Subscriber Data Management

Release 9.1

System Configuration User Guide

910-6698-001 Revision A

June 2013

Tekelec

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

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

About this document

This document describes how configure the Subscriber Data Management (SDM) applications using the Command Line Interface (CLI) or the Web Craft Interface (WebCI).

Scope and audience

Use this document to locate system configuration procedures. For detailed information about commands and parameters, refer to the *SDM System Configuration Reference Manual*.

This document is intended for 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 Customer Care Center, and how to locate the customer documentation on the Customer Support site.
- *Getting Started* contains information regarding safety precautions and how to begin using the Subscriber Database Management system.
- *User Interfaces* describes the user interfaces that allow the operator to configure the system or provision subscribers. The description includes functionalities, command convention, navigation method, command execution, and the GUI symbols used in the WebCI.
- *HLR Application Configuration* contains information pertaining to the configuration of the HLR application.
- *HLR Features Configuration* contains information pertaining to the configuration of HLR Features.
- *SIP Application Configuration* describes the configuration of the SIP application.
- *IMS-HSS/SLF Application Configuration* outlines the procedures to configure the IMS-HSS and SLF.
- *AAA Application Configuration* outlines the procedures to configure the AAA.
- *DNS Enum server configuration* describes the configuration of the DNS Enum server.
- *HSS/AAA Support for Early IMS Security Configuration* describes the configuration of the HSS/AAA Support for Early IMS Security.
- *LTE-HSS Application Configuration* outlines the procedures to configure the LTE-HSS.
- *EIR Application Configuration* provides the procedures to configure the Equipment Identity Register (EIR) through the WebCI.
- *LTE-EIR Application Configuration* provides the initial procedures on how to configure the LTE-EIR through the WebCI.

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

✋	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)
⚡	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
⚠	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Related publications

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

Customer Care Center

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

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

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

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

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

TAC Regional Support Office Hours:

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

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

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

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

  - **Argentina**

    Phone:

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

    Phone:

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

    TAC Regional Support Office Hours:

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

    Phone:

    1230-020-555-5468
  - **Colombia**

    Phone:

    01-800-912-0537
  - **Dominican Republic**

    Phone:

    1-888-367-8552
  - **Mexico**

    Phone:

    001-888-367-8552
  - **Peru**

    Phone:

    0800-53-087
  - **Puerto Rico**

    Phone:

    1-888-367-8552 (1-888-FOR-TKLC)
  - **Venezuela**

    Phone:

0800-176-6497

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

  Regional Office Hours:

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

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

Locate Product Documentation on the Customer Support Site

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

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

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

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

Chapter 2

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

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

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.

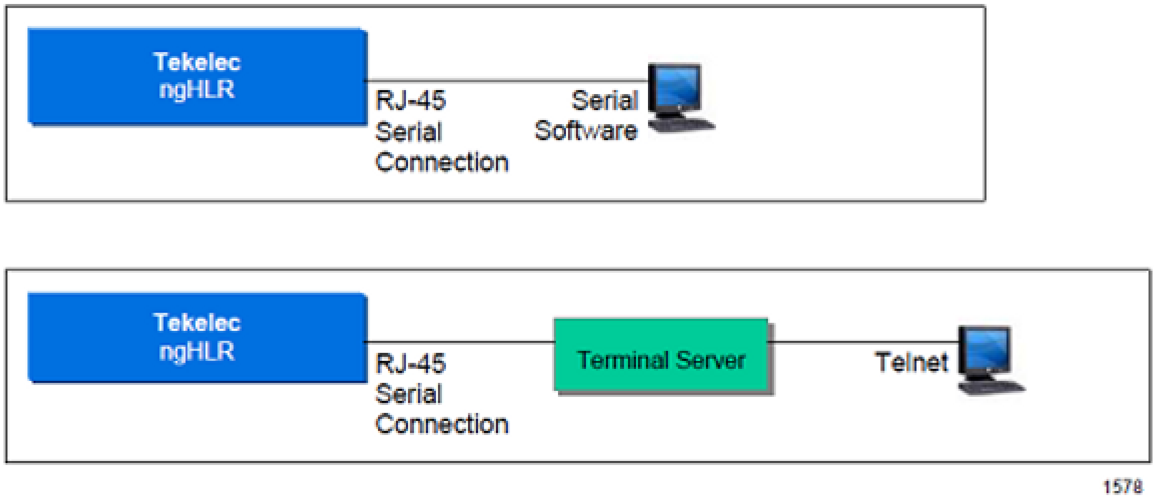
Establish serial connection

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.

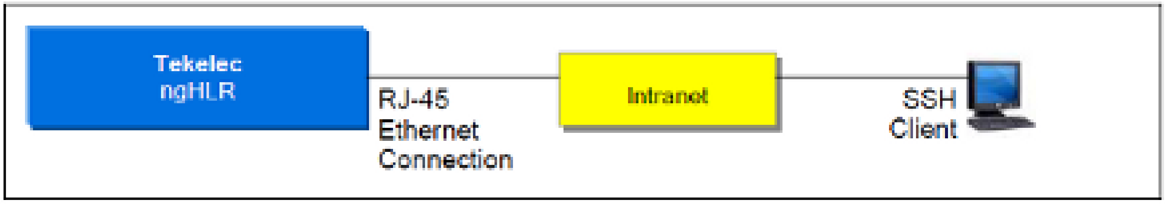


Establish Secure Shell (SSh) connection

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.

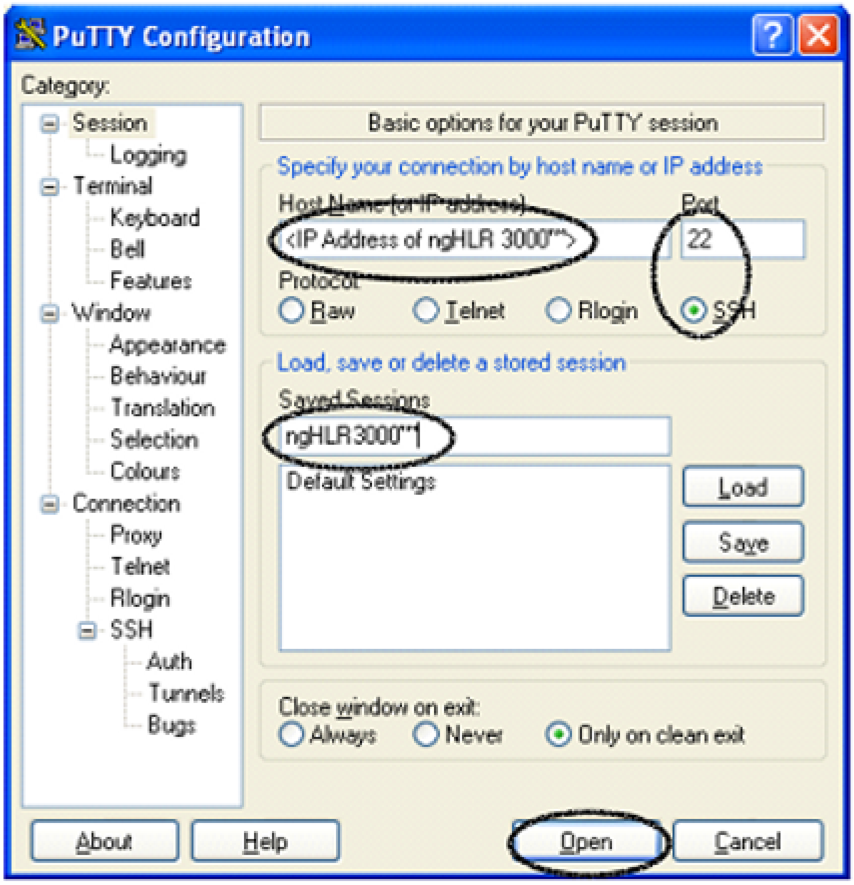


2. Connect other end of cable to PC or other terminal device running a terminal emulation program.
3. Start SSh client.

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.



Host Name (or IP address): <IP Address of ngHLR 3000**>

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions: ngHLR3000**

Close window on exit: ○ Always ○ Never ● Only on clean exit

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)

Chapter 3

User Interfaces

Topics:

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

Command Line Interface (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:

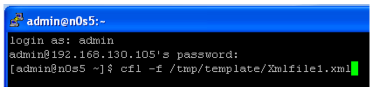
Table 3: Pre-defined users

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
```



```
login as: admin
admin@192.168.130.105's password:
[admin@n0s5 ~]$ cfl -f /tmp/template/Xmlfile1.xml
```

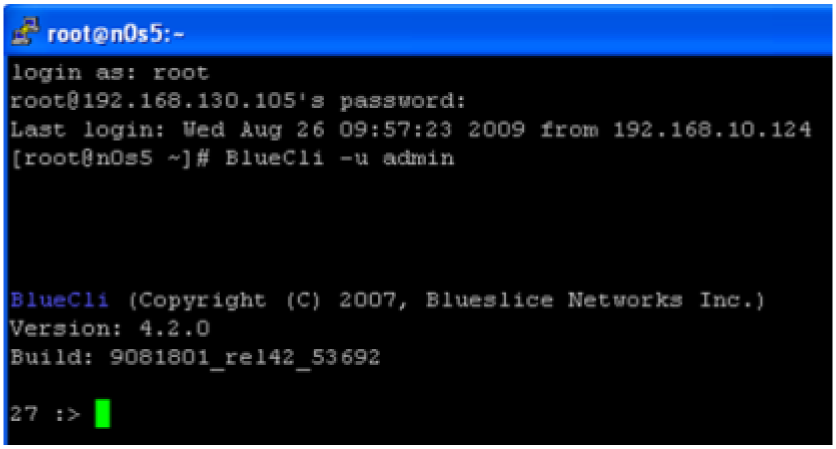
After starting a CLI session for the first time, and with the user having changed its own password or as per the operator's convenience, with the administrator having changed the users' password, the user now accesses the system with its UserName and new password. Refer to *Creating and Managing Users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



root@n0s5:~

```
login as: root
root@192.168.130.105's password:
Last login: Wed Aug 26 09:57:23 2009 from 192.168.10.124
[root@n0s5 ~]# BlueCli -u admin



BlueCli (Copyright (C) 2007, Blueslice Networks Inc.)
Version: 4.2.0
Build: 9081801_rel42_53692

27 :>
```

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.

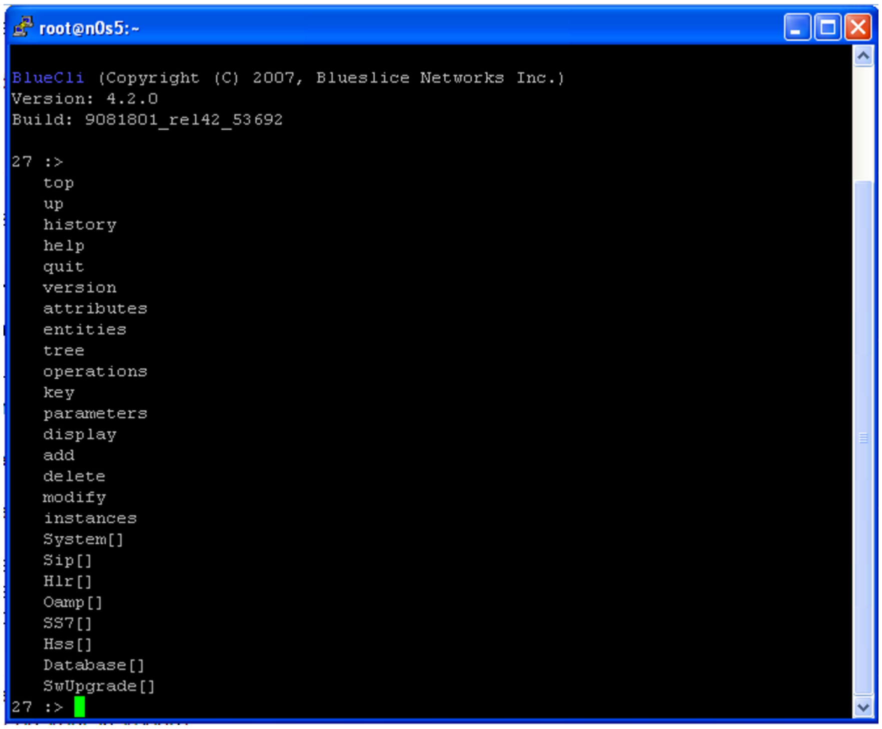
Steps to Navigate and Perform Operations on Entities from the CLI

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.



```
BlueCli (Copyright (C) 2007, Blueslice Networks Inc.)
Version: 4.2.0
Build: 9081801_rel42_53692

27 :>
   top
   up
   history
   help
   quit
   version
   attributes
   entities
   tree
   operations
   key
   parameters
   display
   add
   delete
   modify
   instances
   System[]
   Sip[]
   Hlr[]
   Oamp[]
   SS7[]
   Hss[]
   Database[]
   SwUpgrade[]
27 :>
```

Figure 3: CLI subsystems

The following SDM subsystems can be accessed:

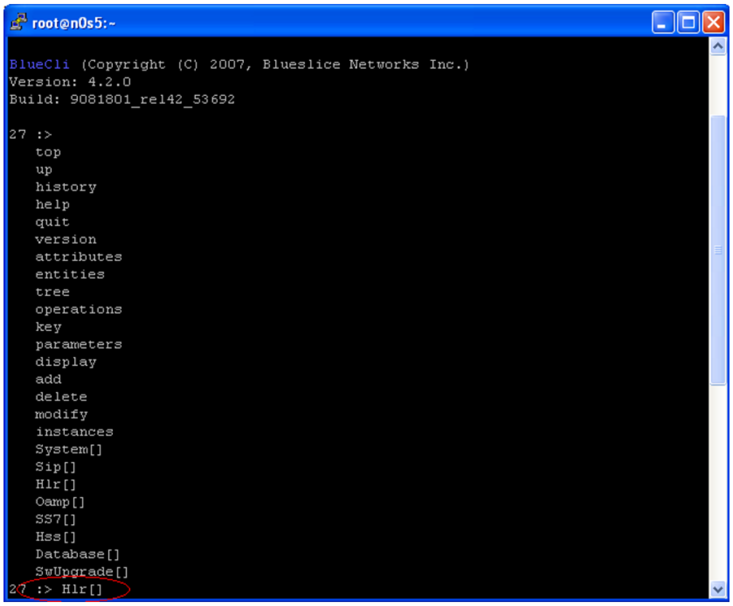
Table 4: Accessing subsystems through CLI

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[]`

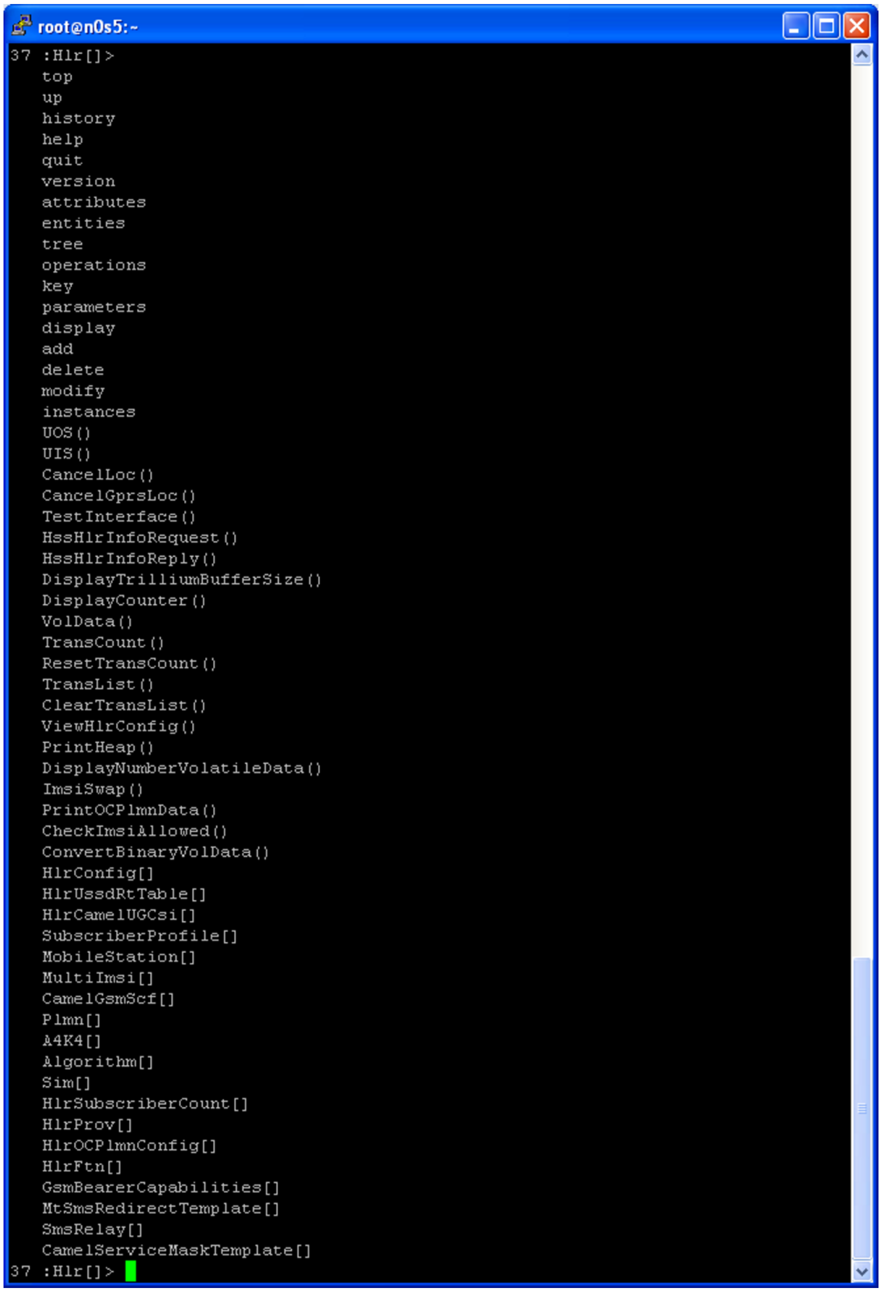


```
BlueCli (Copyright (C) 2007, Blueslice Networks Inc.)
Version: 4.2.0
Build: 9081801_rel42_53692

27 :>
   top
   up
   history
   help
   quit
   version
   attributes
   entities
   tree
   operations
   key
   parameters
   display
   add
   delete
   modify
   instances
   System[]
   Sip[]
   Hlr[]
   Oamp[]
   SS7[]
   Hss[]
   Database[]
   SwUpgrade[]
27 :> 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.



```
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

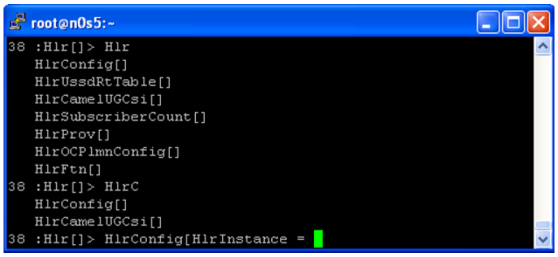
Command	Definition
`delete`	Deletes instances from the system
`display`	Display the instances
`entities`	Show sub-entities
`help`	Display help options
`history`	Lists history of commands
`instances`	Display all instances of an entity
`key`	Show navigation key attributes
`modify`	Make changes to instances
`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.



