** to start all services of the active System Controller node. Wait for all services to be started completely.

10. Start all other services that were running previously on the other blades from the WebCI using this procedure for each blade: *Start services on a slot*.

Manual switchover

The roles of an active Service and a standby Service (i.e., CoreSystemController) can be switched by invoking the switchover command from the WebCI. A switchover is performed from the active Service

because only the active Service can command the standby to take over control. A manual switchover can only be performed on the active instances of the following services:

- CoreSystemController
- Database
- Ldap

Manual switchovers are typically performed in the following situations:

- Verify proper switching action between active and standby and that standby will become active
- Switch the roles of the blades
- Upgrade current software to a new load
- Shut down blades to perform hardware maintenance.

Warning: A manual switchover cannot be performed on the service while the hardware scan is still in progress. When the hardware scan is initiated, the system automatically raises an alarm (AlarmId: 6815) and eventually clears it once the hardware scan is completed. A manual switchover can only be performed after this alarm has been automatically cleared by the system.

Caution: A switchover is service affecting and will result in a loss of traffic. It is recommended a switchover be done in a maintenance window when there is minimal traffic.

Performing a manual switchover

This procedure describes how to perform a manual switchover using the WebCI.

1. From the main menu, go to **System** > **Shelf View.**.

2. Click the symbol preceding the slot for which you wish to display more detailed information.

   This will display all the services running on that slot and their state (started/stopped).

3. Click the symbol preceding the service for which you wish to display more detailed information.

   This will display all the modules running within this service and their Operational state, Administrative state, Ha Role, and Resource state.

4. Verify the HaRole of the service for which you wish to perform a switchover.

   Note: A switchover can only be performed on an active instance of the services working in an active/standby mode.

5. Click the **SWO** button located in the same row as the active service for which you wish to perform a switchover.

6. The following warning will appear:

   ```
   This operation may be service affecting, Continue?
   ```

7. Click **OK** if you wish to Continue and perform a switchover or click **Cancel**.

8. Verify that the switchover took place by reading the HaRole value.

   Note: The standby blade will initialize first before changing into standby mode.

Viewing/Modifying Database Replication Monitoring (DRM) Configuration

The Database Replication Monitoring (DRM) process (see detailed description in the "Self Healing" section of the *SDM Product Description*) is configured by the Tekelec *My Oracle Support (MOS)*. The Network Operator can display and modify this configuration data from the Database Replication Monitoring table (DrmConfig[] entity) through one of the User Interfaces (CLI, WebCI, SOAP, CmdFileLoader).

This section describes how to display/modify the DRM configuration data from the WebCI.

To achieve this, follow the steps described below:

Requirements: Log in to a WebCI session with a username and password. Refer to *Starting a WebCI Session*.

1. Open the **Database** folder by clicking on it.
2. Open the **Backup/Restore/DRM** window (see figure below *Figure 56: Database Replication Monitoring (DRM)*)
3. The DRM configuration data will be displayed in the Database Replication Monitoring table.

   If you wish to modify any of this data, click on the **Modify** button located underneath the table. This will open up the DrmConfig Provisioning window, which allows you to enter the new values.

   For further instructions on how to navigate through the WebCI, refer to the "Web Craft Interface" section of the *SDM Monitoring, Maintaining, Troubleshooting – Reference Manual* and to *Web Craft Interface (WebCI)* in this document.

   For details on the DrmConfig[ ] entity and its parameters, refer to the "Self Healing (Database Replication Monitoring" section of the *SDM System Configuration – Reference Manual*.
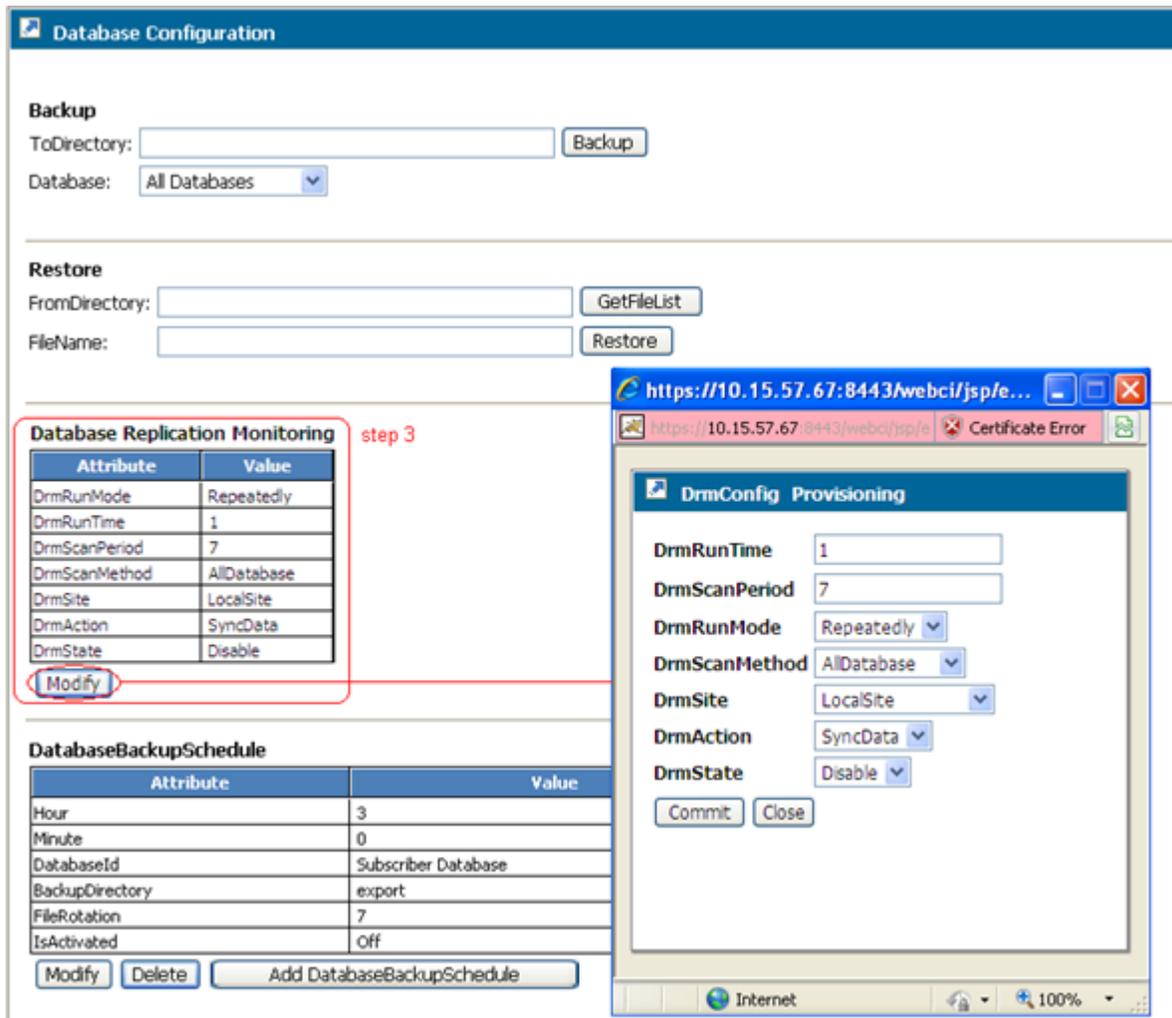
Figure 56: Database Replication Monitoring (DRM)

The DRM produces report files, which are saved in the active System Controller blade under the following directory: */blue/var/drm*.

There are three types of DRM reports:

4. The Schema Checker report, which includes any difference detected on the database structure.
5. The Data Checker report, which includes all the run-time consistency replication checks.
6. The Data Sync report, which includes the re-synchronized data that was different from the master server.

The Network Operator can analyze these reports and send it to the Tekelec *My Oracle Support (MOS)* if anomalies are detected.

Hereunder are instructions on how to access the DRM report files from a Telnet/SSH client:

Prerequisite: Connect to the system's active SystemController blade.

To view the system DRM report files, go to the drm directory, as shown in this example:

```
[admin@u1s3]# cd /blue/var/drm
[admin@u1s3 drm]# ll
total 12
-rw-rw-rw- 1 admin admin 344 Sep 30 15:23 u1s3-DataCheck-20100930192247.txt
-rw-rw-rw- 1 root root 727 Sep 30 15:23 u1s3-DataSync-20100930192247.txt
-rw-rw-rw- 1 root root 178 Sep 30 15:22 u1s3-SchemaCheck-20100930192247.txt
[admin@u1s3 drm]# more {DRM report file}
```

Where {DRM report file} is in the following format:

```
<Database>-<Host>-<Operation>-<Timestamp>.txt.
```

`<Database>`: represents the database's name which is monitored (such as: bluedb, bluedbvol, etc.).

`<Host>`: the slave database IP address in the following format: 255.255.255.255

`<Operation>`: schema check (i.e. database structure check), data check (i.e. data discrepancies detection) or data sync (i.e. data discrepancies correction).

Timestamp represents the time when the DRM file is created and has the format yyyymmddhhmmss.

Example:

```
[admin@u1s3 drm]# more u1s3-DataCheck-20100930192247.txt
---------------------------------
----- Start Data Check process -----
---------------------------------
>>>>> Start Data Check process on node: 10.15.57.67 in a Master-Slave replication
 <<<<<
Differences on P=3306,h=169.254.1.4
DB        TBL           CHUNK CNT_DIFF CRC_DIFF BOUNDARIES
blueoam_1 oamdatabase     0       1         1 1=1
```

This is an example of a Data Checker report.

>> Start Data Check process on nodes: 10.15.56.234, 10.15.56.235 in a Master-Master replication<<

```
DATABASE       CHUNK HOST      ENGINE COUNT  CHECKSUM          TIME WAIT  STAT  LAG
TABLE
----------------------------------------------------------------------------
Spdb           0 10.15.56.234 InnoDB 18704  0009a68fe1daeab   0   0      NULL
NULL
subscription
Spdb           0 10.15.56.235 InnoDB 18704  52baff89b41fc796  0   0      NULL
NULL
subscription
```

When viewing the Data Checker report it is important to note that there is a limitation due to the fact that the subscription table has one column. The data check uses the checksum to compare tables and it is possible that discrepancies may not be detected. Use the count in conjunction with the time to detect replication issues.

Viewing State of Database in Geo-Redundant Deployment

The following procedure can be used to view the state of the database of a system in a geo-redundant deployment.

Display the State of the Database from the CLI

This procedure describes how to display the state of the database.

1. Go to the Database subsystem, by typing:

```
:>
Database[]
```

2. Display the state of the database by typing the following:

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

Information similar to the following will be displayed:

DbGeoState: ReferenceProtected

Viewing the Provisioning VIP Addresses Configured on the System

Display the Provisioning VIP addresses of the system from the CLI

This procedure describes how to display the Provisioning VIP addresses configured on the system.

1. Go to the System subsystem, by typing:

```
:>
System[]
```

2. Go to the Shelf subsystem and specify the identification of the shelf for which you wish to view the configured Provisioning VIP addresses (i.e., ShelfId=1), and type:

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

3. Display the Provisioning VIP addresses of the system by typing the following:

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

Information similar to the following will be displayed:

```
ShelfId|Netmask|IpAddress|VipType|
--------------------------------
1|255.255.255.0|192.168.50.13|1
1|255.255.255.0|192.168.50.14|3
Displayed: 2
```

Putting the TCAP Layer Out of Service/in Service

Execute a TCAP out of service/TCAP in service.

This procedure describes the steps on how to put the TCAP layer out of service or back in service.

1. Navigate to `HLR > HLR Configuration`.

   The HLR Configuration window will appear.

2. Click on the **TCAP** tab.

Figure 57: TCAP Tab From The HLR Configuration Window

3. Click on the **TCAP out of service** button or on the **TCAP in service** button depending on the action you wish to take.

4. A warning message will pop up and ask you to confirm the action.

   If you wish to go ahead with the execution of this operation, click **OK**, otherwise click **Cancel**.

Performing a Cancel Location/Cancel GPRS Location

Cancel Location/Cancel GPRS Location.

This procedure describes the steps on how to perform a Cancel Location/Cancel GPRS Location in order to force the HLR to send a MAP_CANCEL_LOCATION message to the current VLR/SGSN location for the specified subscriber IMSI.

1. Navigate to `HLR > HLR Configuration`.

   The HLR Configuration window will appear.

2. Click on the **CancelLOC** tab to access the window shown below.

Figure 58: CancelLOC Tab From The HLR Configuration Window

3. In the white box, enter the **IMSI number** for which you wish the HLR to send a MAP_CANCEL_LOCATION message for.

4. A warning message will pop up and ask you to confirm the action.

   If you wish to go ahead with the execution of this operation, click **OK**, otherwise click **Cancel**.

Troubleshooting a Geo-Redundant System – Backup/Restore Procedures

This section presents restore constraints for geo-redundant systems, various restore scenarios and the procedures to execute those scenarios.

Restore constraints for geo-redundant systems

Geo-redundancy affects restore operations after a database backup.

Database selection

When the geo-redundancy is enabled, a database restore must be done carefully since more constraints affect this operation. Let's take the following diagram as an example:
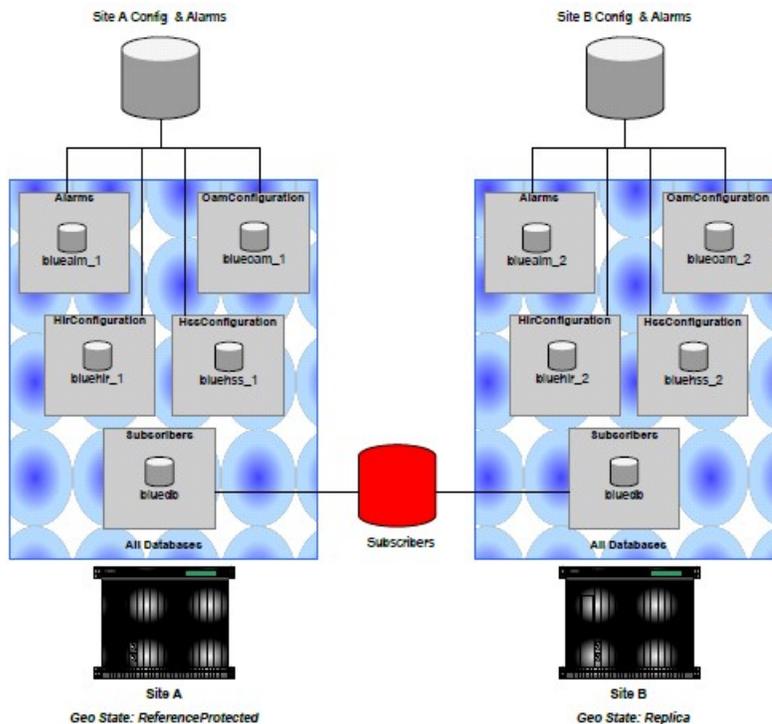
Figure 59: Backup source in a geo-redundant deployment

When performing a backup, the Network Operator must select one of the following options:

• All Databases

- Alarms
- OampConfiguration
- HlrConfiguration
- HssConfiguration
- Subscribers

With geo-redundancy, we must remember that some database apply to one single site while others are shared between the two geo-redundant sites. The Alarms, OamConfiguration, HlrConfiguration and HssConfiguration databases contain the configuration of a single site. When a backup of those databases is done, it must be restored on the same site.

The Subscribers database contains the data shared between sites through geo-redundancy. Therefore, this database can be restored anywhere.

When all the databases are backed up, both configuration data and subscribers are backed up. Therefore, a part of the backup can be restored anywhere while the other part applies only to one site. The result is that a full backup can be restored only on the same site from where it has been taken.

Note: When geo-redundancy is enabled, a full backup can be restored only on the same site from where it has been taken. Use individual database backup instead.

Site Selection

When geo-redundancy is enabled, a database backup cannot be installed on any site. Restoring a backup on the *Replica* site won't work if the geo-redundancy is enabled. The following example shows why.