```
38 :Hlr[]> Hlr
   HlrConfig[]
   HlrUssdRtTable[]
   HlrCamelUGCsi[]
   HlrSubscriberCount[]
   HlrProv[]
   HlrOCPlmnConfig[]
   HlrFtn[]
38 :Hlr[]> HlrC
   HlrConfig[]
   HlrCamelUGCsi[]
38 :Hlr[]> HlrConfig[HlrInstance = 
```

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:

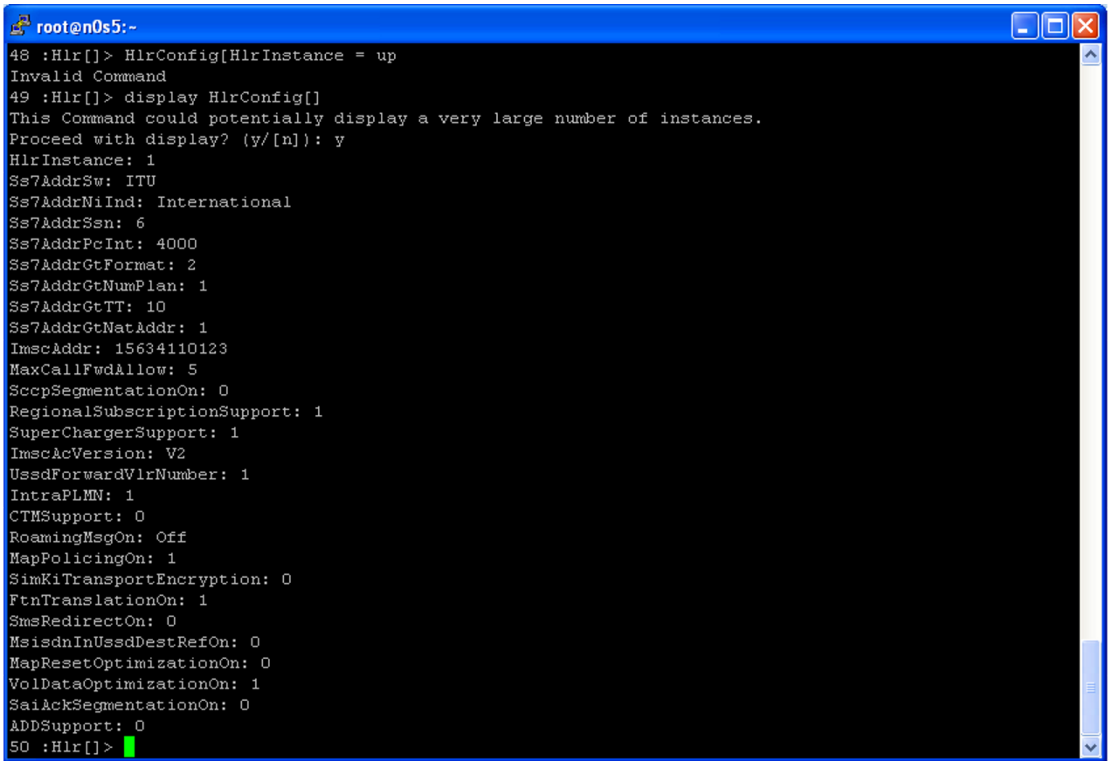
a) Type the UNIX command `UP` to go back to the next higher level, for example, the HLR subsystem level.

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.



```
48 :Hlr[]> HlrConfig[HlrInstance = up
Invalid Command
49 :Hlr[]> display HlrConfig[]
This Command could potentially display a very large number of instances.
Proceed with display? (y/[n]): y
HlrInstance: 1
Ss7AddrSw: ITU
Ss7AddrNiInd: International
Ss7AddrSsn: 6
Ss7AddrPcInt: 4000
Ss7AddrGtFormat: 2
Ss7AddrGtNumPlan: 1
Ss7AddrGtTT: 10
Ss7AddrGtNatAddr: 1
ImscAddr: 15634110123
MaxCallFwdAllow: 5
SccpSegmentationOn: 0
RegionalSubscriptionSupport: 1
SuperChargerSupport: 1
ImscAcVersion: V2
UssdForwardVlrNumber: 1
IntraPLMN: 1
CTMSupport: 0
RoamingMsgOn: Off
MapPolicingOn: 1
SimKiTransportEncryption: 0
FtnTranslationOn: 1
SmsRedirectOn: 0
MsisdnInUssdDestRefOn: 0
MapResetOptimizationOn: 0
VolDataOptimizationOn: 1
SaiAckSegmentationOn: 0
ADDSupport: 0
50 :Hlr[]>
```

e) Type the value of the mandatory attribute.

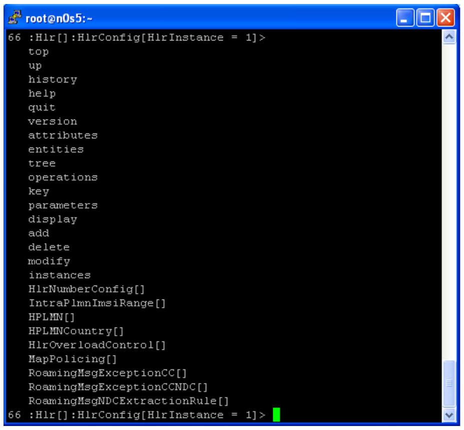
8. Type a semicolon after the mandatory attribute and press <TAB> twice.

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 above.



root@n0s5:~

```
66 :Hlr[]:HlrConfig[HlrInstance = 1]>
   top
   up
   history
   help
   quit
   version
   attributes
   entities
   tree
   operations
   key
   parameters
   display
   add
   delete
   modify
   instances
   HlrNumberConfig[]
   IntraPlmnImsiRange[]
   HPLMN[]
   HPLMNCountry[]
   HlrOverloadControl[]
   MapPolicing[]
   RoamingMsgExceptionCC[]
   RoamingMsgExceptionCCNDC[]
   RoamingMsgNDCExtractionRule[]
66 :Hlr[]:HlrConfig[HlrInstance = 1]>
```

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

At this point, you can do 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
`<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.

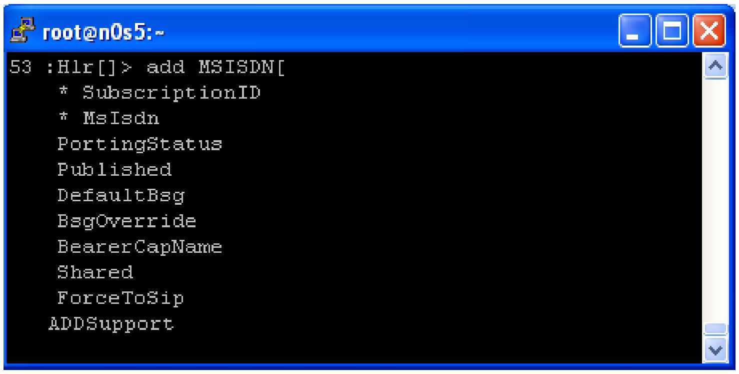
Table 8: CLI characters

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 (*).



```
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

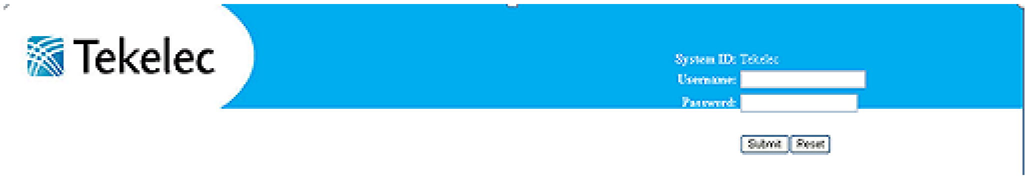
To access the Web Craft Interface (WebCI), enter the following URL in the web browser:

```
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

User	Default UserName	Default UserPasswd	Group Name
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.

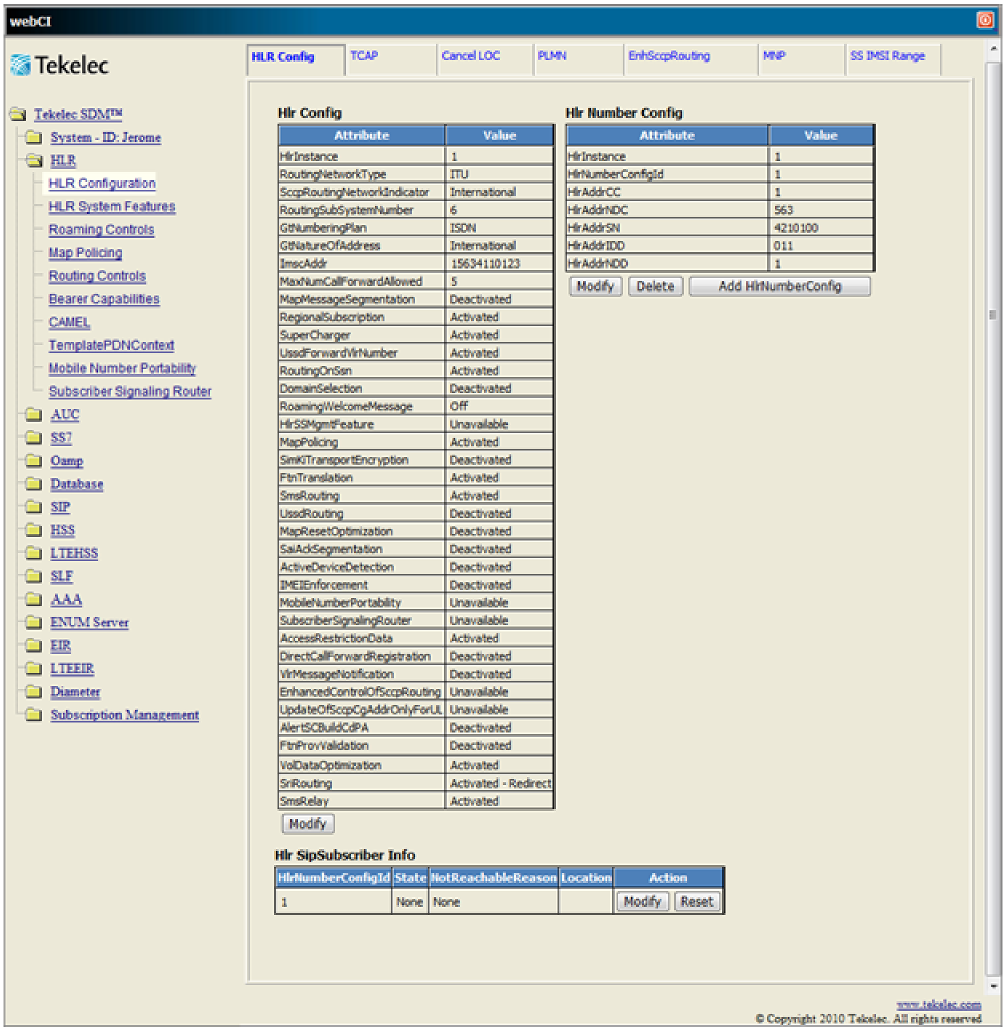
Displaying a WebCI window

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.



Hlr Config

Attribute	Value
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
HlrSSMgmtFeature	Unavailable
MapPolicing	Activated
SimKiTransportEncryption	Deactivated
FtnTranslation	Activated
SmsRouting	Activated
UssdRouting	Deactivated
MapResetOptimization	Deactivated
SaiAckSegmentation	Deactivated
ActiveDeviceDetection	Deactivated
IMEIEnforcement	Deactivated
MobileNumberPortability	Unavailable
SubscriberSignalingRouter	Unavailable
AccessRestrictionData	Activated
DirectCallForwardRegistration	Deactivated
VlrMessageNotification	Deactivated
EnhancedControlOfSccpRouting	Unavailable
UpdateOfSccpCgAddrOnlyForUL	Unavailable
AlertSCBuildCdPA	Deactivated
FtnProvValidation	Deactivated
VolDataOptimization	Activated
SriRouting	Activated - Redirect
SmsRelay	Activated

Hlr Number Config

Attribute	Value
HlrInstance	1
HlrNumberConfigId	1
HlrAddrCC	1
HlrAddrNDC	563
HlrAddrSN	4210100
HlrAddrIDD	011
HlrAddrNDD	1

Hlr SipSubscriber Info

HlrNumberConfigId	State	NotReachableReason	Location	Action
1	None	None		Modify Reset

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.

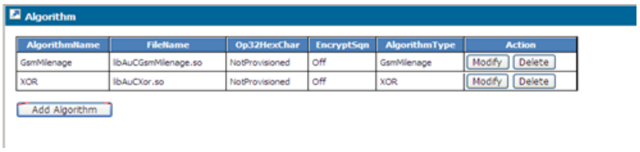
  For information on all the different symbols displayed in the WebCI, refer to the "Operations available" section of the "Web Craft Interface (WebCI)" chapter in the *SDM System Configuration – Reference Manual* .

  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.



AlgorithmName	FileName	Op32HexChar	EncryptSqn	AlgorithmType	Action
GsmMilenage	libAuCGsmMilenage.so	NotProvisioned	Off	GsmMilenage	Modify Delete
XOR	libAuCXor.so	NotProvisioned	Off	XOR	Modify Delete

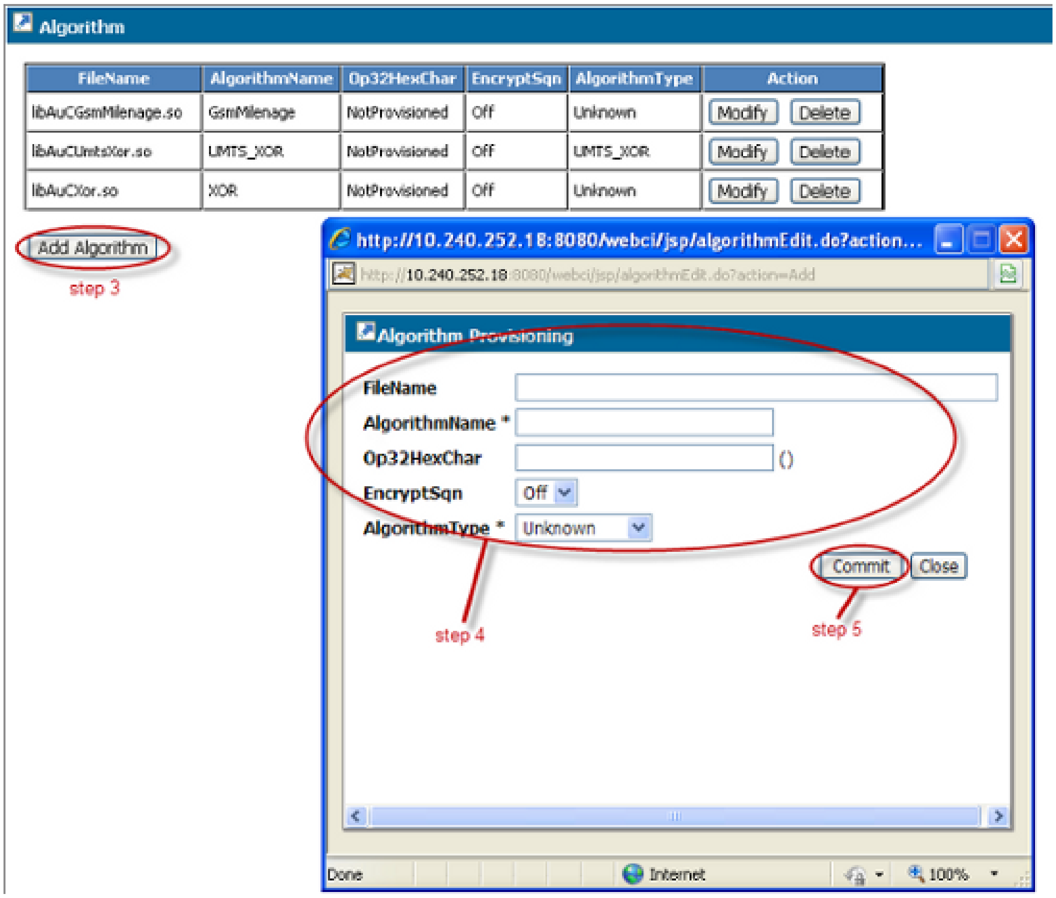
Add an entry - AuC Algorithm

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.



Algorithm

FileName	AlgorithmName	Op32HexChar	EncryptSqn	AlgorithmType	Action
libAuCGsmMilenage.so	GsmMilenage	NotProvisioned	Off	Unknown	Modify Delete
libAuCUmtsXor.so	UMTS_XOR	NotProvisioned	Off	UMTS_XOR	Modify Delete
libAuCXor.so	XOR	NotProvisioned	Off	Unknown	Modify Delete

Algorithm Provisioning

FileName

AlgorithmName *

Op32HexChar ()

EncryptSqn Off

AlgorithmType * Unknown

Add Algorithm
step 3
http://10.240.252.18:8080/webci/jsp/algorithmEdit.do?action...
http://10.240.252.18:8080/webci/jsp/algorithmEdit.do?action=Add
Commit
Close
step 4
step 5
Done
Internet
100%

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

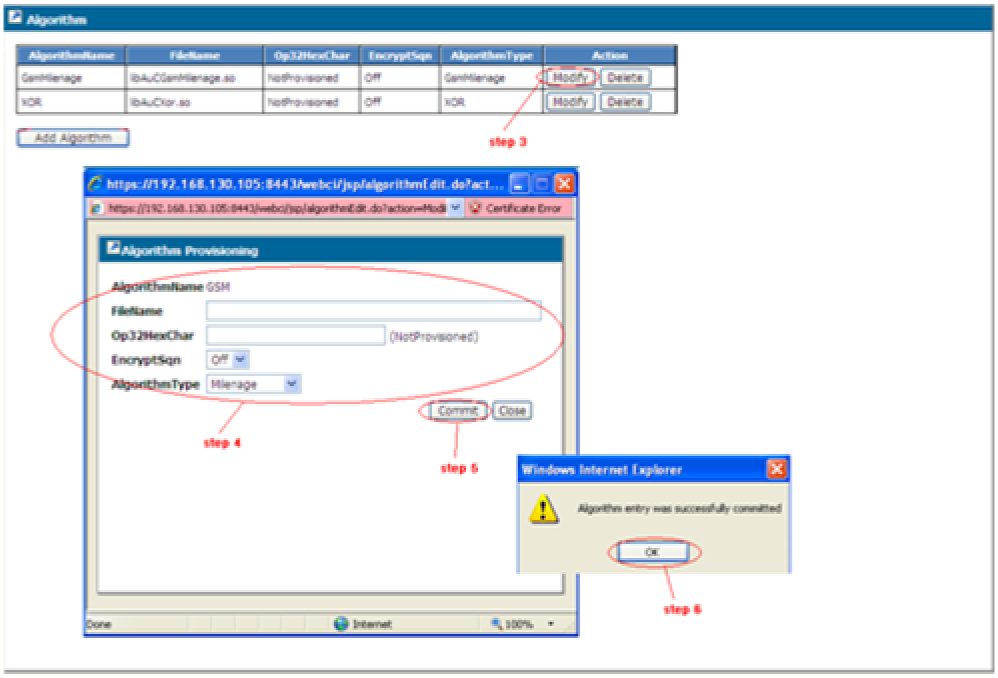
This procedure describes how to modify a table entry by using the Authentication (AuC) algorithm files as an example.

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.



Algorithm

AlgorithmName	FileName	Op32HexChar	EncryptSqn	AlgorithmType	Action
GsmMilenage	libAuCGsmMilenage.so	NotProvisioned	Off	GsmMilenage	Modify Delete
XOR	libAuCXor.so	NotProvisioned	Off	XOR	Modify Delete

https://192.168.130.105:8443/webci/jsp/algorithmEdit.do?action=Modi

Algorithm Provisioning

AlgorithmName GSM
FileName
Op32HexChar (NotProvisioned)
EncryptSqn Off
AlgorithmType Milenage

Windows Internet Explorer

Algorithm entry was successfully committed

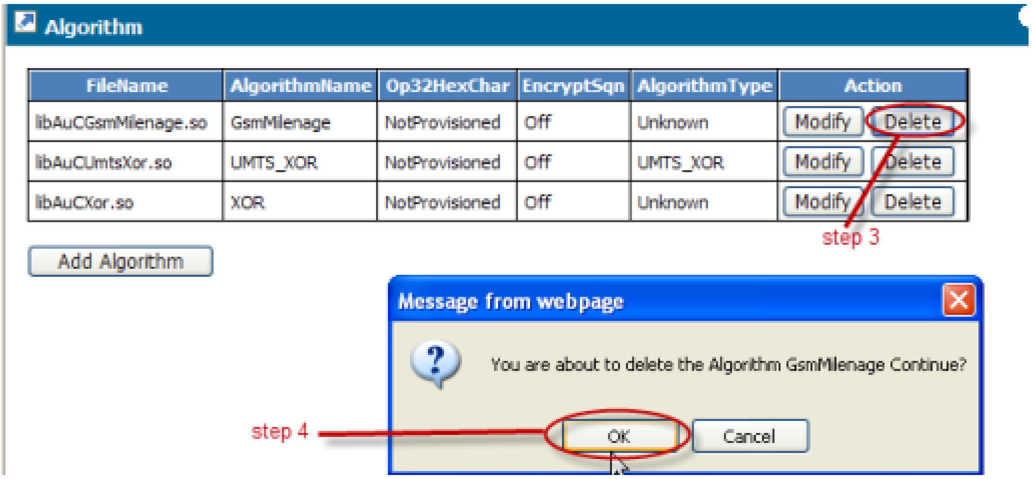
3. Click the **Modify** button next to the algorithm to be modified.
   A provisioning pop-up window opens, for example, *Algorithm Provisioning*.
4. Modify the required information.
5. Click **Commit**.
   The system returns a confirmation message:
   ```
   Algorithm entry was successfully committed
   ```
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.



FileName	AlgorithmName	Op32HexChar	EncryptSqn	AlgorithmType	Action
libAuCGsmMilenage.so	GsmMilenage	NotProvisioned	Off	Unknown	Modify Delete
libAuCUmtsXor.so	UMTS_XOR	NotProvisioned	Off	UMTS_XOR	Modify Delete
libAuCXor.so	XOR	NotProvisioned	Off	Unknown	Modify Delete

You are about to delete the Algorithm GsmMilenage Continue?

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.

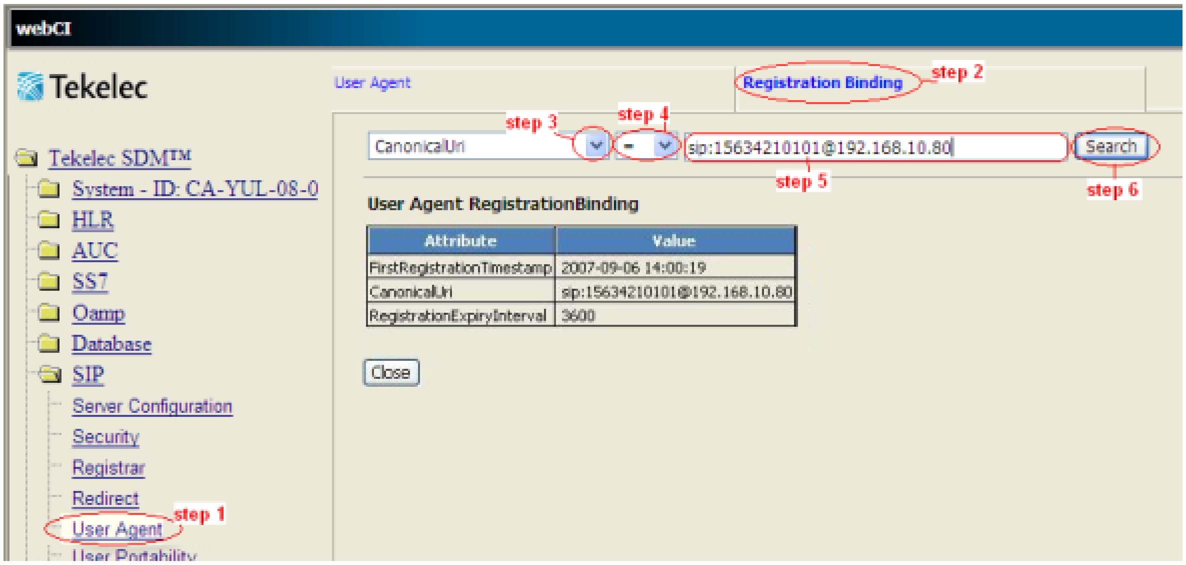
The procedure hereunder is an example of the steps to follow in order to display the SIP User Agent RegistrationBinding table using the WebCI's search engine. The logic used in this procedure can be used for any WebCI window that requires the search engine to be used in order to display its content.

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**.



CanonicalUri = sip:15634210101@192.168.10.80

User Agent RegistrationBinding

Attribute	Value
FirstRegistrationTimestamp	2007-09-06 14:00:19
CanonicalUri	sip:15634210101@192.168.10.80
RegistrationExpiryInterval	3600

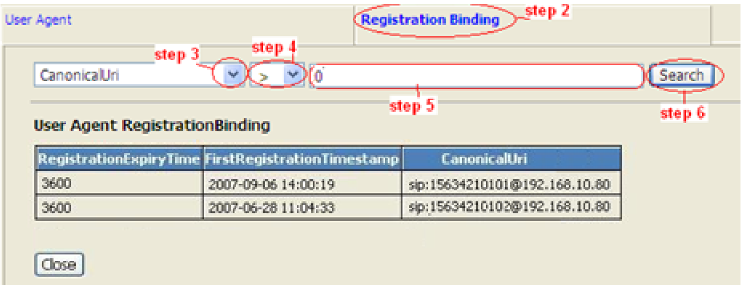
3. Click the **UaRegistrationBinding** tab.
4. Select one of the following RegistrationBinding attributes from the first drop-down menu:

```
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.



CanonicalUri > 0

User Agent RegistrationBinding

RegistrationExpiryTime	FirstRegistrationTimestamp	CanonicalUri
3600	2007-09-06 14:00:19	sip:15634210101@192.168.10.80
3600	2007-06-28 11:04:33	sip:15634210102@192.168.10.80

The search results display the User Agent RegistrationBinding table with one or more RegistrationBindings.

Ending a WebCI session

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

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.

Table 11: Access Privileges 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	**WebCI**
SecurityAccessPrivileges table	**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 *Customer Care Center* 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

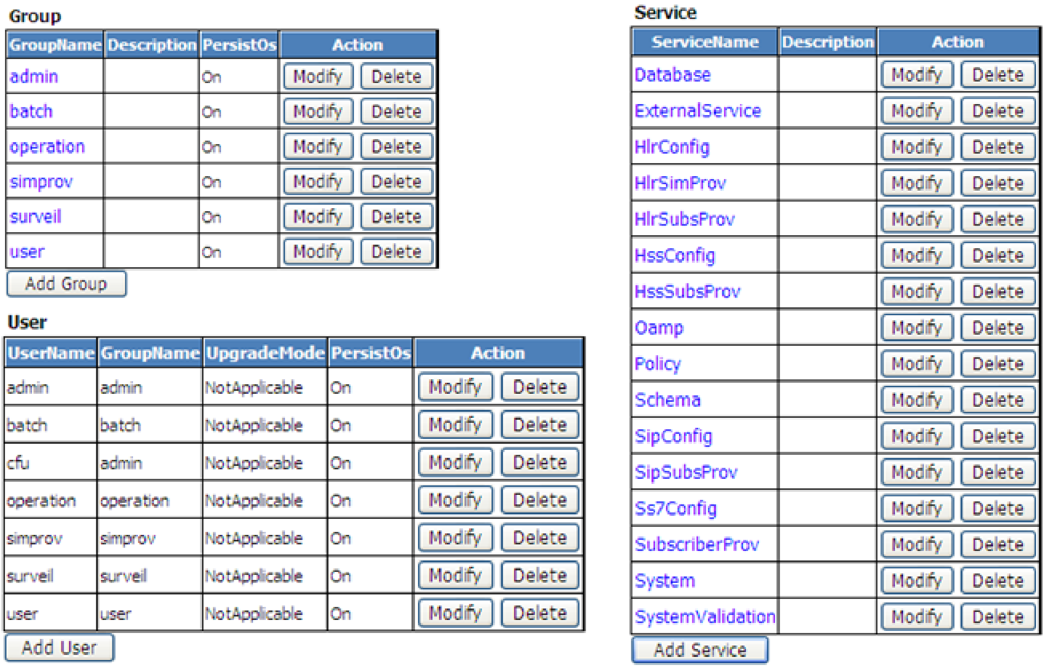
View all User Management Information from the WebCI

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.



Group

GroupName	Description	PersistOs	Action
admin		On	Modify Delete
batch		On	Modify Delete
operation		On	Modify Delete
simprov		On	Modify Delete
surveil		On	Modify Delete
user		On	Modify Delete

User

UserName	GroupName	UpgradeMode	PersistOs	Action
admin	admin	NotApplicable	On	Modify Delete
batch	batch	NotApplicable	On	Modify Delete
cfu	admin	NotApplicable	On	Modify Delete
operation	operation	NotApplicable	On	Modify Delete
simprov	simprov	NotApplicable	On	Modify Delete
surveil	surveil	NotApplicable	On	Modify Delete
user	user	NotApplicable	On	Modify Delete

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

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 the User table using CLI

This section provides the CLI procedures to create, display, and delete users from the User table.

- Creating user
- Displaying user
- Modifying user

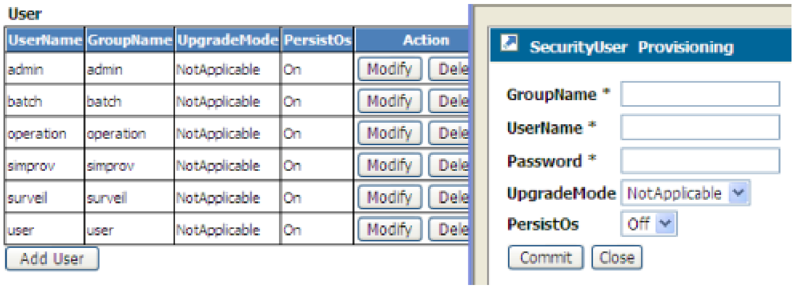
Creating User from the WebCI

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.



User

UserName	GroupName	UpgradeMode	PersistOs	Action
admin	admin	NotApplicable	On	Modify Dele
batch	batch	NotApplicable	On	Modify Dele
operation	operation	NotApplicable	On	Modify Dele
simprov	simprov	NotApplicable	On	Modify Dele
surveil	surveil	NotApplicable	On	Modify Dele
user	user	NotApplicable	On	Modify Dele

SecurityUser Provisioning

GroupName *

UserName *

Password *

UpgradeMode NotApplicable

PersistOs Off

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

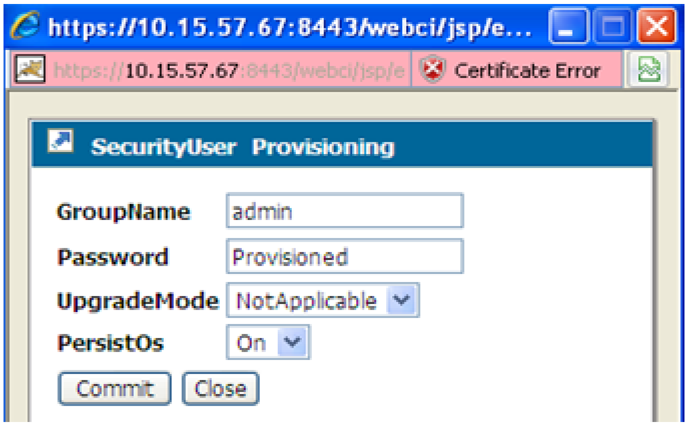
Each user can modify its own password by modifying the User[ ] entity and entering the value of the new password desired. However, only the administrator of the system can modify the following:

- 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.



https://10.15.57.67:8443/webci/jsp/e...
https://10.15.57.67:8443/webci/jsp/e
Certificate Error

SecurityUser Provisioning

GroupName admin

Password Provisioned

UpgradeMode NotApplicable

PersistOs On

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 from the WebCI

By default, six groups are defined in the system: user, operation, surveil, admin, batch, simprov. The groups can be viewed by all users, but the administrator of the system is the only one that can add/modify/delete groups.

This section outlines the procedures to display the Group entity. For details on this table, refer to the “User Management through CLI” section of the *SDM System Configuration - Reference Manual* . To perform the tasks in the following list, refer to the procedure for the step by step instructions.

- Displaying groups
- Creating groups
- Modifying groups
- Deleting groups

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

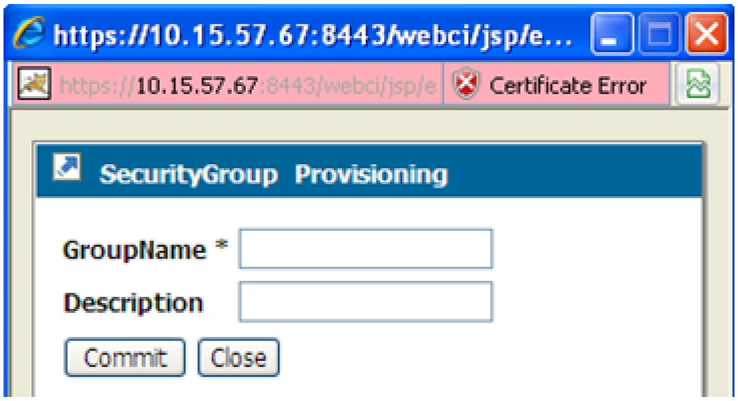
This procedure creates a group and defines access privileges by provisioning permissions for each service.

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.


https://10.15.57.67:8443/webci/jsp/e...
https://10.15.57.67:8443/webci/jsp/e
Certificate Error
SecurityGroup Provisioning
GroupName *
Description
Commit
Close

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.

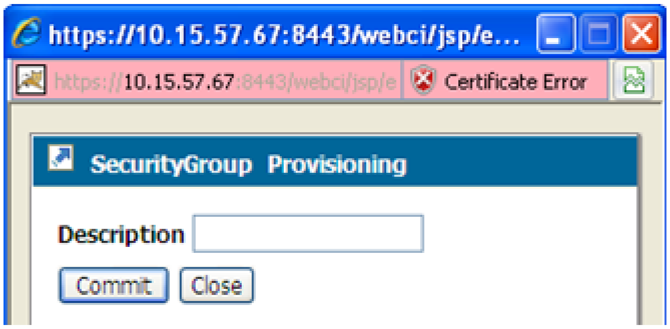

https://10.15.57.67:8443/webci/jsp/e...
https://10.15.57.67:8443/webci/jsp/e
Certificate Error
SecurityGroup Provisioning
Description
Commit
Close

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

Each of the following six groups has predefined access privileges for specific services: user, admin, surveillance, batch, operation and simprov.

Each access privilege gives a single group the privilege to access a single service, which has predefined permissions (read, write, execute). Each service groups entities by functionalities. All services are predefined in the system and cannot be created or modified. Only the administrator can modify the AccessPrivileges table.

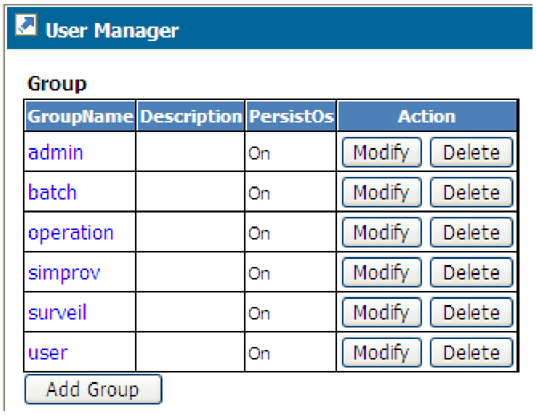
These procedures provision access privileges:

- Display Access Privileges
- Modify Access Privileges
- Display All Groups from the AccessPrivileges table

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.

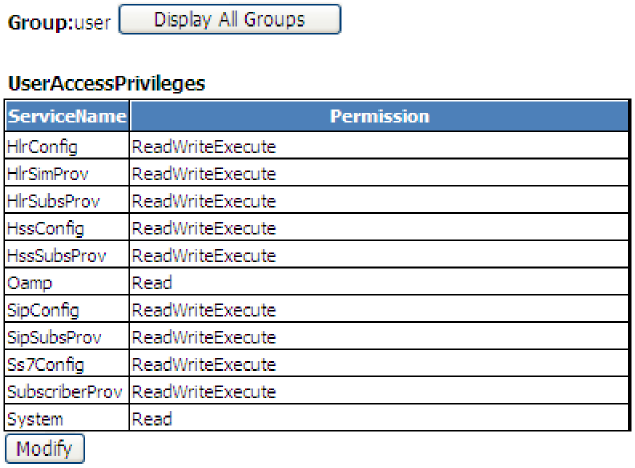


User Manager

Group

GroupName	Description	PersistOs	Action
admin		On	Modify Delete
batch		On	Modify Delete
operation		On	Modify Delete
simprov		On	Modify Delete
surveil		On	Modify Delete
user		On	Modify Delete

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.