In the next figure, we see that we have two geo-redundant sites. Site A is *ReferenceProtected* while site B is *Replica*. If we restore a backup on the *replica* site (site B), we need to restart site B after the backup has been restored. When site B restarts, it automatically connects to the geo-redundant site A. However, this operation synchronizes the site B database with site A *reference* database. This operation overwrites completely the data that was restored on site B at step 2.
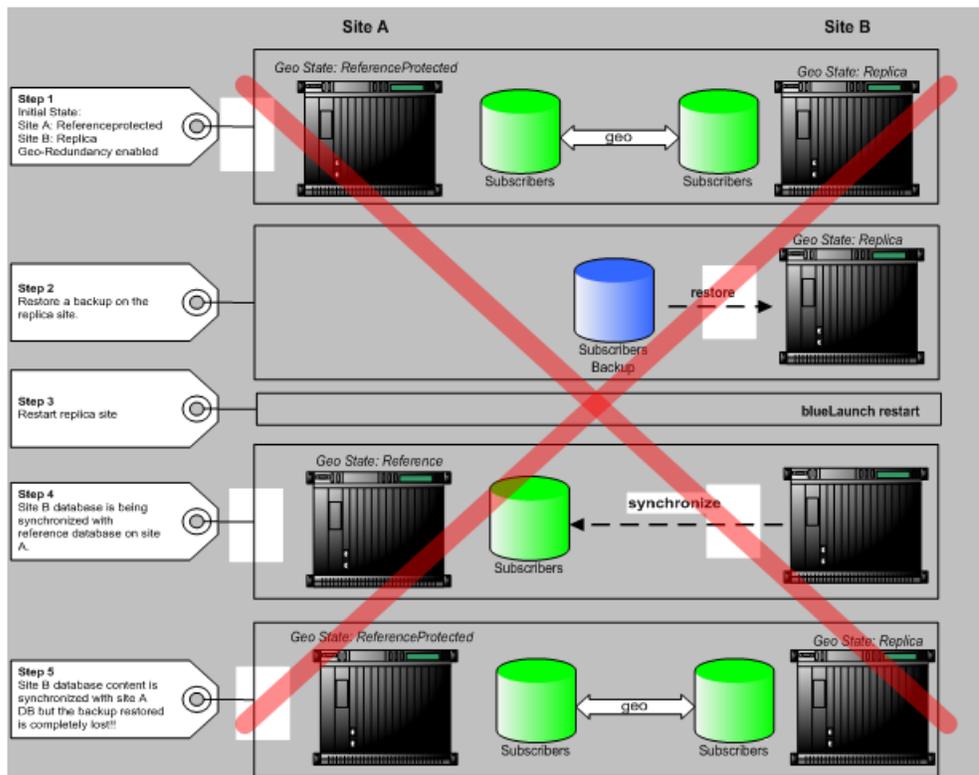
Figure 60: Restoring a backup on the Replica site of a geo-redundant deployment

The way to restore a backup on a geo-redundant system and propagate the backup to the peer site is to shutdown the Replica site, install the backup on the Reference site, restart the Reference site and then restart the Replica site. The last step will synchronize the Replica database with the backup restored on the Reference site.

If the user can only restore the backup on the Replica site because he only has a full backup of the Replica site's database (and not only a Subscribers database backup as recommended) it can do so by disabling the geo-redundancy and clearing the geo-redundancy status.

Clearing Geo-redundancy Status

Before starting a site to force it to take the reference role (if the peer site is not started), the entry in the OamConfiguration database that indicates the location of the most recent *Reference* site must be cleared. Contact the Tekelec *My Oracle Support (MOS)* to clear the geo-redundancy status.

Restarting a 2-Blade System

Target setup:
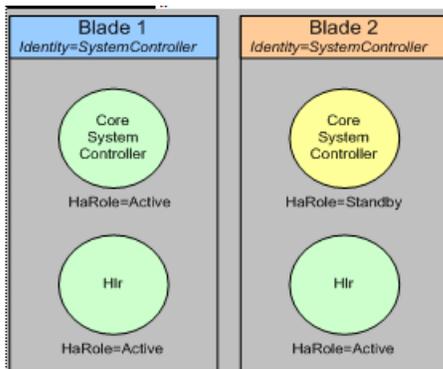
1. Stop the standby system controller (blade 2).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]> StopServices()
```

2. Restart the blade that hosts the active system controller (blade 1).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade1SlotId]> RestartServices()
```

   • The connection to the WebCI/CLI will be lost while the blade is restarting.

   • It will be available again once the restart is completed.

3. Start the blade that hosts the standby system controller (blade 2).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]> StartServices()
```

4. Wait for standby blade initialization to complete (blade 2).

5. Display the status of ServiceInstance() running on the standby blade (blade 2) and wait for all OpState to go to *enabled* state.

```
9 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId ]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId     |ServiceState|
_____
 1|   locked|       healthy|
9|unassigned|disabled|SystemController|CoreSystemController|    Started| 1|
unlocked|      healthy|     9|unassigned|disabled|SystemController|
    Hlr|    Started| 10 :System[]:Shelf[ShelfId = 1]:Slot[SlotId =
Blade2SlotId]> display ServiceInstance[] This Command could potentially display
 a very large number of instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId     |ServiceState|
_____
 1|  unlocked|       healthy|    9|standby   |enabled
|SystemController|CoreSystemController|    Started| 1|  unlocked|      healthy|
    9|unassigned|disabled|SystemController|          Hlr|    Started|
11 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId     |ServiceState|
```

```
_____
  1|  unlocked|       healthy|      9|standby    |enabled
|SystemController|CoreSystemController|    Started| 1|  unlocked|       healthy|
     9|active     |enabled |SystemController|                 Hlr|    Started|
```

Restoring a Backup on a 2-Blade System

Initial setup:

1. Stop all **user services** (Hlr, Hss, HssProvisioning) on both blades
2. Stop the standby CoreSystemController service.
3. Restore the backup.
4. Restart the active system controller blade from the shell:

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade1SlotId]>RestartServices() 17
:System[]>
```

   a) This step will restart the CoreSystemController and user service on blade 1.

5. Start the blade that host the standby system controller (blade 2)

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]>StartServices() 17 :System[]>
```

6. Wait for standby blade initialization to complete (blade 2).

   Display the status of ServiceInstance() running on the standby blade (blade 2) and wait for all OpState to go to *enabled* state.

```
9 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId      |ServiceState|
_____
 1|    locked|       healthy|
9|unassigned|disabled|SystemController|CoreSystemController|    Started| 1|
unlocked|       healthy|      9|unassigned|disabled|SystemController|
     Hlr|    Started| 10 :System[]:Shelf[ShelfId = 1]:Slot[SlotId =
Blade2SlotId]> display ServiceInstance[] This Command could potentially display
 a very large number of instances. Proceed with display? (y/[n]): y
```

```
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |    IdentityId    |
    ServiceId      |ServiceState|
─────────────────────────────────────────────────────────────────────────────────
 1|  unlocked|      healthy|    9|standby   |enabled
|SystemController|CoreSystemController|    Started| 1|  unlocked|      healthy|
     9|unassigned|disabled|SystemController|           Hlr|     Started|
11 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |    IdentityId    |
    ServiceId      |ServiceState|
─────────────────────────────────────────────────────────────────────────────────
 1|  unlocked|      healthy|    9|standby   |enabled
|SystemController|CoreSystemController|    Started| 1|  unlocked|      healthy|
     9|active    |enabled |SystemController|           Hlr|     Started|
```

Restarting a system with Front-End Nodes

Use this procedure to restart a system with more than two blades.

Target setup:
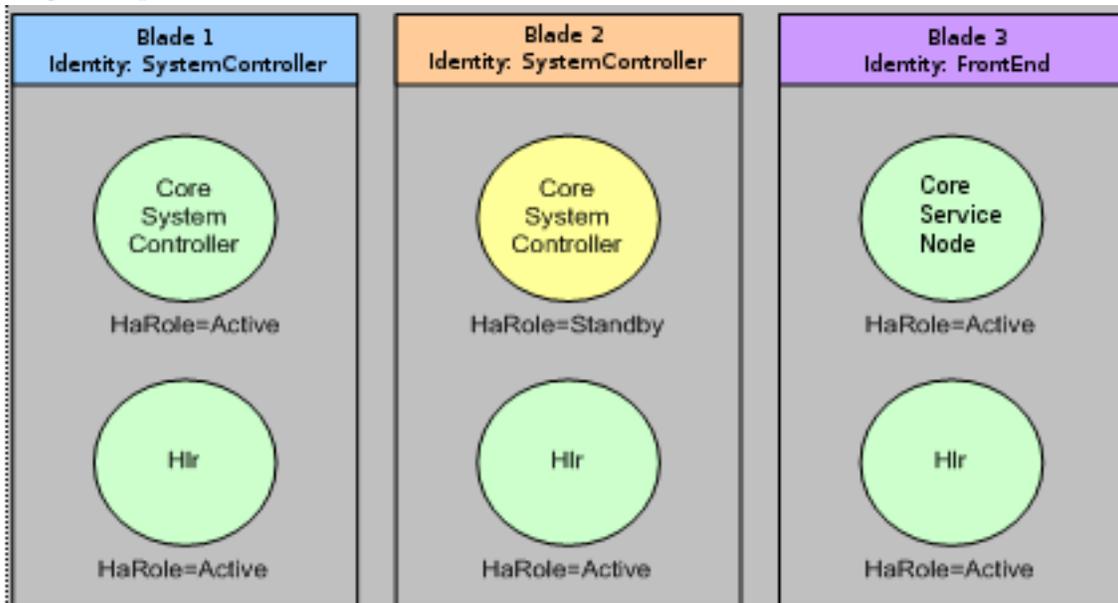
Figure 61: Multiple Blade System with Front-End Node(s)

1. Stop the front-end node blade (blade 3).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade3SlotId]>StopServices() 17 :System[]>
```

2. Stop the standby system controller (blade 2).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]>StopServices() 17 :System[]>
```

3. Restart the blade that hosts the active system controller (blade 1).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade1SlotId]>RestartServices() 17
:System[]>
```

- The connection to the WebCI/CLI will be lost while the blade is restarting.