Group:user

UserAccessPrivileges

ServiceName	Permission
HlrConfig	ReadWriteExecute
HlrSimProv	ReadWriteExecute
HlrSubsProv	ReadWriteExecute
HssConfig	ReadWriteExecute
HssSubsProv	ReadWriteExecute
Oamp	Read
SipConfig	ReadWriteExecute
SipSubsProv	ReadWriteExecute
Ss7Config	ReadWriteExecute
SubscriberProv	ReadWriteExecute
System	Read

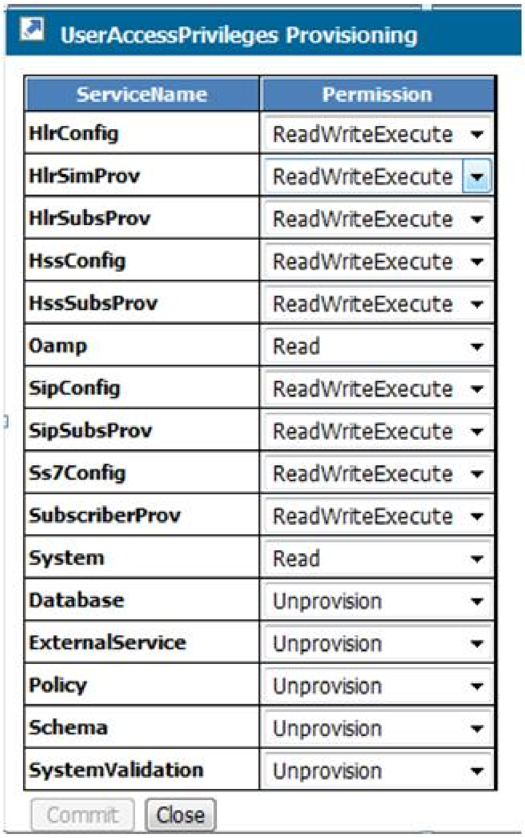
3. Click **Display All Groups** to return to the User Manager window.

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.



UserAccessPrivileges Provisioning

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.

Display all groups from the AccessPrivileges table in the WebCI

This procedure describes the steps to go back to the Groups/Users main window from the AccessPrivileges table and display all Groups in the Group table. For details on the Group Management attributes, refer to the "User Management through CLI" section of the *SDM System Configuration - Reference Manual* .

From the User Manager window displaying the AccessPrivileges table, click on the **Display All Groups** button beside the GroupName.

(see above).

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 *Customer Care Center* for assistance).

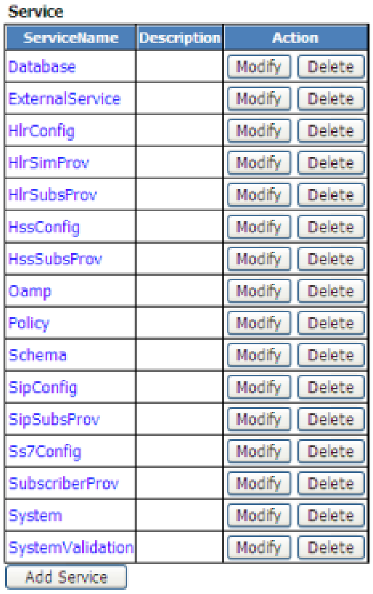
The system administrator can then

- 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*.

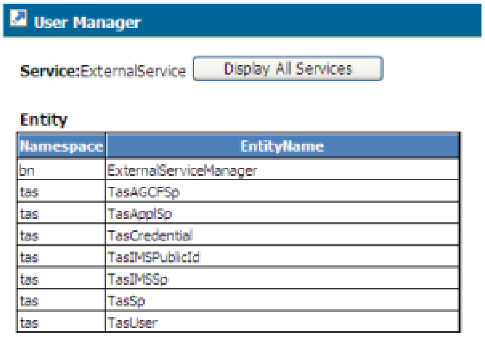
1. From the main menu, navigate to **Oamp ➤ User Manager**
   The User Manager window displays including the Services table. The Service table displays all the services defined in the system.



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

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



Service:ExternalService

Entity

Namespace	EntityName
bn	ExternalServiceManager
tas	TasAGCFSp
tas	TasApplSp
tas	TasCredential
tas	TasIMSPublicId
tas	TasIMSSp
tas	TasSp
tas	TasUser

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).

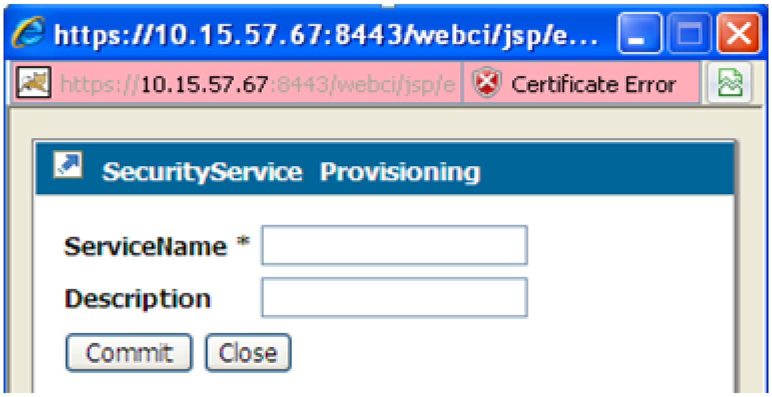

https://10.15.57.67:8443/webci/jsp/e...
https://10.15.57.67:8443/webci/jsp/e
Certificate Error
SecurityService Provisioning
ServiceName *
Description
Commit
Close

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 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 user/application combinations

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

Table 14: 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 login options.

For an external application to subscribe to notifications for specific applications, entities, or attributes, the application must have a user account defined by the SDM system administrator. The user account defined in the User[ ] entity contains the username, password, and application name (from the user/application association defined in the UserApplicationMap[ ] entity.

Note: The application must have been pre-defined in the ApplicationIdentity[ ] entity.

Depending on the user interface used, the following procedures define users and associate them to applications by provisioning the UserApplicationMap table.

Users can only create and display the User table, modify user passwords, and assign a group to each user.

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

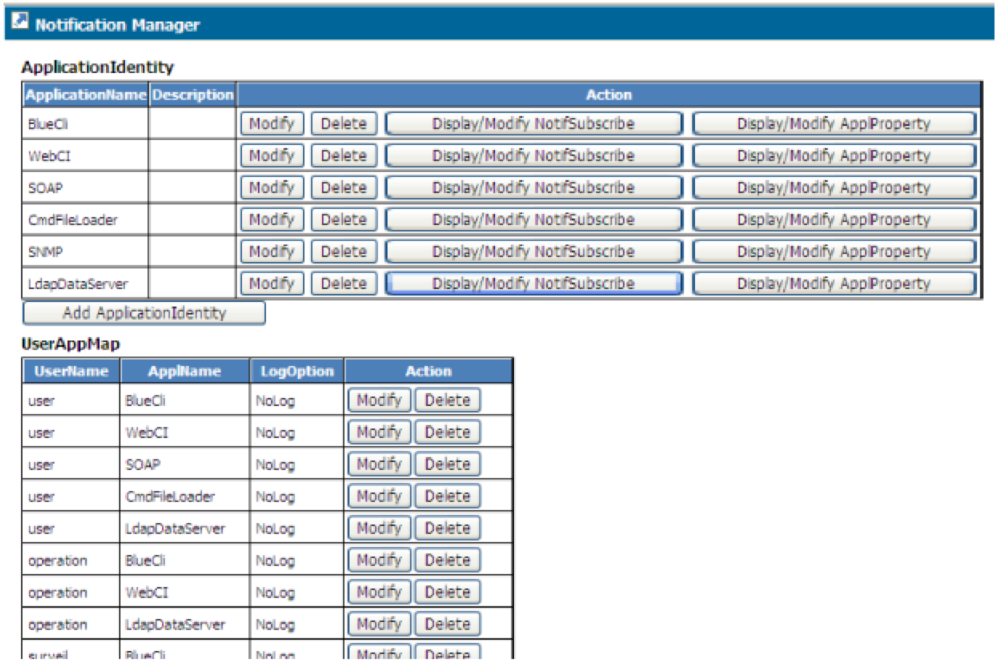
Requirements: All WebCI provisioning procedures require the operator to log into a WebCI session with a valid username and password.

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.



Notification Manager

ApplicationIdentity

ApplicationName	Description	Action			
BlueCli		Modify	Delete	Display/Modify NotifSubscribe	Display/Modify ApplProperty
WebCI		Modify	Delete	Display/Modify NotifSubscribe	Display/Modify ApplProperty
SOAP		Modify	Delete	Display/Modify NotifSubscribe	Display/Modify ApplProperty
CmdFileLoader		Modify	Delete	Display/Modify NotifSubscribe	Display/Modify ApplProperty
SNMP		Modify	Delete	Display/Modify NotifSubscribe	Display/Modify ApplProperty
LdapDataServer		Modify	Delete	Display/Modify NotifSubscribe	Display/Modify ApplProperty

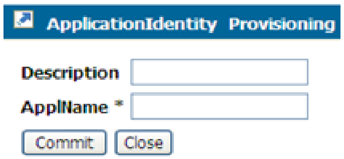
UserAppMap

UserName	ApplName	LogOption	Action	
user	BlueCli	NoLog	Modify	Delete
user	WebCI	NoLog	Modify	Delete
user	SOAP	NoLog	Modify	Delete
user	CmdFileLoader	NoLog	Modify	Delete
user	LdapDataServer	NoLog	Modify	Delete
operation	BlueCli	NoLog	Modify	Delete
operation	WebCI	NoLog	Modify	Delete
operation	LdapDataServer	NoLog	Modify	Delete
surveil	BlueCli	NoLog	Modify	Delete

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.



ApplicationIdentity Provisioning

Description	
ApplName *	

Figure 13: ApplicationIdentity Provisioning Window to Create Applications

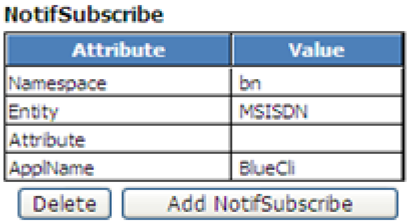
4. Click **Commit** when all the information has been entered.
5. When the confirmation message "`Entity entry was successfully committed`" appears, click **OK**.

--- 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.



NotifSubscribe

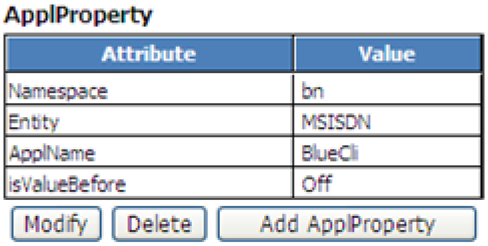
Attribute	Value
Namespace	bn
Entity	MSISDN
Attribute	
ApplName	BlueCli

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.

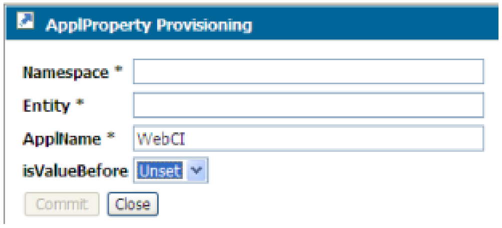


ApplProperty

Attribute	Value
Namespace	bn
Entity	MSISDN
ApplName	BlueCli
isValueBefore	Off

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

- 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 15: 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*.

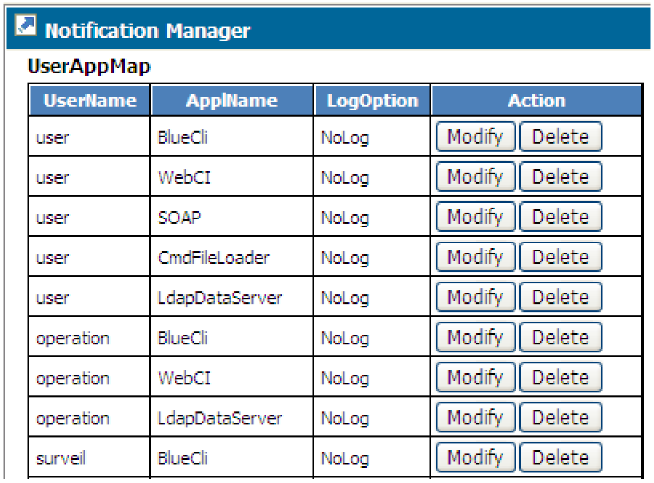
WebCI	**CLI**
Creating user	Provisioning users
Modifying user	
Deleting user	

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.

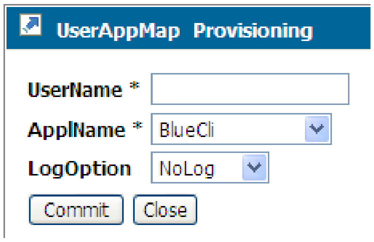


UserAppMap

UserName	ApplName	LogOption	Action
user	BlueCli	NoLog	Modify Delete
user	WebCI	NoLog	Modify Delete
user	SOAP	NoLog	Modify Delete
user	CmdFileLoader	NoLog	Modify Delete
user	LdapDataServer	NoLog	Modify Delete
operation	BlueCli	NoLog	Modify Delete
operation	WebCI	NoLog	Modify Delete
operation	LdapDataServer	NoLog	Modify Delete
surveil	BlueCli	NoLog	Modify Delete

2. Perform one of the following operations:
   - Click **Add UserAppMap** to add a new user/application combination.

     The UserAppMap Provisioning pop-up window opens.



UserAppMap Provisioning

UserName *

ApplName * BlueCli

LogOption NoLog

- 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

HLR Application Configuration

Topics:

This chapter contains information pertaining to the configuration of the HLR application.

A4K4 Transport Encryption Algorithm

The Tekelec AuC provisioning system supports the A4 Transport Encryption Algorithms and K4 Transport keys. This authentication algorithm can be used if the security needs to be increased. Refer to the "A4/K4 Transport Encryption Algorithm" section of the *SDM Product Description* for a more detailed description of this algorithm and the implementation in the Tekelec ngHLR.

Configuring A4/K4 Transport Encryption Algorithm

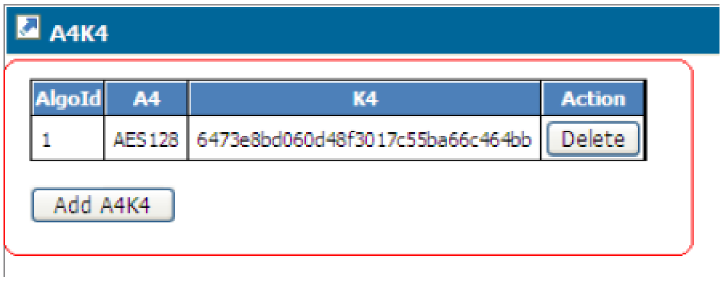
Configure the A4/K4 table using the WebCI.

- The A4/KA Transport Encryption Algorithm feature must be enabled using the SimKiTransportEncryption parameter in the HlrConfig table. Refer to the *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* section of this document.

The Tekelec ngHLR performs authentication with the data entered in the A4K4 table. The Tekelec AuC provisioning system supports the A4 Transport Encryption Algorithms and K4 Transport keys. This authentication algorithm can be used if the security needs to be increased. Refer to the “A4/K4 Transport Encryption Algorithm” section of the *SDM Product Description* for a more detailed description of this algorithm and the implementation in the Tekelec ngHLR.

Use the WebCI interface to configure the Tekelec ngHLR with the A4/K4 Transport Encryption Algorithm.

1. Go to **AUC>A4K4**



AlgoId	A4	K4	Action
1	AES128	6473e8bd060d48f3017c55ba66c464bb	Delete

Figure 14: AUC A4K4 Window

2. Provision the Algorithm table using one of these options:

   - **Add** a A4K4 entry.
   - **Delete**one entry at a time.

     Note:

     - Prior to deleting an A4K4 table entry, ensure that the SIM configuration is not referring to the AlgoId of the A4/K4 entry you wish to delete.
     - All SIM entries that refer to the A4K4 entry you wish to delete must first be modified (AlgoId parameter must be changed) or deleted to remove this reference

Note: Once the K4 key has been provisioned in the Tekelec ngHLR, it is encrypted with A7/K7 before being stored in the database. A7 is a proprietary algorithm and K7 is hard-coded. Hence, the K4 key displayed by the WebCI appears encrypted and longer.

Configuring the AuC

Configure the Algorithm table using the WebCI.

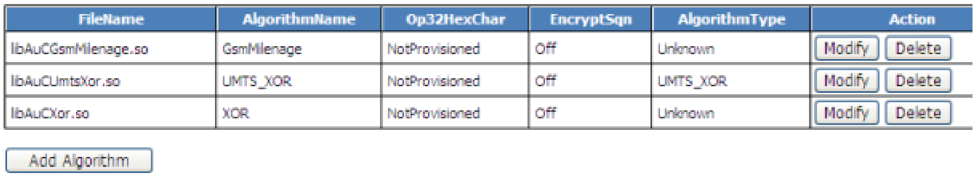
- The new algorithm file must be stored in the /blue/lib directory prior to running this procedure and it must have a so file extension (.so). This is usually done by Tekelec's Technical Support Team at installation.
- Prior to deleting an Algorithm entry, ensure that no SIM configuration is referring to the AlgorithmName of the Algorithm entry you wish to delete.

The Authentication Center (AuC) is used to provide authentication and radio link privacy to users on the GSM and UMTS networks. The Authentication Center supports XOR, UMTS_XOR, Comp128, Gsm Milenage and Milenage algorithms.

All SIM entries that refer to the AlgorithmName of the algorithm entry you wish to delete must first be modified (AlgorithmName table parameter must be changed) or deleted to remove this reference.

1. Go to **AUC>Algorithm**

   Figure 15: AUC Algorithm Window

FileName	AlgorithmName	Op32HexChar	EncryptSqn	AlgorithmType	Action
libAuCGsmMilenage.so	GsmMilenage	NotProvisioned	Off	Unknown	Modify Delete
libAuCUmtsXor.so	UMTS_XOR	NotProvisioned	Off	UMTS_XOR	Modify Delete
libAuCXor.so	XOR	NotProvisioned	Off	Unknown	Modify Delete

2. Provision the Algorithm table using one of these options:

   - **Add** an algorithm.
   - **Delete**one entry at a time.
   - **Modify**one entry at a time.

   Note:

   - The AlgorithmType attribute cannot be modified from Unknown, XOR, Comp128, GsmMilenage, UMTS_XOR to Milenage. However, it can be modified between the five values Unknown, XOR, UMTS_XOR, Comp128 and GsmMilenage.
   - If the AlgorithmType attribute is created as Milenage, it cannot be modified, it must be deleted and recreated.
   - Be careful when modifying the FileName attribute to make sure the library is matching the AlgorithmType

Configuring the HLR

The Tekelec ngHLR is usually configured at installation by the Tekelec *Customer Care Center*. The following information needs to be configured to run the HLR application:

1. SS7 configuration information
2. Activate/Deactivate HLR features.

3. HLR Address (one HLR address is configured at installation).

   Multiple HLR Addresses can be configured for one Tekelec ngHLR.

4. The state, location and non reachable reason for each HLR address defined in the system.

   This indicates to the ngHLR what information it must include in the MAP SRI-ack in the case where a subscriber (with both GSM and SIP subscriber profiles) is reachable only in the SIP domain.