- It will be available again once the restart is completed.

4. Start the blade that hosts the standby system controller (blade 2).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]>StartServices() 17 :System[]>
```

5. Wait for standby blade initialization to complete (blade 2).

6. Display the status of ServiceInstance() running on the standby blade (blade 2) and wait for all OpState to go to the *enabled* state.

```
9 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId    |
   ServiceId      |ServiceState|
-----------------------------------------------------------------------------------
 1|    locked|        healthy|
9|unassigned|disabled|SystemController|CoreSystemController|     Started| 1|
unlocked|        healthy|      9|unassigned|disabled|SystemController|
    Hlr|      Started| 10 :System[]:Shelf[ShelfId = 1]:Slot[SlotId =
Blade2SlotId]> display ServiceInstance[] This Command could potentially display
 a very large number of instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId    |
   ServiceId      |ServiceState|
-----------------------------------------------------------------------------------
 1| unlocked|        healthy|     9|standby   |enabled
|SystemController|CoreSystemController|     Started| 1| unlocked|       healthy|
    9|unassigned|disabled|SystemController|               Hlr|      Started|
11 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId    |
   ServiceId      |ServiceState|
-----------------------------------------------------------------------------------
 1| unlocked|        healthy|     9|standby   |enabled
|SystemController|CoreSystemController|     Started| 1| unlocked|       healthy|
    9|active    |enabled |SystemController|               Hlr|      Started|
```

7. Start the front-end node blade (blade 3).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade3SlotId]>StartServices() 17 :System[]>
```

8. Wait for front-end node blade initialization to complete (blade 3).

9. Display the status of ServiceInstance() running on the standby blade (blade 3) and wait for all OpState to go to the *enabled* state.

```
9 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade3SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |IdentityId |
```

```
ServiceId    |ServiceState|
─────────────────────────────────────────────────────────────────────────────
 1|    locked|       healthy|
10|unassigned|disabled|FrontEndNode|CoreSServiceNode|    Started| 1|  unlocked|
    healthy|       10|unassigned|disabled|FrontEndNode|            Hlr|
Started| 10 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade3SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |IdentityId |
ServiceId    |ServiceState|
─────────────────────────────────────────────────────────────────────────────
 1|    locked|       healthy|    10|    active|
enabled|FrontEndNode|CoreSServiceNode|    Started| 1|  unlocked|      healthy|
    10|unassigned|disabled|FrontEndNode|           Hlr|     Started| 11
:System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade3SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |IdentityId |
ServiceId    |ServiceState|
─────────────────────────────────────────────────────────────────────────────
 1|    locked|       healthy|    10|    active|
enabled|FrontEndNode|CoreSServiceNode|    Started| 1|  unlocked|      healthy|
    10|    active| enabled|FrontEndNode|           Hlr|     Started|
```

Restoring a backup on a system with Front-End Nodes

This procedure restores a backup on a system with more than two blades.

Initial setup:
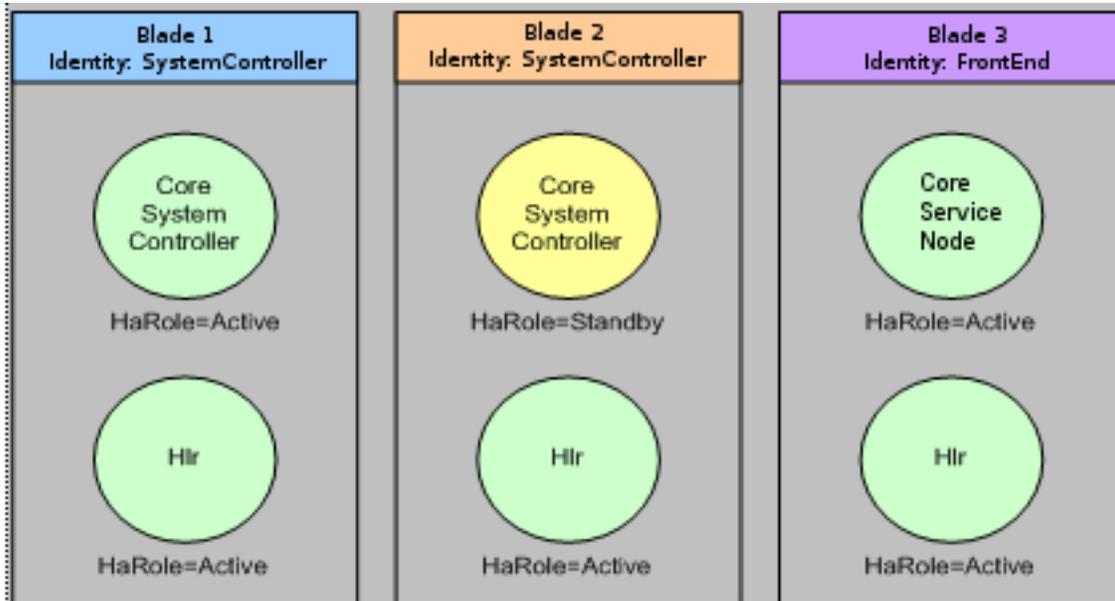
1. Stop the front-end node blade (blade 3).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade3SlotId]>StopServices() 17 :System[]>
```

2. Stop the standby system controller (blade 2).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]> StopServices() 17 :System[]>
```

3. Stop all user services (Hlr, HSS, HssProvisioning) on active system controller blade (blade 1).

4. Restore the backup.

5. Restart the blade that hosts the active system controller (blade 1).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade1SlotId]>RestartServices() 17
:System[]>
```

- The connection to the WebCI/CLI will be lost while the blade is restarting.

- It will be available again once the restart is completed.

6. Start the blade that hosts the standby system controller (blade 2).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade2SlotId]>StartServices() 17 :System[]>
```

7. Wait for standby blade initialization to complete (blade 2).

8. Display the status of ServiceInstance() running on the standby blade (blade 2) and wait for all OpState to go to the *enabled* state.

```
9 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId     |ServiceState|
_____
 1|   locked|      healthy|
9|unassigned|disabled|SystemController|CoreSystemController|    Started| 1|
unlocked|      healthy|      9|unassigned|disabled|SystemController|
   Hlr|     Started| 10 :System[]:Shelf[ShelfId = 1]:Slot[SlotId =
Blade2SlotId]> display ServiceInstance[] This Command could potentially display
 a very large number of instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId     |ServiceState|
_____
 1|  unlocked|      healthy|     9|standby  |enabled
|SystemController|CoreSystemController|    Started| 1|  unlocked|     healthy|
     9|unassigned|disabled|SystemController|              Hlr|     Started|
11 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade2SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |   IdentityId   |
   ServiceId     |ServiceState|
_____
 1|  unlocked|      healthy|     9|standby  |enabled
|SystemController|CoreSystemController|    Started| 1|  unlocked|     healthy|
     9|active    |enabled |SystemController|              Hlr|     Started|
```
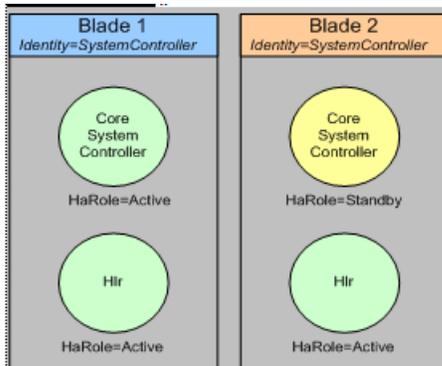
9. Start the service on node blade (blade 3).

```
:System[]:Shelf[ShelfId=1]:Slot[SlotId=Blade3SlotId]> StartServices() 17
:System[]>
```

10. Wait for front-end node blade initialization to complete (blade 3).

11. Display the status of ServiceInstance() running on the front-end node blade (blade 3) and wait for all OpState to go to the *enabled* state.

```
9 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade3SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |IdentityId |
ServiceId    |ServiceState|
-----------------------------------------------------------------------------------------
 1|    locked|       healthy|
10|unassigned|disabled|FrontEndNode|CoreSServiceNode|    Started| 1|  unlocked|
     healthy|    10|unassigned|disabled|FrontEndNode|           Hlr|
Started| 10 :System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade3SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |IdentityId |
ServiceId    |ServiceState|
-----------------------------------------------------------------------------------------
 1|    locked|       healthy|    10|    active|
enabled|FrontEndNode|CoreSServiceNode|    Started| 1|  unlocked|       healthy|
    10|unassigned|disabled|FrontEndNode|           Hlr|      Started| 11
:System[]:Shelf[ShelfId = 1]:Slot[SlotId = Blade3SlotId]> display
ServiceInstance[] This Command could potentially display a very large number of
 instances. Proceed with display? (y/[n]): y
ShelfId|AdminState|ResourceState|SlotId|  HaRole  |OpState |IdentityId |
ServiceId    |ServiceState|
-----------------------------------------------------------------------------------------
 1|    locked|       healthy|    10|    active|
enabled|FrontEndNode|CoreSServiceNode|    Started| 1|  unlocked|       healthy|
    10|    active| enabled|FrontEndNode|           Hlr|     Started|
```

Scenarios

This section describes the procedures for different restore scenarios. In each case, two diagrams show the system's geo-redundancy initial state and final state. Each section also provides a table identifying which database is affected by the restore scenario.