5. An IMSI range, a HPLMN and a HPLMN Country can all be defined and associated to an HLR address (also known as HLR Identity: CC-NDC-SN).

   The Tekelec ngHLR supports multiple IMSI ranges to be defined per HLR Address, multiple CC-NDC to be defined as Home PLMN, multiple CCs to be defined as HPLMN Country.

The operator can view all of this configuration information from the WebCI's HLR folder, by opening the HLR Configuration window. Some of this information can be modified during running-time, without needing to restart the HLR services.

HLR Feature/Functionality Modification

Most HLR features or functionalities can be modified dynamically, that is, while the system is running. Other HLR features or functionalities require a restart of the HLR service to commit the modifications. The following table identifies these modification types.

Table 16: HLR feature or functionality modification types

Dynamic modification	HLR service restart
RegionalSubscription	MapMessageSegmentation
UssdForwardVlrNumber	SuperCharger
RoutingOnSsn	FtnTranslation
DomainSelection	UssdRouting
RoamingWelcomeMessage	MapResetOptimization
MapPolicing	VolDataOptimization
SimKiTransportEncryption	SaiAckSegmentation
SmsRouting	DirectCallForwardRegistration
ActiveDeviceDetection	VlrMessageNotification (see notes)
MobileNumberPortability	
SubscriberSignalingRouter	
AccessRestrictionData	
EnhancedControlOfSccpRouting	
UpdateOfSccpCgAddrOnlyForUL	
FtnProvValidation (FTN Provisioning validation through the OAM interface)	

Dynamic modification	HLR service restart
SMSRelay	
AlertSCBuildCdPA	
SriRouting	
VlrMessageNotification (see notes)	
EnhancedSccpAllowedPlmn	
MtRoamingRetry	

Note: The Network Operator can activate/deactivate the VLR Message Notification feature dynamically:

- for the entire system, by activating/deactivating from the WebCI's HLR Configuration - VlrMsgNotification tab.

  AND
- on a per subscriber basis, by provisioning from the WebCI the SubsVlrMsgNotificationOn parameter in the subscriber's Service Profile (SubscriberProfile)

Note: The VLR Message Notification feature is based on the same notification mechanism used for the Roaming Welcome Notification feature and may generate a large number of XML notifications. This number will impact the performance and/or decrease the maximum number of subscriber that can be provisioned on the system. This feature must only be enabled on a system that is dimensioned accordingly (for a given capacity AND traffic model). The Network Operator must contact the Tekelec *Customer Care Center* prior to enabling this feature to prevent any performance issues.

Viewing Activation Status of HLR Features and Activating/deactivating Them Individually

The Hlr Config table is configured by the Tekelec *Customer Care Center* at installation. It is located in the HLR Configuration window, which can be opened by extending the WebCI's HLR folder. However, most HLR features can be modified dynamically by the operator during running time of the system, by simply clicking on the **Modify** button, which will open the HlrConfig Provisioning window and then clicking on the Activate or Deactivate button available for each feature. Note that the Activate/Deactivate button is not available for the features that are Unavailable. You must contact the Tekelec *Customer Care Center* in order to make the feature available to activate (when made available, it is by default deactivated).

The HLR features that can be dynamically modified during running time of the system are as follows:

- RegionalSubscription
- MapMessageSegmentation
- SuperCharger
- UssdForwardVlrNumber
- RoutingOnSsn
- DomainSelection
- RoamingWelcomeMessage
- MapPolicing
- SimKiTransportEncryption

- FtnTranslation
- SmsRouting
- UssdRouting
- MapResetOptimization
- VolDataOptimization
- SaiAckSegmentation
- ActiveDeviceDetection
- MobileNumberPortability
- SubscriberSignalingRouter
- AccessRestrictionData
- DirectCallForwardRegistration
- VlrMessageNotification*
- EnhancedControlOfSccpRouting
- UpdateOfSccpCgAddrOnlyForUL
- FtnProvValidation (FTN Provisioning validation through the OAM interface)
- SMSRelay
- AlertSCBuildCdPA
- EnhancedSccpAllowedPlmn
- MtRoamingRetry

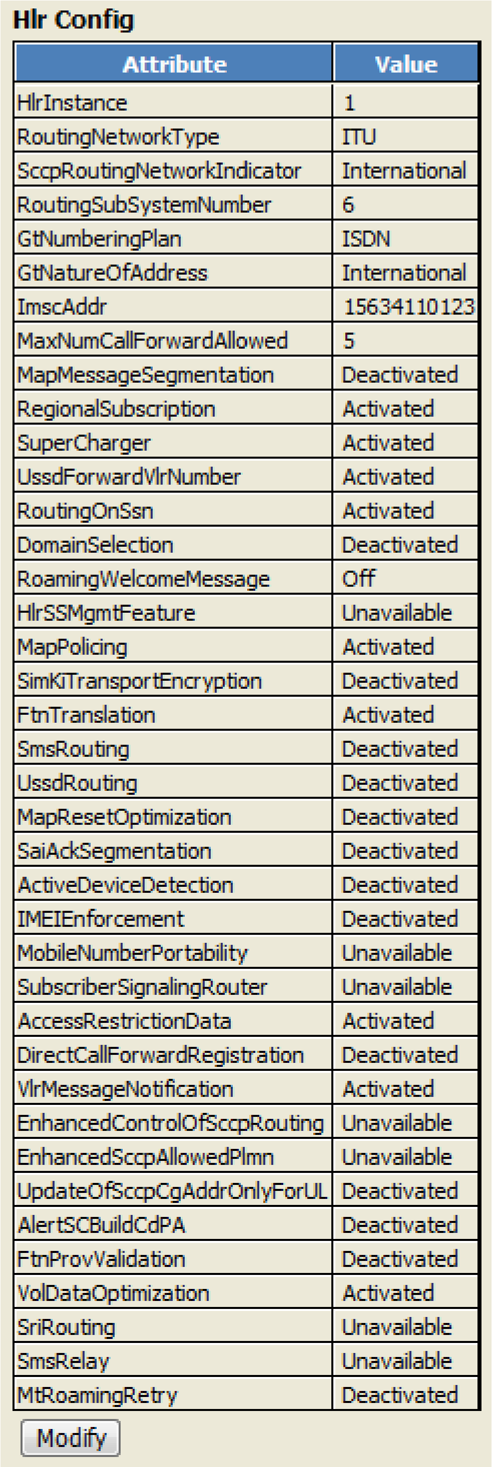
* the Network Operator can activate**/deactivate the VLR Message Notification feature dynamically:

- for the entire system, by activating/deactivating from the WebCI's HLR Configuration - VlrMsgNotification tab.

And

- on a per subscriber basis, by provisioning the subscriber's Service Profile (SubscriberProfile)'s SubsVlrMsgNotificationOn parameter through the WebCI.

Note: The VLR Message Notification feature is based on the same notification mechanism used for the Roaming Welcome Notification feature and may generate a large number of XML notifications. This number will impact the performance and/or decrease the maximum number of subscriber that can be provisioned on the system. This feature must only be enabled on a system that is dimensioned accordingly (for a given capacity AND traffic model). The Network Operator must contact the Tekelec *Customer Care Center* prior to enabling this feature to prevent any performance issues.



Hlr Config

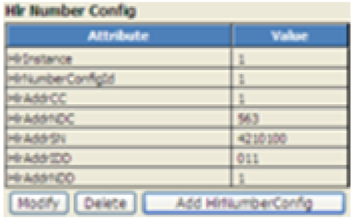
Attribute	Value
HlrInstance	1
RoutingNetworkType	ITU
SccpRoutingNetworkIndicator	International
RoutingSubSystemNumber	6
GtNumberingPlan	ISDN
GtNatureOfAddress	International
ImscAddr	15634110123
MaxNumCallForwardAllowed	5
MapMessageSegmentation	Deactivated
RegionalSubscription	Activated
SuperCharger	Activated
UssdForwardVlrNumber	Activated
RoutingOnSsn	Activated
DomainSelection	Deactivated
RoamingWelcomeMessage	Off
HlrSSMgmtFeature	Unavailable
MapPolicing	Activated
SimKiTransportEncryption	Deactivated
FtnTranslation	Activated
SmsRouting	Deactivated
UssdRouting	Deactivated
MapResetOptimization	Deactivated
SaiAckSegmentation	Deactivated
ActiveDeviceDetection	Deactivated
IMEIEnforcement	Deactivated
MobileNumberPortability	Unavailable
SubscriberSignalingRouter	Unavailable
AccessRestrictionData	Activated
DirectCallForwardRegistration	Deactivated
VlrMessageNotification	Activated
EnhancedControlOfSccpRouting	Unavailable
EnhancedSccpAllowedPlmn	Unavailable
UpdateOfSccpCgAddrOnlyForUL	Deactivated
AlertSCBuildCdPA	Deactivated
FtnProvValidation	Deactivated
VolDataOptimization	Activated
SriRouting	Unavailable
SmsRelay	Unavailable
MtRoamingRetry	Deactivated

Figure 16: HLR Configuration Parameters

Creating HLR Identity(ies) by Defining HLR Address(es)

The operator can configure the Tekelec ngHLR with multiple HLR addresses (also known as HLR numbers).

To achieve this, the operator must provision the Hlr Number Config table one entry at a time. This table can be found in the WebCI's HLR Configuration window, which can be opened from the menu's HLR folder. Note that at installation, the Tekelec *Customer Care Center* configures one HLR address for the Tekelec ngHLR.



Hlr Number Config

Attribute	Value
HlrInstance	1
HlrNumberConfigId	1
HlrAddrCC	1
HlrAddrNDC	563
HlrAddrSN	4210100
HlrAddrIDD	011
HlrAddrNDD	1

Figure 17: Configuring HLR Addresses From The HLR Configuration Window

When provisioning an HLR address, the following must be provided:

1. The CC-NDC-SN must be provisioned to define the HLR identity.
2. The IDD and NDD.
3. HLR Instance.

   For now, the Tekelec ngHLR only supports one HLR instance.
4. An Id (HlrNumberConfigId) must be defined to identify the HLR identity.

Once this table provisioned with the needed HLR identities, the operator can define HPLMNs, HPLMN Countries and IMSI ranges and associate each of these definitions to a specific HLR identity by specifying the correct ID (HlrNumberConfigId). Refer to *Defining PLMNs, Multiple Home PLMNs and HPLMNs Country* and *Associating an HPLMN, HPLMN Country and an HLR Identity to an IMSI range* for instructions on how to define PLMNs, HPLMNs and HPLMN Countries and on how to associate them to an HLR identity along with an IMSI range.

For more details on what is supported when configuring the Tekelec ngHLR with HLR addresses, PLMNs, HPLMNs, HPLMN Countries and IMSI ranges, refer to the following sections of SDM Product Description:

"HLR Number Configuration"

"Multiple IMSI range per HLR"

"Support for multiple CC-NDC as Home PLMN"

"Support for multiple Home PLMN Country definitions"

Configuring the MAP-SRI Interworking with SIP Subscribers

For a subscriber with both the GSM/SIP Subscriber Profiles provisioned in the Tekelec ngHLR, the Tekelec ngHLR can be configured to handle calls, as follows:

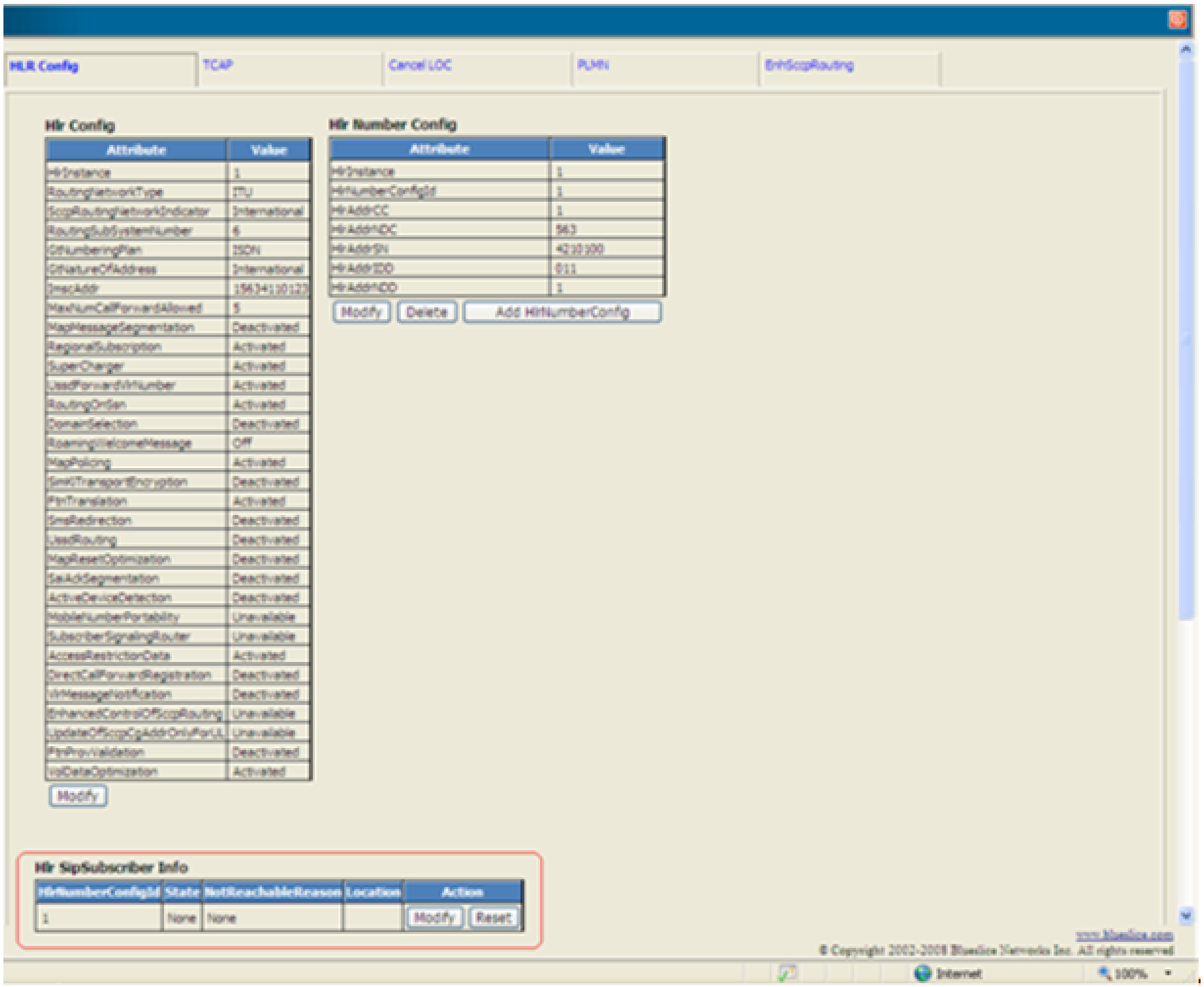
- Send back a MAP SRI-ack with the state/location information in the case where the GSM/SIP subscriber is only reachable in the SIP domain. This will allow the call to continue and for the Tekelec ngHLR to route it to the SIP domain.

  The Hlr SipSubscriberInfo table allows the operator to define the state, location and non reachable reason for each HlrNumberConfig entry (HLR Address) defined in the system. This indicates to the Tekelec ngHLR what information it must include in the MAP SRI-ack.

  The Hlr SipSubscriber Info table can be provisioned, by executing one of the following operations from the HLR Configuration window that can be opened from the WebCI's HLR folder:

  Modify. The default entry provisioned at installation can be modified at any point during running time. Can this be done dynamically from the WebCI.

  Reset. The entry already provisioned can be reset to the default values.



Hlr Config

Attribute	Value
HlrInstance	1
RoutingNetworkType	ITU
ScpRoutingNetworkIndicator	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
SmsTransportEncryption	Deactivated
FtnTranslation	Activated
SmsRedirection	Deactivated
UssdRouting	Deactivated
MapResetOptimization	Deactivated
SaiAckSegmentation	Deactivated
ActiveDeviceDetection	Deactivated
MobileNumberPortability	Unavailable
SubscriberSignalingRouter	Unavailable
AccessRestrictionData	Activated
DirectCallForwardRegistration	Deactivated
VlrMessageNotification	Deactivated
EnhancedControlOfScpRouting	Unavailable
UpdateOfScpCgAddrOnlyForUL	Unavailable
FtnProvValidation	Deactivated
VoDataOptimization	Activated

Hlr Number Config

Attribute	Value
HlrInstance	1
HlrNumberConfigId	1
HlrAddrCC	1
HlrAddrNDC	563
HlrAddrSN	4210100
HlrAddrIDD	011
HlrAddrNDD	1

Hlr SipSubscriber Info

HlrNumberConfigId	State	NotReachableReason	Location	Action
1	None	None		Modify Reset

www.blueslice.com
© Copyright 2002-2008 Blueslice Networks Inc. All rights reserved
Internet
100%

Figure 18: Hlr SipSubscriber Info Table From The HLR Configuration Window*314*

Defining PLMNs, Multiple Home PLMNs and HPLMNs Country

From the WebCI, the PLMN tab in the HLR Configuration window offers the possibility for the operator to define one or all of the following:

- PLMNs
- Home PLMNs
- Home PLMNs Country
- IMSI Ranges and associate them to an HLR address (identity) and an HPLMN and HPLMN Country.

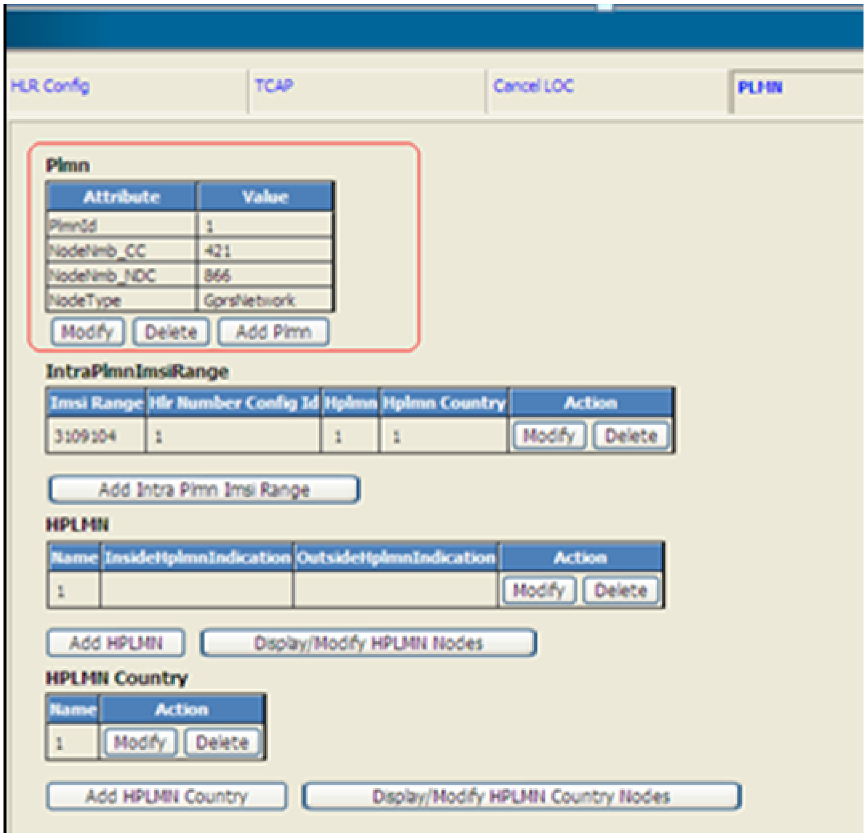
Defining PLMNs

The operator can define PLMNs for which zone codes can be provisioned for each subscriber. This table only needs to be provisioned if you wish to provision a subscriber profile with PLMN zone codes.