Each scenario traffic impact is categorized using one of the following options:

- *No Impact*: During the procedure, there is always a site running that can handle traffic
- *Major Impact*: During the procedure, all applications on all sites are shut down for a long period of time and even both site are completely shut down at one point.
- *Minimal Impact*: The procedure has been designed to minimize the downtime. Most of the time, one of the site is running and can handle traffic.

Restoring Subscribers Backup

This is the typical scenario that should be used to restore the 'Subscribers' database backup on a geo-redundant system.

Prerequisite: The Network Operator has already taken a backup of the 'Subscribers' database.

At the end, restoring this backup will affect the following DB:

Table 33: Restoring Subscriber Backup

DB	Site A	Site B
Subscribers	+	+
OamConfiguration		
HlrConfiguration		
HssConfiguration		
SipConfiguration		

TRAFFIC IMPACT: Major Impact

<u>Scenario:</u>

Figure 62: Restoring The 'Subscribers' Database Backup In A Geo-redundant Deployment

<u>Procedure:</u>

1. Disable geo-redundancy on *replica* site (site B) using **System:DisableGeoRedundancy()** operation in BlueCli.

2. Site B should go to *UnassignedDisabled* state and site A *Reference*.

3. Enable geo-redundancy on *replica* site (site B) using **System:EnableGeoRedundancy()** operation in BlueCli.

4. Site B should go to *UnassignedEnabled* state and site A geo state should stay unchanged.

5. Restore the backup on *reference* site (site A) using *Restoring a Backup on a 2-Blade System* or *Restoring a backup on a system with Front-End Nodes*.

6. Restart *replica* site (site B) using *Restarting a 2-Blade System* or *Restarting a system with Front-End Nodes*.

7. Site B should go to *Replica* state and site A *ReferenceProtected*.

   <u>Final state:</u>

Figure 63: Final State Of The Geo-redundant Sites After Restoring The 'Subscribers' Database Backup

Restoring a Full Backup Taken on the *Reference* Site

This is a scenario where the operator wants to restore a full backup that was taken on the *reference* site. A full backup can be restored **only on the site it has been taken**. In this case, the backup must be restored on the *reference* site.

At the end, restoring this backup will affect the following databases:

Table 34: Databases Affected by Backup Restoration on Reference Site

DB	Site A	Site B
Subscribers	+	+
OamConfiguration	+	
HlrConfiguration	+	
HssConfiguration	+	
SipConfiguration	+	

TRAFFIC IMPACT: Major Impact

Scenario:
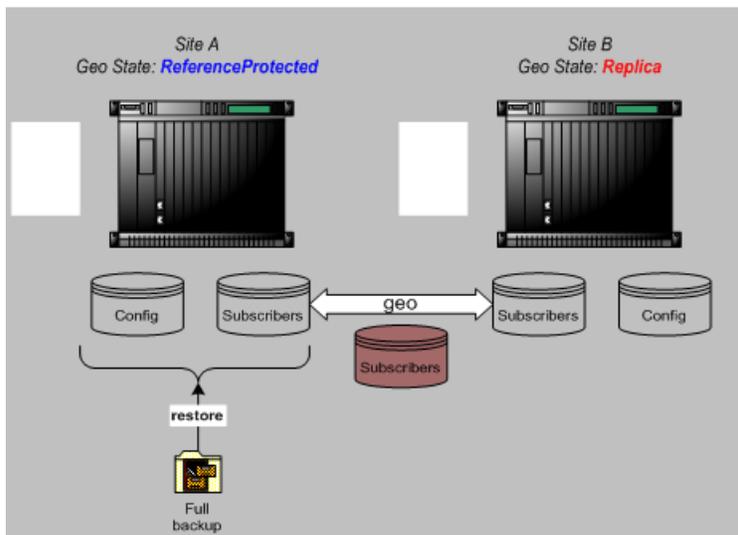
Figure 64: Restoring A Full Backup On The Reference Site

<u>Procedure:</u>

1. Disable geo-redundancy on *replica* site (site B) using **System:DisableGeoRedundancy()** operation in BlueCli.

2. Site B should go to *UnassignedDisabled* state and site A *Reference*.

3. Enable geo-redundancy on *replica* site (site B) using **System:EnableGeoRedundancy()** operation in BlueCli.

4. Site B should go to *UnassignedEnabled* state and site A geo state should stay unchanged.

5. Restore the backup on *reference* site (site A) using *Restoring a Backup on a 2-Blade System* or *Restoring a backup on a system with Front-End Nodes*.

6. Restart *replica* site (site B) using *Restarting a 2-Blade System* or *Restarting a system with Front-End Nodes*.

7. Site B should go to *Replica* state and site A *ReferenceProtected*.

   <u>Final state:</u>

Figure 65: Final State After Restoring A Full Backup On The Reference Site

Restoring a Full Backup Taken on the Replica Site

This describes how to restore a full database backup that was taken on the replica site. A full backup can be restored only on the site it has been taken. In this case, the backup must be restored on the replica site. This procedure requires to shutdown the reference site; therefore, it will produce a geo-redundancy switch-over. It means that at the end, the initial reference will be replica and the initial replica will be the reference.

At the end, restoring this backup will affect the following databases:

Table 35: Restoring a Full Backup Taken on the Replica Site

DB	Site A	Site B
Subscribers	+	+
OamConfiguration		+
HlrConfiguration		+
HssConfiguration		+
SipConfiguration		+

TRAFFIC IMPACT: Major Impact

Scenario:
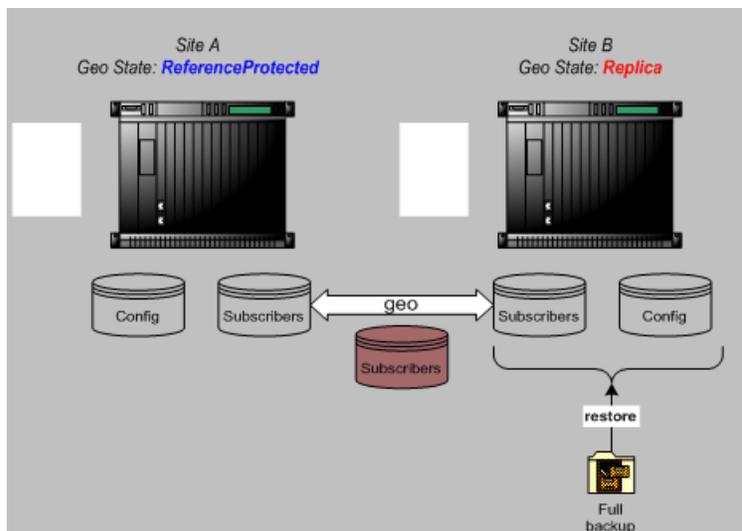
Figure 66: Restoring A Full Database Backup On The Replica Site

Procedure:

1. Disable geo-redundancy on reference site (site A) using **System:DisableGeoRedundancy()** operation in BlueCli.
2. Site A should go to UnassignedDisabled state and site B PendingReference.
3. Force Site B to Reference state by calling **System:ForceGeoReference()** on site B CLI.
4. Site B should go to Reference state.

5. Enable geo-redundancy on replica site (siteA) using **System:EnableGeoRedundancy()** operation in BlueCli.

6. Site A should go to UnassignedEnabled state and site B geo state should stay unchanged.

7. Restore the backup on reference site (site B) using *Restoring a Backup on a 2-Blade System* or *Restoring a backup on a system with Front-End Nodes*.

8. Restart new replica site (site A) using procedure *Restarting a 2-Blade System* or *Restarting a system with Front-End Nodes*.

9. Site A should go to Replica state and site B ReferenceProtected.
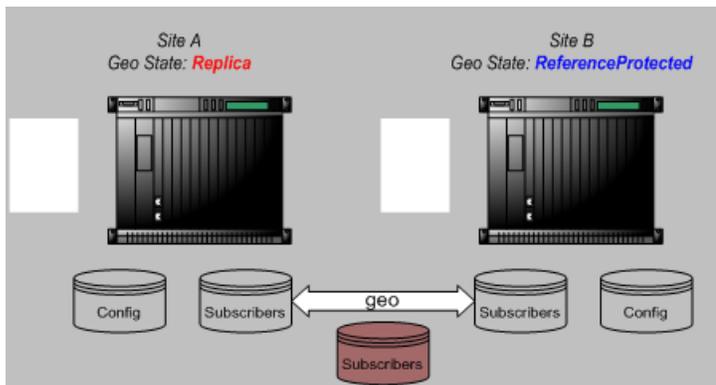
Final state:

Figure 67: Final State After Restoring A Full Backup On The Replica Site

Restoring a Configuration Backup Taken on the *Reference* Site

This describes how to restore a configuration database backup that was taken on the *reference* site.

A configuration backup can be restored **only on the site it has been taken**. In this case, the backup must be restored on the *reference* site.

This scenario is not traffic impacting since the *replica* site can continue to run while the backup is being restored. After backup restore, the *replica* site will take the *reference* role since site A need to be restarted in order to apply the back upped.

At the end, restoring this backup will affect the following databases:

Table 36: Databases Affected by Configuration Backup on Reference Site

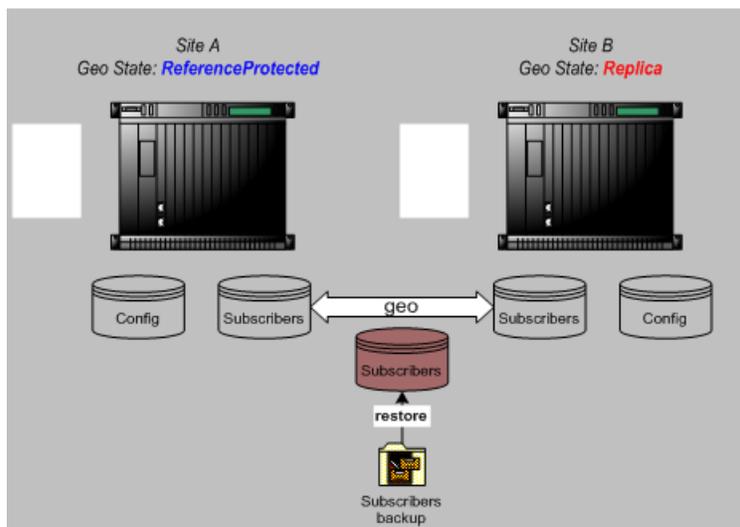| DB	Site A	Site B
Subscribers		
OamConfiguration	+	
HlrConfiguration	+	
HssConfiguration	+	
SipConfiguration	+	

TRAFFIC IMPACT: No Impact

<u>Scenario:</u>
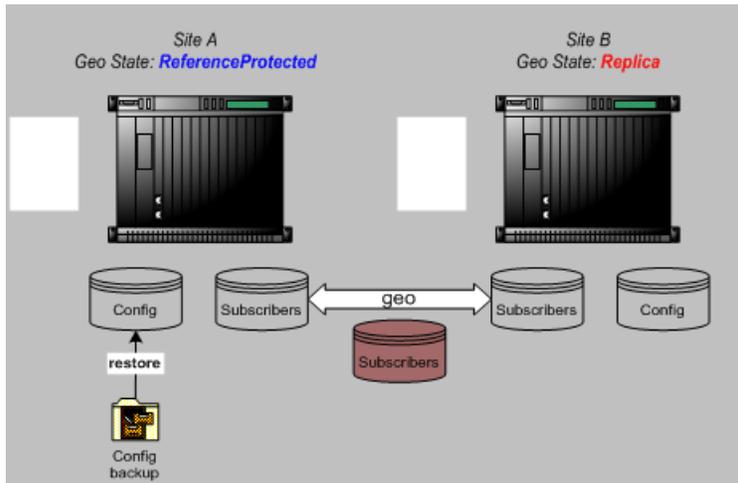
Figure 68: Restoring Configuration Database Backup On Reference Site

<u>Procedure:</u>

1. To prevent traffic impact, all traffic should be re-directed to site B.
2. Disable geo-redundancy on *reference* site (site A) using **System:DisableGeoRedundancy()** operation in BlueCli.
3. Site A should go to *UnassignedDisabled* state and site B *PendingReference*.
4. Force Site B to *Reference* state by calling **System:ForceGeoReference()** on site B CLI.
5. Site B should go to *Reference* state.
6. Enable geo-redundancy on *replica* site (site A) using **System:EnableGeoRedundancy()** operation in BlueCli.
7. Site A should go to *UnassignedEnabled* state and site B geo state should stay unchanged.
8. Restore the backup on site (site A) using *Restoring a Backup on a 2-Blade System* or *Restoring a backup on a system with Front-End Nodes*
9. Traffic can be restored on site A.
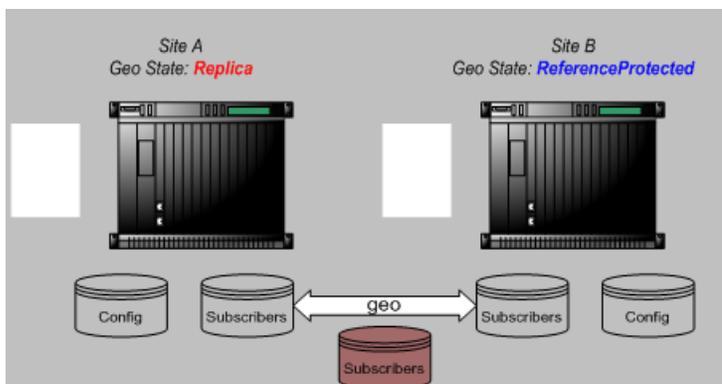
<u>Final state:</u>

Figure 69: Final State After Restoring A Configuration Database Backup On Reference Site

Restoring a Configuration Backup Taken on the *Replica* Site

This describes how to restore a configuration database backup that was taken on the *replica* site.

A configuration backup can be restored **only on the site it has been taken**. In this case, the backup must be restored on the *replica* site.

This scenario is not traffic impacting since the *reference* site can continue to run while the backup is being restored. After backup restore, the *replica* site will take back the *replica* role since the *reference* site is never stopped.

At the end, restoring this backup will affect the following databases:

Table 37: Databases Affected by Configuration Backup on Replica Site

DB	Site A	Site B
Subscribers		
OamConfiguration		+
HlrConfiguration		+
HssConfiguration		+
SipConfiguration		+

TRAFFIC IMPACT: No Impact

Scenario:
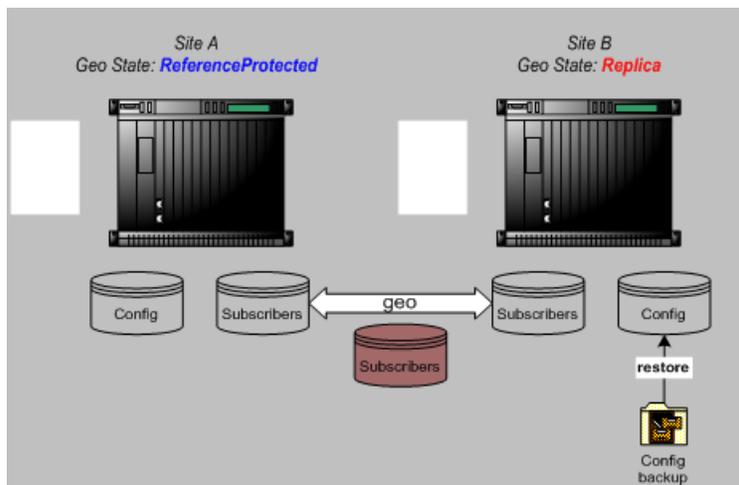
Figure 70: Restoring A Configuration Database Backup On The Replica Site

Procedure:

1. To prevent traffic impact, all traffic should be re-directed to site A.
2. Disable geo-redundancy on *replica* site (site B) using **System:DisableGeoRedundancy()** operation in BlueCli.
3. Site B should go to *UnassignedDisabled* state and site A *Reference*.

4. Enable geo-redundancy on *replica* site (site B) using **System:EnableGeoRedundancy()** operation in BlueCli.

5. Site B should go to *UnassignedEnabled* state and site A geo state should stay unchanged.

6. Restore the backup on *replica* site (site B) using *Restoring a Backup on a 2-Blade System* or *Restoring a backup on a system with Front-End Nodes*.