To achieve this, the operator must extend the WebCI's HLR folder from the menu bar and open the HLR Configuration window. From there, the operator must access the PLMN tab and provision the following:

The Plmn table, which allows the operator to provision PLMN definitions for which zone codes will be provisioned on a per subscriber basis.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .


HLR Config
TCAP
Cancel LOC
PLMN
Modify
Delete
Add Plmn
Add Intra Plmn Imsi Range
Add HPLMN
Display/Modify HPLMN Nodes
Add HPLMN Country
Display/Modify HPLMN Country Nodes

Plmn

Attribute	Value
PlmnId	1
NodeNmb_CC	421
NodeNmb_NDC	866
NodeType	GprsNetwork

IntraPlmnImsiRange

Imsi Range	Hlr Number Config Id	Hplmn	Hplmn Country	Action
3109104	1	1	1	Modify Delete

HPLMN

Name	InsideHplmnIndication	OutsideHplmnIndication	Action
1			Modify Delete

HPLMN Country

Name	Action
1	Modify Delete

Figure 19: Provisioning PLMN Definitions

Once this table has been provisioned, you can now provision subscriber profiles with Zone codes referring to one of the PLMN defined in this table. Refer to the *SDM Subscriber Provisioning – User Guide* for instructions on how to provision in bulk Subscriber Profiles with zone codes using XML files. Also refer to the *SDM Subscriber Provisioning – Reference Manual* for:

- An XML request example of how to provision a subscriber profile with zone codes (entity name: SubscriberPlmnZone).
- Details on the SubscriberPlmnZone entity, its parameters, the values supported and the default values.

In addition to provisioning the Plmn table with new entries, the following operations can be performed for this table:

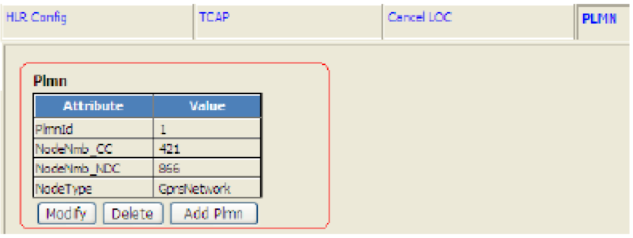
Delete. PLMN definitions can be deleted one at a time. Prerequisite: If any Subscriber Profiles refer to this PLMN, you must first delete the reference from the Subscriber Profile. Refer to the *SDM Troubleshooting, Monitoring, Maintenance – User Guide* document for instructions on how to modify a Subscriber Profile from the WebCI. Refer to the *SDM Subscriber Provisioning – User Guide* for instructions on how to modify Subscriber Profiles in bulk using XML files.

Modify. The CC, NDC or NodeType can be modified for a PLMN definition.

Defining PLMNs with PLMN zone code

If any Subscriber Profiles refer to this PLMN, you must first delete the reference from the Subscriber Profile. Refer to the SDM Troubleshooting, Monitoring, Maintenance – User Guide document for instructions on how to modify a Subscriber Profile from the WebCI. Refer to the *SDM Subscriber Provisioning –User Guide* for instructions on how to modify Subscriber Profiles in bulk using XML files.

1. Go to **HLR**>**HLR Configuration**
2. Click the **PLMN** tab.



Plmn

Attribute	Value
PlmnId	1
NodeNmb_CC	421
NodeNmb_NDC	866
NodeType	GprsNetwork

Figure 20: Defining PLMNs

3. Provision the PLMN table using one of these options:

   - **Add** a new PLMN entry.
   - **Modify**the CC, NDC or NodeType of a PLMN definition.
   - **Delete**PLMN definitions one at a time.

   Note: If a Subscriber Profiles refers to this PLMN, first delete the reference from the Subscriber Profile. Refer to the procedure on how to modify Subscriber Profiles in bulk using XML files in the *SDM Subscriber Provisioning –User Guide*

Once this table has been provisioned, you can provision subscriber profiles with Zone codes referring to one of the PLMNs defined in this table.

- Refer to the *SDM Subscriber Provisioning User Guide* for instructions on how to provision in bulk subscriber profiles with zone codes using XML files.
- refer to the SDM Subscriber Provisioning – Reference Manual for:
  - An XML request example of how to provision a subscriber profile with zone codes (entity name: SubscriberPlmnZone).
  - Details on the SubscriberPlmnZone entity, its parameters, supported values and default values.

Defining Home PLMNs

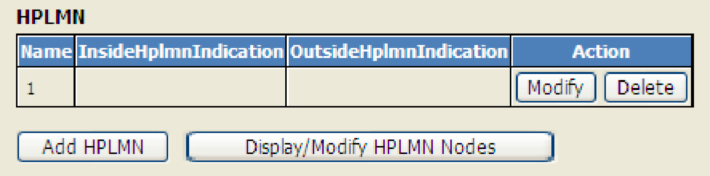
Define the Home PLMN for the Tekelec ngHLR.

The operator can configure the Tekelec ngHLR with multiple Home PLMNs, which can be defined as a set of up to 100 different CC-NDC combinations. Inside/Outside HPLMN Indicators can also be defined for each HPLMN, to indicate and distinguish when a subscriber is roaming inside or outside the HPLMN. These indicators are used for the 'Per Subscriber ATI screening' feature (refer to the feature description in the *SDM Product Description Manual*), when the subscriber's ATI information is set to 'HlrStoredStateAndHplmnIndication' in its HLR profile.

1. Go to **HLR>Configuration**

   The HLR Configuration window opens.

2. Click the **PLMN** tab.



HPLMN

Name	InsideHplmnIndication	OutsideHplmnIndication	Action
1			Modify Delete

Figure 21: Provisioning Home PLMNs

3. Provision the HPLMN table using one of these options:

   - **Add HPLMN** at least one HPLMN definition by defining:
     - HPLMN identification number
     - HPLMN name
     - Optionally, inside/outside HPLMN indicators
     - PPRAddress
     - HGMLCAddress

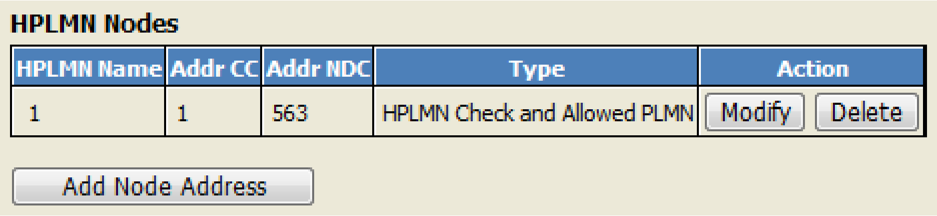
     Repeat this step for each HPLMN definition.
   - **Modify** one entry at a time. To change an HPLMN ID, delete the ID and recreate it with a different Id.
   - **Delete** one HPLMN definition at a time.

     Note:

     - An HPLMN Country definition that has already been associated to an HLR identity and an IMSI range in the IntraPlmnImsiRange table cannot be deleted.

- Deleting an HPLMN Country definition also deletes all CCs provisioned for this HPLMN Country.
- An HPLMN Country definition that has already been associated to an HLR identity and an IMSI range in the IntraPlmnImsiRange table cannot be deleted.

4. Display the HPLMN Nodes table by clicking **Display/Modify HPLMN Nodes** on the HPLMN table.



HPLMN Nodes

HPLMN Name	Addr CC	Addr NDC	Type	Action
1	1	563	HPLMN Check and Allowed PLMN	Modify Delete

Figure 22: Provisioning Home PLMN Nodes

5. Click **Add Node Address** on the HPLMN Nodes table to provision a CC-NDC combination for a specific Home PLMN that is defined in the HPLMN table.

   Repeat this step as needed until a set of up to 100 different CC-NDC combinations has been provisioned.

   A type is also provisioned and it indicates whether or not a node is allowed within an HPLMN based on its CC-NDC.

   The type is used to authorize the message to be accepted by the ngHLR and it can be one of the following:

HPLMN Check and Allowed PLMN	The subscriber is in the HPLMN or roaming in an allowed PLMN
HPLMN Check	The subscriber is in the HPLMN
Allowed PLMN	The subscriber is roaming in an allowed PLMN

6. As needed, perform these additional operations:

   - **Delete** CC-NDC combinations provisioned for an HPLMN definition one at a time from the HPLMN Node table.
   - Toggle between **Hide HPLMN Nodes** and **Display/Modify HPLMN Nodes** to hide or display the HPLMN Node table in the WebCI.

Defining HPLMNs Country:

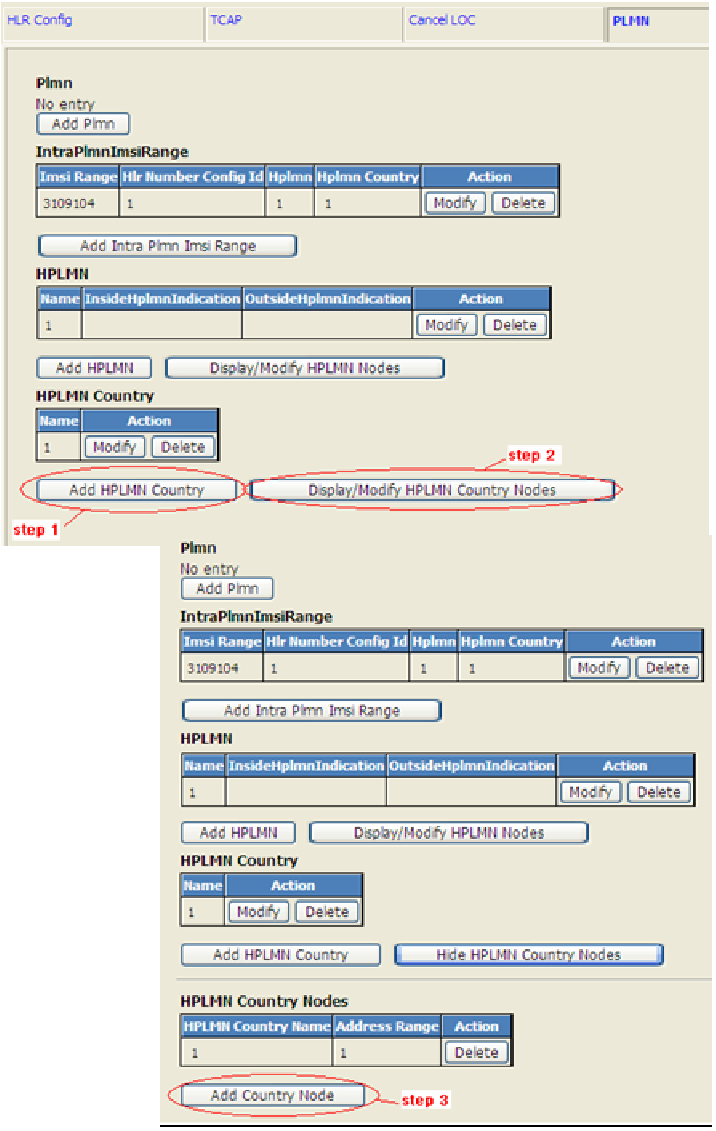
The operator can configure the ngHLR with multiple Home PLMN Countries, which can be defined as a list of CCs.

To achieve this, the following steps must be followed from the PLMN tab in the WebCI's HLR Configuration window. Note: The HLR Configuration window can be opened from the menu's HLR folder.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

1. The HPLMN Country table must be provisioned to have at least one HPLMN Country definition provisioned.
2. The HPLMN Country Nodes table must be displayed.
3. An address range (CC) can be provisioned for a specific Home PLMN Country that is already defined in the HPLMN Country table.

   This step can be repeated several times if you wish to define a list of CCs as Home PLMN Country.


HLR Config
TCAP
Cancel LOC
PLMN

Plmn

No entry

IntraPlmnImsiRange

Imsi Range	Hlr Number Config Id	Hplmn	Hplmn Country	Action
3109104	1	1	1	Modify Delete

Add Intra Plmn Imsi Range

HPLMN

Name	InsideHplmnIndication	OutsideHplmnIndication	Action
1			Modify Delete

Add HPLMN
Display/Modify HPLMN Nodes

HPLMN Country

Name	Action
1	Modify Delete

step 2
Add HPLMN Country
Display/Modify HPLMN Country Nodes
step 1

Plmn

No entry

Add Plmn

IntraPlmnImsiRange

Imsi Range	Hlr Number Config Id	Hplmn	Hplmn Country	Action
3109104	1	1	1	Modify Delete

Add Intra Plmn Imsi Range

HPLMN

Name	InsideHplmnIndication	OutsideHplmnIndication	Action
1			Modify Delete

Add HPLMN Display/Modify HPLMN Nodes

HPLMN Country

Name	Action
1	Modify Delete

HPLMN Country Nodes

HPLMN Country Name	Address Range	Action
1	1	Delete

Figure 23: Provisioning Home PLMN Countries

In addition to provisioning the HPLMN Country and HPLMN Country Nodes tables with new entries, the following operations can be performed for these tables:

Delete. The following can be deleted:

a) HPLMN Country definitions can be deleted one at a time from the HPLMN Country table.

Note1: It is not possible to delete a HPLMN Country definition that has already been associated to an HLR identity and an IMSI range in the IntraPlmnImsiRange table.

Note2: Deleting a HPLMN Country definition also deletes all the CCs provisioned for this HPLMN Country.

b) CCs provisioned for a HPLMN Country definition can be deleted one at a time from the HPLMN Country Nodes table.

Modify. HPLMN Country definitions can be modified one at a time from the HPLMN Country table. Only the name given to a HPLMN Country can be modified. To change the Id of a HPLMN Country entry, it must be deleted and recreated with the different Id.

Hide HPLMN Country Nodes. This operation allows the operator to hide the HPLMN Country Node table. This table remains provisioned as is, the WebCI simply won't display it. It can be displayed again with all its entries provisioned by clicking on the **Display/Modify HPLMN Country Nodes** button.

Associating an HPLMN, HPLMN Country and an HLR Identity to an IMSI range

Once at least one Home PLMN and Home PLMN Country are defined, the operator can associate them to an HLR identity and a specific IMSI range. Prior to doing so, make sure you have already defined at least one HLR identity (HLR address). Refer to section 4.1.4 "Creating HLR identity(ies) by defining HLR Address(es)" of this document for instructions on how to define an HLR identity when provisioning an HLR address.

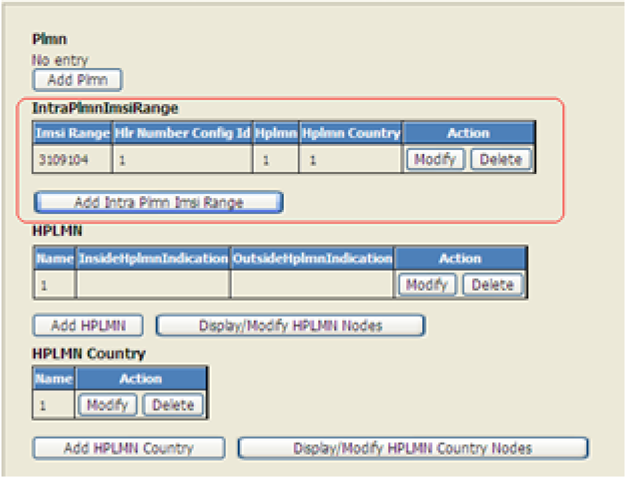
To achieve this, the operator must extend the WebCI's HLR folder from the menu bar and open the HLR Configuration window. From there, the operator must access the PLMN tab and provision the following:

Prerequisites: The HlrNumberConfig table must be provisioned with at least one HLR address (identity) and at least one HPLMN and HPLMN Country must be defined. Refer to the previous sections of this chapter for instructions on how to provision an HLR identity, an HPLMN and an HPLMN Country.

The IntraPlmnImsiRange table, which allows the operator to define the supported IMSI ranges and associate each of them with one HLR identity (address), one HPLMN and HPLMN Country.

Note: Since the Tekelec ngHLR supports multiple IMSI ranges per HLR address (identity), it is possible to define the same HLR identity and/or the same definitions of HPLMN and/or HPLMN Country for different IMSI ranges. Simply add a new entry in the IntraPlmnImsiRange table with the same HLR identity and/or HPLMN and/or HPLMN Country, but with a different IMSI range value.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.



Plmn

No entry

IntraPlmnImsiRange

Imsi Range	Hlr Number Config Id	Hplmn	Hplmn Country	Action
3109104	1	1	1	Modify Delete

HPLMN

Name	InsideHplmnIndication	OutsideHplmnIndication	Action
1			Modify Delete

HPLMN Country

Name	Action
1	Modify Delete

Add Plmn
Add Intra Plmn Imsi Range
Add HPLMN
Display/Modify HPLMN Nodes
Add HPLMN Country
Display/Modify HPLMN Country Nodes

Figure 24: Defining IMSI Ranges And Associating Them To An HLR Identity, A HPLMN And A HPLMN Country

In addition to provisioning the IntraPlmnImsiRange table with new entries, the following operations can be performed for this table:

Delete. An IMSI Range and its associations to an HLR identity, HPLMN and HPLMN Country can be deleted by clicking on the Delete button located in the same row as the IMSI Range you wish to delete. Prerequisite: Subscribers with IMSIs that fall within the IMSI range that you wish to delete must be deleted prior to deleting the HLR IntraPlmnImsiRange entry with that IMSI range. Refer to the SDM Subscriber Provisioning- User Guide for instructions on how to delete subscriber profiles in bulk with an XML file and refer to the SDM Troubleshooting, Monitoring, Maintenance – User Guide for instructions on how to delete a subscriber profile from the WebCI.

Modify. The association between an IMSI Range and an HLR identity and/or HPLMN and/or HPLMN Country definitions can be modified.