7. Traffic can be restored on site B.

Final state:

Figure 71: Final State After Restoring A Configuration Database Backup On The Replica Site

Restoring a Configuration Backup from a Full Database Backup Taken on the *Reference* Site

This describes how to restore a configuration database backup from a full database backup that was taken on the *reference* site.Such backup can be restored **only on the site it has been taken**. In this case, the backup must be restored on the *reference* site.

This scenario is not traffic impacting since the *replica* site can continue to run while the backup is being restored. After backup restore, the *replica* site will take the *reference* role since site A need to be restarted in order to apply the back upped. In this scenario, the configuration and subscribers databases will be restored from the full backup. However, since the peer site will take over the reference role, the subscriber's database will be overwritten by the peer site database content. At the end, only the configuration database will be restored.

At the end, restoring this backup will affect the following databases:

Table 38: Databases Affected by Backup Restoration

| DB	Site A	Site B
Subscribers		
OamConfiguration	+	
HlrConfiguration	+	
HssConfiguration	+	
SipConfiguration	+	

TRAFFIC IMPACT: No Impact

<u>Scenario:</u>
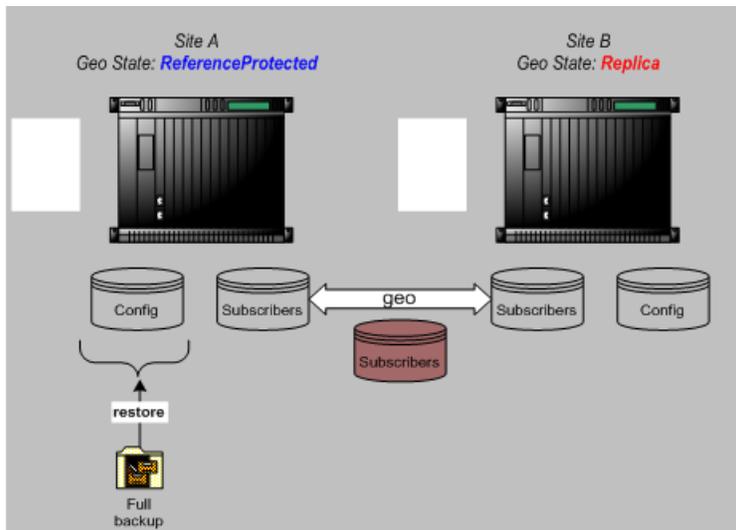
Figure 72: Restoring A Configuration Backup From A Full Database Backup On The Reference Site

<u>Procedure:</u>

1. To prevent traffic impact, all traffic should be re-directed to site B.
2. Disable geo-redundancy on *reference* site (site A) using **System:DisableGeoRedundancy()** operation in BlueCli.
3. Site A should go to UnassignedDisabled state and site B *PendingReference*.
4. Force Site B to Reference state by calling **System:ForceGeoReference()** on site B CLI.
5. Site B should go to Reference state.
6. Enable geo-redundancy on replica site (site A) using **System:EnableGeoRedundancy()** operation in BlueCli.
7. Site A should go to *UnassignedEnabled* state and site B geo state should stay unchanged.
8. Restore the backup on *reference* site (site A) using procedure *Restoring a Backup on a 2-Blade System* or *Restarting a system with Front-End Nodes*.
9. Traffic can be restored on site A.
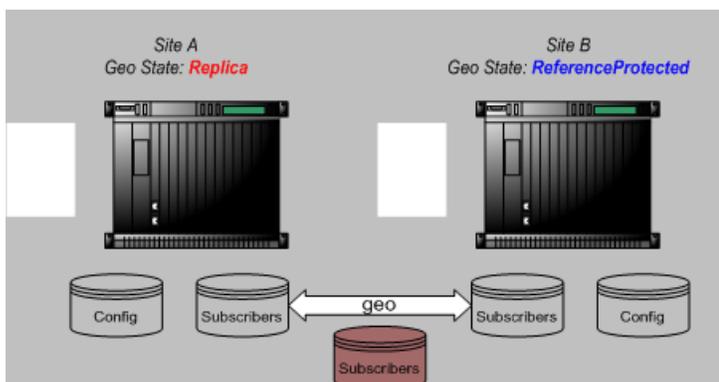
   <u>Final state:</u>

Figure 73: Final State After Restoring A Configuration Backup From A Full Database Backup On The Reference Site

Restoring a Configuration Backup from a Full Database Backup Taken on the *Replica* Site

This describes how to restore a configuration database backup from a full database backup that was taken on the *replica* site. Such backup can be restored **only on the site it has been taken**. In this case, the backup must be restored on the *replica* site.

This scenario is not traffic impacting since the *reference* site can continue to run while the backup is being restored. In this scenario, the configuration and subscribers databases will be restored from the full backup. However, the replica site restored subscriber's database will be overwritten by the peer reference site database content. At the end, only the configuration database will have been restored on the replica.

At the end, restoring this backup will affect the following databases:

Table 39: Databases Affected by Configuration Backup from Full Database Backup on Replica Site

DB	Site A	Site B
Subscribers		
OamConfiguration		+
HlrConfiguration		+
HssConfiguration		+
SipConfiguration		+

TRAFFIC IMPACT: No Impact

Scenario:
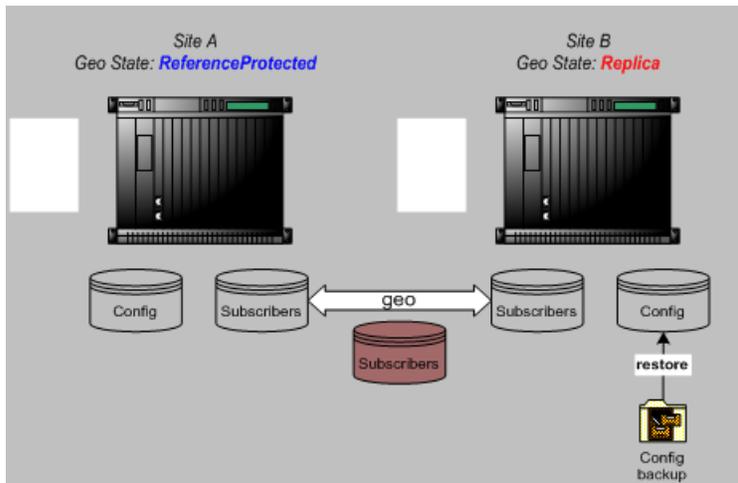
Figure 74: Restoring A Configuration Backup From A Full Database Backup On The Replica Site

Procedure:

1. To prevent traffic impact, all traffic should be re-directed to site A.

2. Disable geo-redundancy on *replica* site (site B) using **System:DisableGeoRedundancy()** operation in TekelecCli.

3. Site B should go to *UnassignedDisabled* state and site A *Reference*.

4. Enable geo-redundancy on *replica* site (site B) using **System:EnableGeoRedundancy()** operation in BlueCli.

5. Site B should go to *UnassignedEnabled* state and site A geo state should stay unchanged.

6. Restore the backup on *replica* site (site B) using *Restoring a Backup on a 2-Blade System* or *Restoring a backup on a system with Front-End Nodes*.
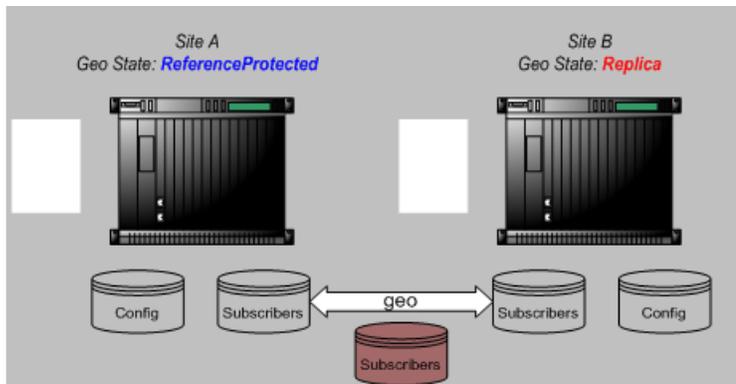
7. Traffic can be restored on site B.
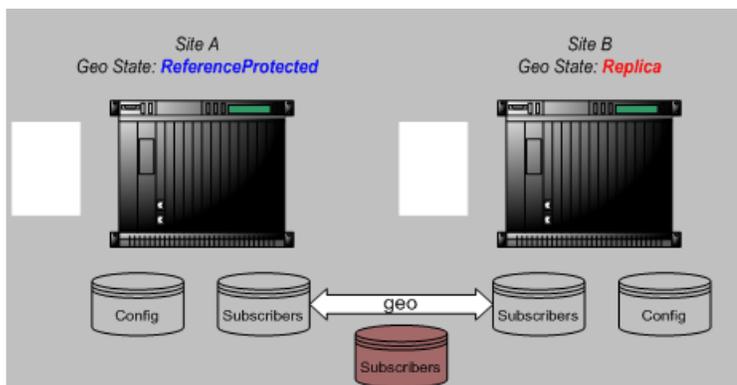
   Final state:

Figure 75: Final State After Restoring A Configuration Backup From A Full Database Backup On The Replica Site

View License and Log Information from the WebCI

This procedure describes the steps to view license and log information. For details on the license attributes, refer to the *SDM Monitoring, Maintenance, Troubleshooting - Reference Manual*

From the main menu, navigate to `Oamp > LicenseManager`.

This will display the License Manager Configuration window (as shown below).
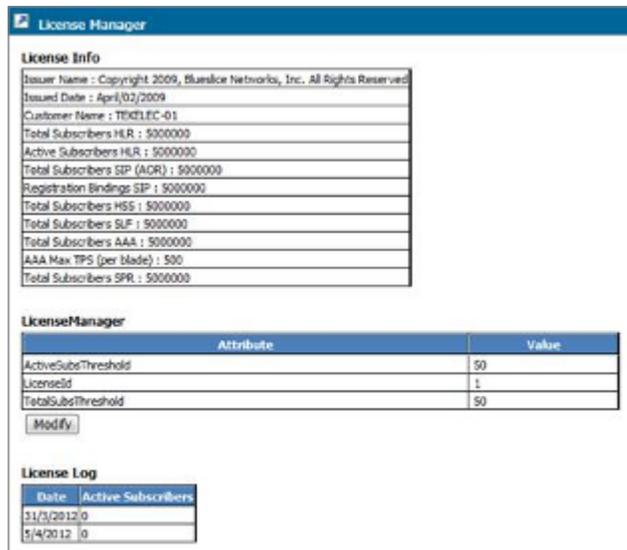
Figure 76: License Manager window

Set Active Subscribers Warning Threshold

This procedure displays the steps on how to modify the Active Subscribers warning threshold, which is applicable for both the HLR and SIP applications. The threshold value is a percentage value from 0-100%. The warning threshold alarm will be triggered when the percentage of HLR/SIP active subscribers exceeds the percentage threshold value.

Note: when the threshold value is set to 0, no warning alarms will be generated. This is the equivalent of disabling this warning alarm.

1. From the main menu, navigate to `Oamp > LicenseManager`.

   This will display the License Management Configuration window.

2. At the bottom of the License Manager table, click **Modify**.

3. When LicenseManager Provisioning window appears (as shown below), enter the percentage threshold to be changed.
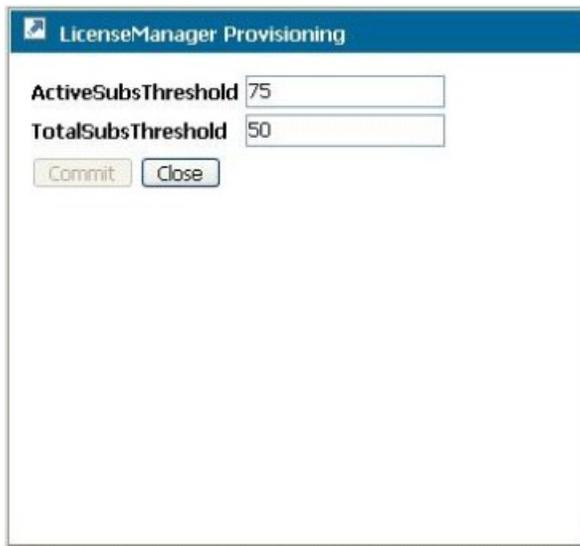
Figure 77: License Management Configuration

4. Click **Commit**.
5. When the confirmation message (**Entity entry was successfully committed**) appears, click **OK**.

Troubleshooting Subscriber Provisioning

Viewing the Number of Active HLR Subscribers

The operator can obtain statistics on the number of active HLR subscribers currently on the system, by viewing the log information reported by the License Manager. Refer to the previous section for step-by-step instructions on how to view 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.

Troubleshooting congestion in SPR Received-Message Queue

When experiencing congestion in the queue for SPR received messages, confirm that the queue-size value aligns with the recommended values. Refer to the **ReceivedMessagesQueueSize** parameter in the HSS SPR Configuration (**HssSprConfig**) table (*SDM System Configuration Reference Manual*)

The internal receive queue is configured with the number of requests that can be received and processed by the HSS. The queue size must be calculated based on the overall TPS dimensioning for the system. Setting a queue size too small may result in congestion due to queue exhaust. Setting the queue size

too large may impact the ability to detect congestion. As a system grows in TPS, the initially configured value may have to be updated.

Glossary

#

3GPP

    3rd Generation Partnership Project. The standards body for wireless communications.

    3rd Generation Partnership Project

A

AAA

    Authentication, Authorization, and Accounting (Rx Diameter command)

AIS

    Alarm Indication Signal

APN

    Access Point Name

    The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.

AuC

    Authentication Center

B

BAOC

    Barring of All Outgoing Calls

BICROAM

    Barring of Incoming Calls when ROAMing outside home PLMN Country

BOIC

    Barring of Outgoing International Calls

B

BOICEXHC	Barring of Outgoing International Calls EXcept those directed to the Home PLMN Country

C

CAMEL	Customized Applications for Mobile networks Enhanced Logic
CFB	Call Forwarding on Mobile Subscriber Busy
CFNRC	Call Forwarding on Mobile Subscriber Not Reachable
CFNRY	Call Forwarding on Mobile Subscriber No Reply
CFU	Call Forwarding Unconditional
CLI	Command-line interface
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CPU	Central Processing Unit

C

CRC	CAM Redundancy Controller
	Cyclic Redundancy Check
	A number derived from, and stored or transmitted with, a block of data in order to detect corruption. By recalculating the CRC and comparing it to the value originally transmitted, the receiver can detect some types of transmission errors.
CS	Controlled Slip
CSU	Channel Service Unit
CSV	Comma-separated values
	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
DNS	Domain Name Services
	Domain Name System
	A system for converting Internet host and domain names into IP addresses.

D

DPC

Destination Point Code - 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, but does not have to be.

E

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 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.

E.164 Number Mapping

ESD

Electro-Static Discharge

ESF

Extended Super Frame

G

GMT

Greenwich Mean Time

GPRS

General Packet Radio Service

G

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.

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.

H

HPLMN   Home Public Land Mobile
                                         Network

HSS   Home Subscriber Server

                                         A central database for subscriber
                                         information.

HTTP   Hypertext Transfer Protocol

I

IMSI   International Mobile Subscriber
                                         Identity

                                         A unique internal network ID
                                         identifying a mobile subscriber.

                                         International Mobile Station
                                         Identity

L

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

LTE   Long Term Evolution

                                         The next-generation network
                                         beyond 3G. In addition to enabling
                                         fixed to mobile migrations of
                                         Internet applications such as Voice
                                         over IP (VoIP), video streaming,
                                         music downloading, mobile TV,
                                         and many others, LTE networks
                                         will also provide the capacity to
                                         support an explosion in demand
                                         for connectivity from a new
                                         generation of consumer devices
                                         tailored to those new mobile
                                         applications.

M

MD5   Message Digest (Version 5)

M

MIB	Management Information Database
	A database of network management information that is used and maintained by the SNMP protocol.
MNP	Mobile Number Portability
	Allows a user to keep his or her mobile phone number despite changing provider. The subscriber also keeps the network carrier code.
MNP-SRF	MNP Signaling Relay Function
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. 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

N

NPDB

Number Portability Database

Database that holds ported numbers. Tekelec implementation is the Real Time Database (RTDB).

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.

OAMP

Operations, Administration, Maintenance and Provisioning

OID

Object Identifier

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

O

belong to different standard organizations. Vendors define private branches that include managed objects for their own products.

P

PDN

Packet Data Network

A digital network technology that divides a message into packets for transmission.

PM

Processing Module

R

RAS

REST Application Server

S

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.

SDM

Subscriber Data Management

SGSN

Serving GPRS Support Node

SIGTRAN

The name given to an IETF working group that produced specifications for a family of protocols that provide reliable

S

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.

SIM

Subscriber Identity Module

An ID card the size of a credit card for GSM network subscribers, and is typically referred to as a chip card or smartcard.

SIP

Session Initiation Protocol

A peer-to-peer protocol used for voice and video communications.

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.

S

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.
SRI	Send Routing Information
	Send_Route_Information Message
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 is an STP, which is a device that routes these messages through the network.
SSH	Secure Shell
	A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.
SSR	SIP Signaling Router

S

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 invoke features in another remote network switch.

TDP

Trigger Detection Point

U

UDP

User Datagram Protocol

USM

User Security Management

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

V

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.