Associating an HPLMN, HPLMN Country and an HLR Identity to an IMSI range

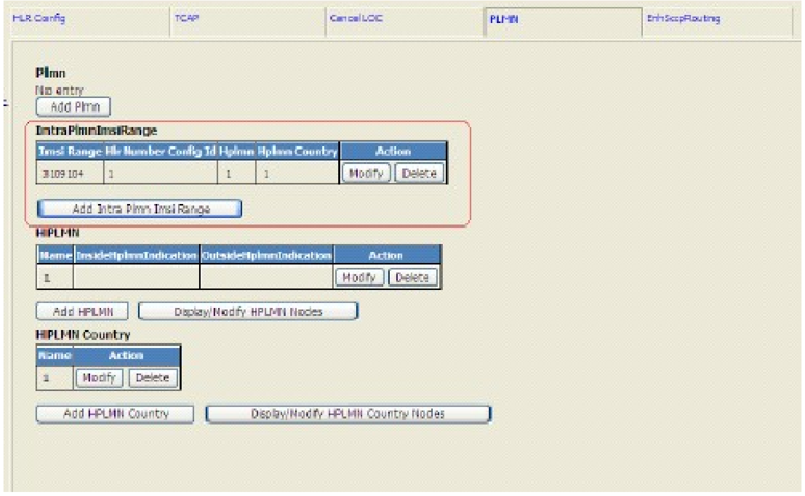
Associate HPLMN or HPLMN Country definitions to an HLR identity and IMSI range using the WebCI.

- The HlrNumberConfig table must be provisioned with at least one HLR address (identity) and at least one HPLMN and HPLMN Country must be defined.

The IntraPlmnImsiRange table allows the operator to define supported IMSI ranges and associate each with one HLR identity (address), one HPLMN definition, and one HPLMN Country definition.

Note: Since the Tekelec ngHLR supports multiple IMSI ranges per HLR address (identity), it is possible to define the same HLR identity and/or the same definitions of HPLMN and/or HPLMN Country for different IMSI ranges. Simply add a new entry in the IntraPlmnImsiRange table with the same HLR identity and/or HPLMN and/or HPLMN Country, but with a different IMSI range value.

1. Go to **HLR>HLR Configuration**
2. Click the **PLMN** tab.


HLR Config
TCAP
CancelLOC
PLMN
EnhSccpRouting
Add Plmn
Add Intra Plmn Imsi Range
Add HPLMN
Display/Modify HPLMN Nodes
Add HPLMN Country
Display/Modify HPLMN Country Nodes

Plmn

No entry

IntraPlmnImsiRange

Imsi Range	Hlr Number Config Id	Hplmn	Hplmn Country	Action
3109 104	1	1	1	Modify Delete

HPLMN

Name	InsideHplmnIndication	OutsideHplmnIndication	Action
1			Modify Delete

HPLMN Country

Name	Action
1	Modify Delete

Figure 25: Provisioning Intra-PLMN IMSI range table

3. Associate an IMSI range with HLR, HPLMN, and HPLMN Country identities in the IntraPlmnImsiRange table using one of these options:
   - Click **Add Intra Plmn Imsi Range** to add a new IMSI range and associate an
     - HLR identity
     - HPLMN identity
     - HPLMN Country identity
   - Click **Delete** to delete an IMSI Range and its associations to HLR, HPLMN, and HPLMN Country identities.

     Note: Subscribers with IMSIs that fall within the IMSI range that you wish to delete must be deleted prior to deleting the HLR IntraPlmnImsiRange entry with that IMSI range.

     - Refer to the *SDM Subscriber Provisioning User Guide* for instructions on how to delete subscriber profiles in bulk with an XML file.
     - Refer to the *SDM Troubleshooting, Monitoring, Maintenance User Guide* for instructions on how to delete a subscriber profile from the WebCI
   - Click **Modify** to change the association between and IMSI range and an HLR identity, or HPLMN definition or HPLMN Country definition.

Configuring the SS7 Stack Using MTP2/SAAL, MTP3 Protocols

The initial SS7 configuration is loaded into the Single Board Computers at installation (before system startup).

The configured SS7 nodes, links, link sets, and subsystem parameters can be modified and new ones can be added from the WebCI.

The following section describes how to provision new SS7 components. To achieve this, procedures describe how to define point codes, interfaces, links, link sets, and route sets in order to configure the SS7 Stack.

In order to operate, administer, and manage the components of an SS7 network, a network operator needs to set and inspect certain values that characterize the configuration of the network components.

So first, this section lists the prerequisite information necessary prior to configuring the SS7 Stack.

Collecting data prior to configuration

Collect all required information prior to configuration.

Collecting SS7 Point Code Data

The SS7 point codes are SS7 network addresses that uniquely identify every switch, Signal Transfer Point (STP). To communicate with the SS7 network, SS7 point codes must be obtained for the Tekelec SDM and for every SS7 network device that it will communicate with. The Tekelec ngHLR only supports one originating point code (OPC) and a minimum of one destination point code (DPC), one DPC per remote SS7 network device.

Collecting CombinedLinkset Data

A combinedLinkset must be defined for a group of all linksets that can be used to reach a particular destination or group of destinations (routes). Each linkset may be associated with up to 16 combined linksets. For each combined linkset that a linkset is a member of, it may be assigned a priority relative to other linksets belonging to that combined linkset.

Collecting Linkset Data

A linkset must be defined for each path between the Tekelec ngHLR and the adjacent STP. If there are two adjacent STPs, two linksets need to be created. A Linkset can contain from 1 to 16 links. The following information must be entered about each linkset:

- Destination Point Code
- Protocol Type (ANSI or ITU)
- CombinedLinkSets
- Collecting Link Data

A link corresponds to the linkset that was previously created. A pair of links will be created for each linkset in the system, for redundancy purposes. For example, if the system has two linksets, two links will be created for each linkset, resulting in the total of four links. The following information must be entered for each link:

- Protocol Variant
- Signalling Link Code (SLC)
- Priority
- Physical Interface
- Timeslot
- Bit Rate
- SlotId

Collecting Link Data

A link corresponds to the linkset that was previously created. A pair of links will be created for each linkset in the system, for redundancy purposes. For example, if the system has two linksets, two links will be created for each linkset, resulting in the total of four links. The following information must be entered for each link:

- Protocol Variant
- Signalling Link Code (SLC)
- Priority
- Physical Interface
- Timeslot
- Bit Rate
- SlotId

Collecting SS7 Route Data

An SS7 route must be defined for each Signalling End Point the Tekelec ngHLR wants to reach. There must be an SS7 route for each linkset. You must be ready to enter the following information about the SS7 route to be created:

- Destination Point Code (DPC)
- Originating Point Code (OPC)
- CombinedLinkset

Collecting SS7 Subsystem Data

One route is defined for each destination subsystem that the SCCP layer may be used to access. The route defines the destination point code used to reach that subsystem as well as any backup point code which replicates the subsystem.

Collecting Concerned Point Code Data

Every remote SignallingPoint interested in knowing about the state changes of the Tekelec ngHLR node shall be configured. They will receive messages such as SSA (Subsystem Allowed), SSP (Subsystem Prohibited), and SSC (Subsystem Congested).

Collecting Global Title Data

All mobile subscriber terminals in a cellular network (e.g. GSM) are usually defined in a specific database, the HLR (i.e., Tekelec ngHLR). The addressing of an HLR node in the telecom network is usually based on the first, most significant half of a mobile subscribe number. When an HLR communicates over the SS7 signalling network, this address information has to be translated into a form that allows routing in the SCCP network. Some of the address information based on the global title series is called a Global Title (GT). A GT needs to be translated into a DPC by the SCCP in order to make it possible for the MTP to route the signalling messages through the SCCP network. The following information must be entered about the GTT to be created:

- Destination Point Code (DPC)
- Subsystem Number (SSN)
- Nature of Address (NA)

- Numbering Plan (NP)
- Digits of the Called or Calling Party Number
- Translation Type (TT)
- Address Indicator (Routing Indicator, GT Indicator, SSN Indicator, Dpc Indicator)
- Network Indicator (NI)

SS7 Signaling Configuration Order

Once the physical ports have been configured on the Interphase cards (usually done by the Tekelec Customer Care Center), the operator can provision, modify or unprovision an SS7 logical node from the WebCI by following specific sequences.

Hereunder is a flow chart that provides an overview of these sequences for the configuration of the SS7 stack in the MTP2/SAAL, MTP3 and SCCP layers. Once all these steps have been followed, the TCAP and MAP layers must also be configured. For instructions on how to configure these last two layers, refer to *Configuring the TCAP layer* and *Configuring the MAP Layer* of this document.

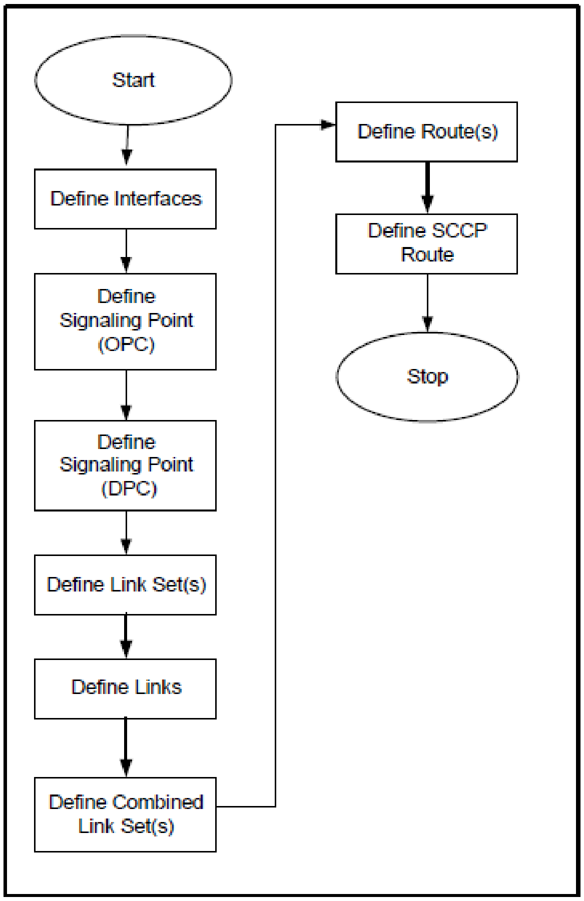


Figure 26: SS7 Node Provisioning Order

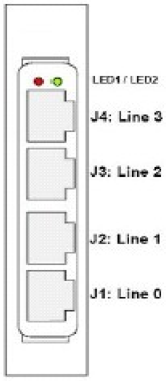
Configuring SS7 Signaling Interfaces (MTP2 or SAAL layer)

Once the physical ports of the network cards have been configured, interface components must be defined and associated with a network card. The interface represents a physical network connection on the network card. The SS7 card used in the SDM is an Interphase 4539F or 3639, which means that two types of Layer 2 interfaces can be configured on that card: MTP2Sap (with either Low Speed Links or High Speed Link type) and/or SAALSap (for High Speed Links). Each port can be configured with one of these two interfaces (Note that only the Tekelec *Customer Care Center* has the authority of reconfiguring those ports).

The following information will have to be provided if using the MTP2 layer: Channel number, physical interface used on the card (Line range: 0 to 3), Mtp2 Protocol Variant used on the link (ITU88, ITU92, ANS88, ANS92), Mtp2LinkType (Low Speed Link or High Speed Link), Timer Profile and slot inside the Tekelec ngHLR chassis on which the interface will be running.

The following information will have to be provided if using the SAAL: virtual port used on the card (Line range: 0 to 3), virtual channel identifier used by the Sap, virtual path identifier, the type of SAAL Link used (E1 or T1), message size and slot inside the Tekelec ngHLR chassis on which the interface will be running.

The 4539F card:



The 3639 card:

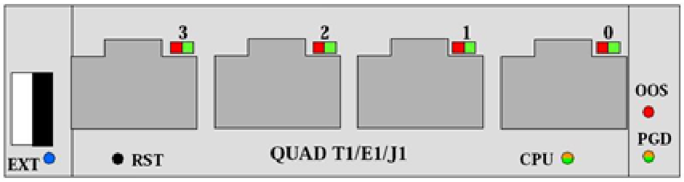


Figure 27: SS7 Link Interface

All these SS7 components can be defined, modified and deleted from the WebCI, in the SS7 folder's MTP2 or SAAL window, depending on the protocol you wish to use.

MTP2 Window

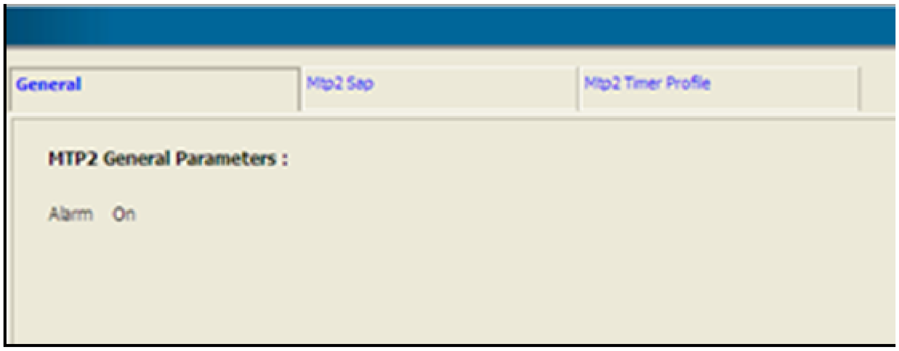
Requirements: Log into a WebCI session with a valid username and password.

The MTP2 view is used to DISPLAY, ADD, ACTIVATE, MODIFY, and DELETE the parameters used to define the MTP2 layer of the SS7 network. The MTP2 Timer profiles can also be displayed from this view. The following MTP2 provisioning tabs are available: General, Mtp2 Sap, and Mtp2 Timer Profile.

Navigate through these tabs to define the interface when configuring SS7 Signaling Links.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

Refer to the SS7 entities section of the *SDM System Configuration - Reference Manual* for more details on the MTP2 parameters.



MTP2 General Parameters :

Alarm On

Figure 28: MTP2 Window For SS7 Signaling Link Configuration

General Tab

The General tab allows to view and modify the MTP2 General parameters.

The following operations are supported for MTP2 General Parameters:

Apply: Modify an existing MTP2 General configuration.

Mtp2 Sap Tab

The Mtp2 Sap tab allows to provision MTP2 Service Access Points (SAPs) which contain the attributes of the physical port and link that is connected to the logical signaling link.

Note: You cannot add an MTP2 Sap on a slot that does not exist. The following error message will appear:

```
Failed to create Mtp2Sap, requested slot# do not have active MTP2 layer
```

The following operations are supported for MTP2 Service Access Points:

`Add MTP2 SAP`: Add a new MTP2 SAP.

`Display timers`: Display and modify Timer Profiles and values associated with this SAP.

`Edit`: Modify an existing MTP2 SAP configuration.

`Activate`: Activate an MTP2 SAP to bind the MTP2 layer to the MTP3 layer.

`Delete`: Delete an MTP2 SAP.

Note: Delete all links referencing this SAP first before deleting the SAP.

Mtp2 Timer Profile Tab

The Mtp2 Timer Profile tab allows to configure MTP2 Timer Profiles.

The following operations are supported for MTP2 Timer Profiles:

`Add Timer Profile`: Add a new MTP2 Timer Profile.

`Display timers`: Display and modify Timer Profiles and values associated with this SAP.

`Delete`: Delete an existing MTP2 Timer Profile.

SAAL Window

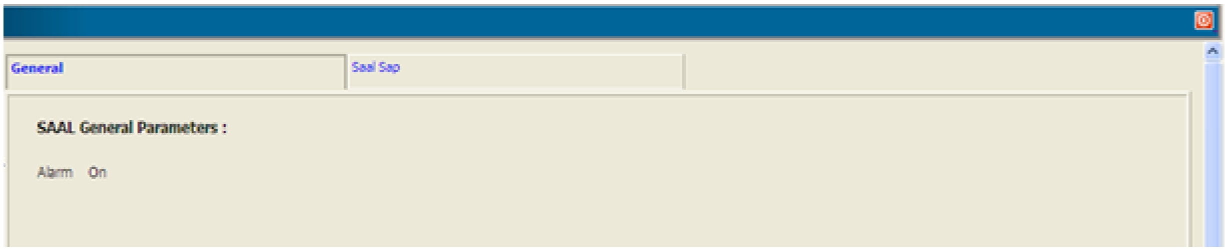
Requirements: Log in to a WebCI session with a valid username and password.

The SAAL view is used to DISPLAY, ADD, ACTIVATE, MODIFY, and DELETE the parameters used to define the SAAL layer of the SS7 network. The following SAAL provisioning tabs are available: General, Mtp2 Sap.

Navigate through these tabs to define the interface when configuring SS7 Signaling Links.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

Refer to the SS7 entities section of the *SDM System Configuration - Reference Manual* for more details on the SAAL parameters.



SAAL General Parameters :

Alarm On

Figure 29: SAAL Window For SS7 Signaling Link Configuration

General tab

The General tab allows to view and modify the SAAL General parameters.

Saal Sap Tab

The Saal Sap tab allows to provision SAAL Service Access Points (SAPs) which contain the attributes of the physical port and link that is connected to the logical signaling link.

Note: You cannot add a SAAL Sap on a slot that does not exist. The following error message will appear:

```
Failed to create SaalSap, requested slot# do not have active SAAL layer
```

The following operations are supported for SAAL Service Access Points:

`Add SAAL SAP`: Add a new SAAL SAP.

`Edit`: Modify an existing SAAL SAP configuration. (i.e. Modify the Message Size)

`Activate`: Activate an SAAL SAP to bind the SAAL layer to the MTP3 layer.

`Delete`: Delete a SAAL SAP. NOTE: Delete all links referencing this SAP first before deleting the SAP.

Configuring SS7 Signaling Point Codes

Defining the Signaling Point Codes consists of defining the SS7 network devices that connect the Tekelec ngHLR to remote switches. To uniquely identify these network devices, a point code must be assigned to each network device, which serves as SS7 network addresses. The point codes must be unique within the SS7 network. These point codes must be obtained from your SS7 network administrator.

Point codes are necessary for the following network devices:

- Tekelec ngHLR
- Signalling Transfer Point (STP)
- Remote Signaling End Point (SEP)

When configuring a Tekelec ngHLR, a point code address and a point code type must be entered along with the protocol type and the network indicator. The PcType is OPC, the SignallingType is SEP, the ProtocolVariant is either ANSI or ITU, the NetworkIndicator is either NATIONAL or INTERNATIONAL and the point code address is a value in the form x.x.x (for ANSI 8bits.8bits.8bits and for ITU 3bits.8bits.3bits).

For configuring point codes for STP, the PcType is DPC, the SignallingType is STP and the point code address is a value in the form x.x.x.

For configuring point codes for Remote SEP, the PcType is DPC, the SignallingType is SEP and the point code address is a value in the form x.x.x.

The Signaling Point Codes can be defined, modified and deleted from the WebCI, in the SS7 folder's MTP3 window.

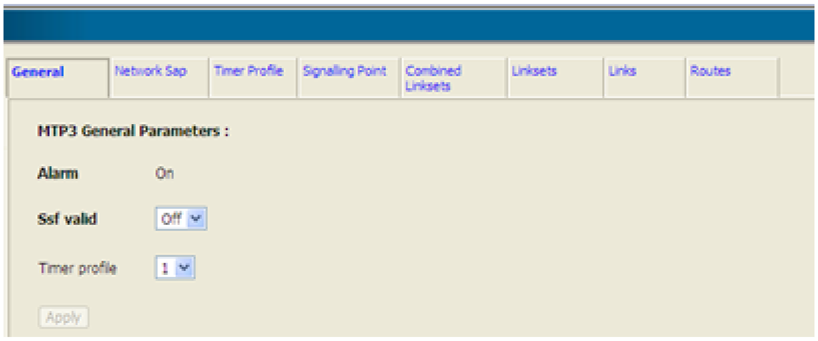
MTP3 Window

Requirements: Log in to a WebCI session with a valid username and password.

The MTP3 view is used to Display, Add, Modify, Delete, Activate, and Deactivate the parameters used to define the MTP3 layer of the SS7 network. The following MTP3 provisioning tabs are available: General, Network Sap, Timer Profile, Signalling Point, Combined Linksets, Linksets, Links, and Routes. Navigate through these tabs to configure SS7 Signaling Routes.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

Refer to the SS7 entities section of the *SDM System Configuration - Reference Manual* for more details on the MTP3 parameters.



MTP3 General Parameters :

Alarm On

Ssf valid Off

Timer profile 1

Figure 30: MTP3 Window

General Tab

The General tab allows you to view and modify the MTP3 General parameters.

The following operations are supported for MTP3 General Parameters:

`Apply`: Modify an existing MTP3 General configuration.

Timer Profile Tab

The Timer Profile tab allows you to configure MTP3 Timer Profiles for the MTP3 Protocol Layer.

The following operations are supported for MTP3 Timer Profiles:

`Add Timer Profile`: Add a new MTP3 Timer Profile.

`Modify Timers`: Display and modify Timer Profiles and values associated with this SAP.

`Delete`: Delete an existing MTP3 Timer Profile.

Signaling Point Tab

The Signaling Point tab allows you to provision MTP3 Signaling Points (SPs). A signaling point can represent either a local (Own Signaling Point - OPC) or a remote signaling point (Destination Signaling Point - DPC). The remote signaling point is an adjacent or far-end node.

The following operations are supported for MTP3 Signaling Points:

`Add Signalling Point`: Add a new MTP3 Signaling Point.

`Modify`: Modify an existing MTP3 Signaling Point configuration.

`Delete`: Delete an MTP3 Signaling Point.

Configuring SS7 Signaling Linksets

At this point, the operator must define the linksets that connect each Tekelec ngHLR node directly to an STP.

The operator can achieve this from the MTP3 window (refer to previous figure) of the WebCI's SS7 folder. More precisely, the linksets can be defined from the MTP3 window's Linksets tab.

Linksets Tab from the WebCI's MTP3 Window

The Linksets tab allows you to configure MTP3 Linksets. Linksets define groups of 1 to 16 links that directly connect two signaling points (SPs).

The following operations are supported for MTP3 Linksets:

`Add LinkSets`: Add a new MTP3 Linkset.

`Delete`: Delete an MTP3 Linkset.

`Display Links`: Display all associated linksets that belong to the Linkset.

`Activate/Deactivate Linksets`: Activate/deactivate all the Links of a LinkSet.

Configuring SS7 Signaling Links

Once the interfaces and Linksets have been defined, the communication links between the Tekelec ngHLR and SS7 STPs can be defined. While linksets define which Signaling Point a given route uses, it is the links that carry the communications traffic. This section describes how to provision the signaling link component. Refer to the previous sections if the interfaces and linksets have not been defined yet.

The operator can provision a SS7 Signaling link component from the MTP3 window (refer to previous figure) of the WebCI's SS7 folder. More precisely, links can be defined from the MTP3 window's Links tab.

To provision a new SS7 link, the operator must open the Link tab from the MTP3 window. For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

Then, it can provision a SS7 link, as follows:

Prerequisites: Provision the SS7 interfaces and Linksets. Refer to the previous sections.

Provision an entry in the MTP3 Links table, by clicking on the Add button. When defining

the SS7 signaling links, the operator must do the following:

1. Define to which Linkset the link will belong to.
2. Specify the following information:
3. Which interface to use: (Mtp2Sap or SaalSap).

   Each SS7 link in the node must be associated with an interface component, which must be associated with a network card.
4. SLC, Adjacent Signaling Points, and Priority.

Links Tab from the WebCI's MTP3 Window

The Links tab allows you to configure MTP3 Links. Links define physical signaling links between the SS7 board and the adjacent signaling points. One link configuration must be performed for each physical signaling link.

The following operations are supported for MTP3 Links:

`Add`: Add a new MTP3 Link.

`Edit`: Modify an existing MTP3 Link configuration.

Note: When an SS7 link is up and running, any modification to the link may cause it to go down and result in signaling failure. The link must be deactivated first before modifying it.

`Delete`: Delete an MTP3 Link.

`Activate`: Activate an MTP3 Link to be available to carry MTP3 user traffic.

`Deactivate`: Remove the link from service and make it unavailable to carry traffic.

Configuring SS7 signaling routes at the MTP3 layer

Once the links have been configured, different routes can be defined between the Tekelec ngHLR and a destination device (STP or SEP).

The routing can be done at two layer levels: MTP3 and SCCP. If you wish to define a route at the SCCP layer level, you must first have configured it in the MTP3 layer.

Configuring the SS7 Signaling Routes at the MTP3 layer includes defining the following:

1. Combined linkset (CombinedLinkSet)
2. The signaling route (Route)
3. The Network Sap

Defining Combined Linkset

After determining the point codes for the network devices, define the combined linkset that will group linksets together.

The Combined Linkset can be defined, modified and deleted from the WebCI, in the SS7 folder's MTP3 window (refer to the previous figure). More precisely, from the MTP3 window's Combined Linksets tab.

Combined Linksets Tab from the WebCI's MTP3 Window:

The Combined Linksets tab allows you to configure MTP3 Combined Linksets. It defines a group of all linksets that can be used to reach a particular destination or group of destinations (routes).

The following operations are supported for MTP3 Combined Linksets:

Add Combined LinkSets: Add a new MTP3 Combined Linkset.

Delete: Delete an MTP3 Combined Linkset.

Display Linksets: Display all associated linksets that belong to the Combined Linkset.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

Defining Routes

The final step in planning SS7 signaling routes is to define the SS7 routes themselves. Routes are defined in terms of the point codes along the path and the combined linksets that lead from the Tekelec ngHLR node through the STPs to each DPC.

Items such as the OPC, DPC, and combinedLinksetId will have to be specified.

The Routes can be defined, modified and deleted from the WebCI, in the SS7 folder's MTP3 window (refer to the previous figure). More precisely, from the MTP3 window's Routes tab.

Routes Tab from the WebCI's MTP3 Window

The Routes tab allows you to configure MTP3 Routes to Destination Point Codes.

The following operations are supported for MTP3 Route:

Add Route: Add a new MTP3 Route.

Modify: Modify an existing MTP3 Route configuration.

Delete: Delete an MTP3 Route.

Note: Delete all the links and linksets prior to deleting the route.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

Defining Network Sap

Defining the Network Sap allows you to define the interface between the SCCP and MTP3 layers.

The Network Sap can be defined, modified and deleted from the WebCI, in the SS7 folder's MTP3 window (refer to the previous figure). More precisely, from the MTP3 window's Network Sap tab.

Network Sap Tab from the WebCI's MTP3 Window

The Network Sap tab allows you to provision MTP3 Network Service Access Points (SAPs) and define the interface between the SCCP and MTP3 layers. One Network SAP is defined for each MTP 3 layer interface that the SCCP layer uses.

Note: You cannot add a second MTP3 Network SAP. The following error message will appear:

```
This operation on MTP3NSap is disabled in LDF environment.
```

The following operations are supported for MTP3 Network Service Access Points:

`Add MTP3 Network SAP`: Add a new MTP3 Network SAP.

`Modify`: Modify an existing MTP3 Network SAP configuration.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

Configuring SS7 Signaling Routes at the SCCP Layer

At the SCCP layer, routes can be defined between the Tekelec ngHLR's signaling stack and the destination systems or subsystems by using either one of the following routing indicators:

- Global Titles

Or

- Destination Point Codes –SSN

The following components must be configured when configuring an SS7 Signaling Route at the SCCP layer:

1. Define General and Timer Profile information

2. Define Network and User Saps
3. Define SCCP Route
4. Define the DPC-SSN of the destination systems or subsystems (the following only needs to be defined in the case where the routing indicator is DPC-SSN):
5. Define Remote SSN
6. Define Concerned Area Point Code
7. Define Concerned Point Codes (Optional)
8. Define the GTs of the destination systems or subsystems (the following only needs to be defined in the case where the routing indicator is GT):
9. Define Global Title Entries
10. Define SCCP Addresses
11. Define Concerned Point Codes (Optional)
12. Define Concerned Point Codes (Optional)

Configuring SCCP Routes with Global Titles as Routing Indicators

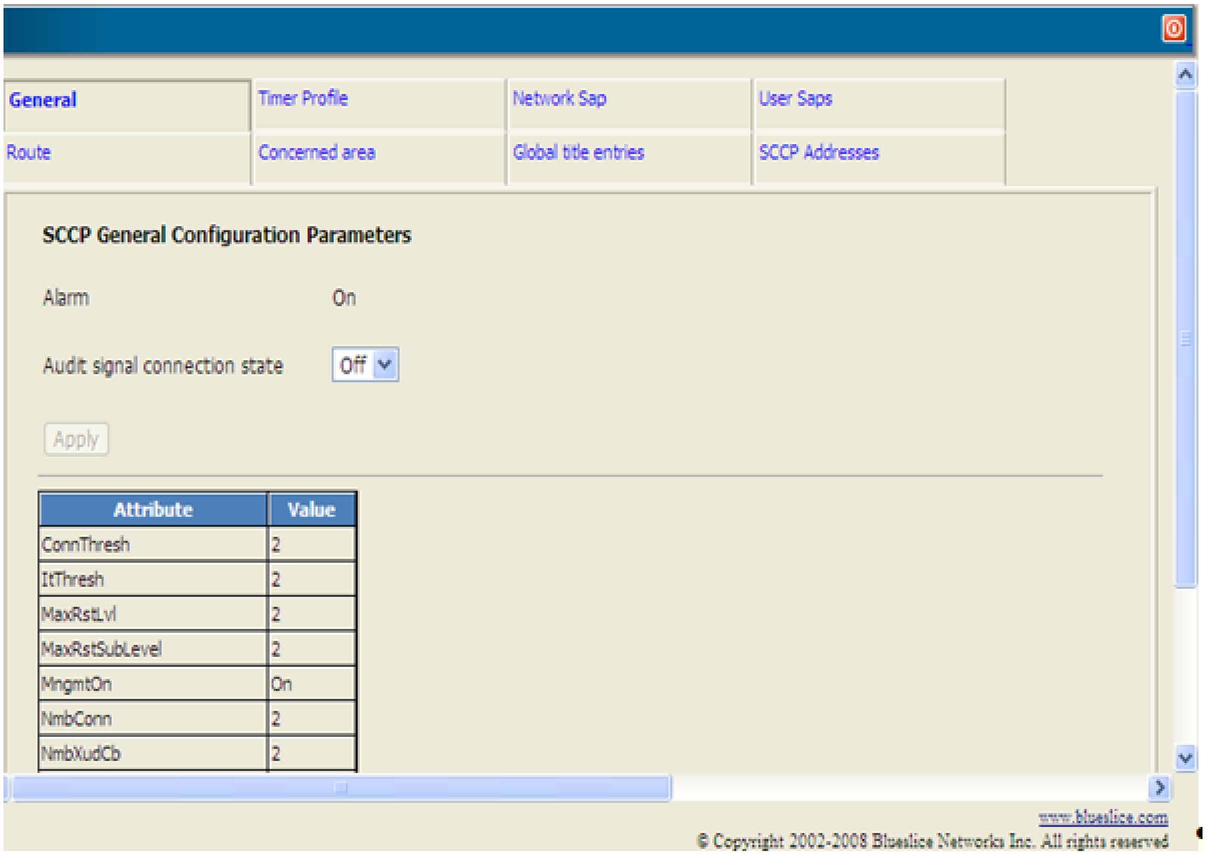
Requirements: Log in to a WebCI session with a valid username and password.

The SCCP view is used to Display, Add, Modify, Delete, Activate, and Deactivate the parameters used to define the SCCP layer of the SS7 network. The following SCCP provisioning tabs are available: General, Timer Profile, Network Sap, User Saps, Route, Concerned area, Global title entries and SCCP Addresses.

Note: The tables in the Concerned area tab don’t need to be provisioned when configuring a route with Global Titles as routing indicators.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

Refer to the SS7 entities section of the *SDM System Configuration - Reference Manual* for more details on the SCCP parameters.



SCCP General Configuration Parameters

Alarm On

Audit signal connection state Off

Attribute	Value
ConnThresh	2
ItThresh	2
MaxRstLvl	2
MaxRstSubLevel	2
MngmtOn	On
NmbConn	2
NmbXudCb	2

Figure 31: SCCP Window

General Tab

The General tab allows to view and modify the SCCP General parameters such as timer values and threshold values that apply to the entire SCCP layer.

The following operations are supported for SCCP General Configuration Parameters:

`Apply`: modify the Audit signal connection state

`Edit General Parameters`: Modify an existing SCCP General Configuration.

Timer Profile Tab

The Timer Profile tab allows to configure SCCP Timer Profiles for the SCCP Layer.

The following operations are supported for SCCP Timer Profiles:

`Add Timer Profile`: Add a new SCCP Timer Profile Configuration.

`Edit Timers`: Display and modify Timer Profiles and values.

`Delete`: Delete an existing SCCP Timer Profile.

Network Sap Tab

The Network Sap tab allows to view the M3UA Network Service Access Points (NSap) automatically created by system to define the interface between the SCCP and M3UA layers. One Network SAP is defined for each M3UA layer interface that the SCCP layer uses.

User Saps Tab

The User Saps tab allows to provision SCCP User Service Access Points (USAPs) and to define the interface between the user applications and SCCP layer. One user SAP is defined for each application using the SCCP layer services.

The following operations are supported for SCCP User Service Access Points:

`Add SCCP User SAP`: Add a new SCCP User SAP configuration.

`Edit`: Modify an existing SCCP User SAP configuration.

`Delete`: Delete an SCCP User SAP.

`Display Concerned PCs`: Display the associated Concerned Point Codes interested in the status change of this USAP.

Route Tab

The Route tab allows to configure SCCP Routes to Destination Point Codes. One route is defined for each destination signalling point that the SCCP Layer may route outgoing messages to.

The following operations are supported for SCCP Route:

`Add Route`: Add a new SCCP Route Configuration.

`Modify`: Modify an existing SCCP Route configuration.

`Delete`: Delete an SCCP Route.

Note: First, delete any Concerned Areas still referencing this route.

Global Title Entries Tab

The Global title entries tab allows to configure SCCP Global Title Entries. Refer to the *SDM System Configuration - Reference Manual* for additional details on the Global Title Entries.

The following operations are supported for SCCP Global Title Entry:

`Add Global Title Entry`: Add a new Global Title Entry configuration.

`Delete`: Delete a Global Title Entry.

SCCP Addresses Tab

The SCCP Addresses tab allows to configure SCCP Addresses. Refer to the *SDM System Configuration - Reference Manual* for additional details on the SCCP Address parameters.

The following operations are supported for SCCP Address:

`Add Address`: Add a new SCCP Address configuration.

`Delete`: Delete an SCCP Address.

Configuring SCCP Routes with DPC-SSNs as Routing Indicators

Requirements: Log in to a WebCI session with a valid username and password.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

The SCCP window (see previous figure) is used to Display, Add, Modify, Delete, Activate, and Deactivate the parameters used to define the SCCP layer of the SS7 network. The following SCCP provisioning tabs are available: General, Timer Profile, Network Sap, User Saps, Route, Concerned area, Global title entries and SCCP Addresses.

Take note that the tables in the following tabs must be provisioned to define a SCCP Route with the DPC-SSN as the routing indicator:

- General
- Timer Profile
- Network Sap
- User Saps
- Route
- Concerned area

  Refer to *Configuring SCCP Routes with Global Titles as Routing Indicators* for more information on the General, Timer Profile, Network Sap, User Saps and Route tabs.

  On the other hand, the Global title entries tab does not need to be provisioned when configuring a route using DPC-SSNs.

  Refer to the SS7 entities section of the *SDM System Configuration - Reference Manual* for more details on the SCCP parameters.

Concerned Area Tab

One route is defined for each destination system or subsystem that the SCCP layer may be used to access. The route defines the destination point code used to reach that subsystem as well as any backup point code which replicates the subsystem.

The Concerned area tab allows to configure SCCP Routes to Destination Point Codes. One route is defined for each destination signaling point that the SCCP Layer may route outgoing messages to.

The following operations are supported for SCCP Concerned Area:

`Add Concerned Area`: Add a new SCCP Concerned Area. Maximum of five Concerned Areas per Route can be added.

`Modify`: Modify an existing SCCP Concerned Area configuration.

`Delete`: Delete an SCCP Concerned Area.

Note: First, delete any Concerned Areas still referencing this route.

`Get concerned PCs`: Add, retrieve and display the Concerned Point Codes for this specific RemoteSSN. All Signalling Points (SPs) interested in knowing about the Tekelec ngHLR state (In Service, Out of Service) shall be configured.

`Get backup PCs`: Add, retrieve and display the list of Backup Point Codes.

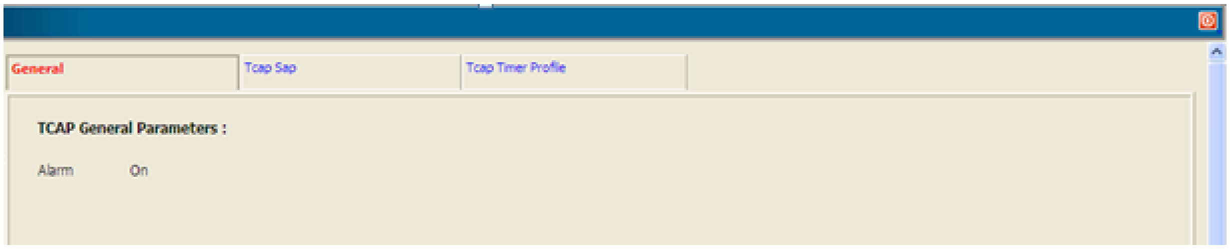
Configuring the TCAP layer

Requirements: Log in to a WebCI session with a valid username and password.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

The TCAP (Transaction Capability Application Part) window is used to Display, Add, Modify, Delete, Activate, and Deactivate the parameters used to define the TCAP layer of the SS7 network. The following TCAP provisioning tabs are available: General, Tcap Sap, Tcap Timer Profile. Refer to the

SS7 entities section of the *SDM System Configuration - Reference Manual* for more details on TCAP parameters.



TCAP General Parameters :

Alarm On

Figure 32: TCAP Window

General Tab

The General tab allows to view the TCAP General Parameter screen.

TCAP Sap Tab

The Tcap Sap tab allows to provision TCAP Service Access Points (SAPs) and define the interface between a TCAP user application and the TCAP layer. One TCAP SAP is defined for each application using the TCAP layer services.

The following operations are supported for TCAP Service Access Points:

`Add TCAP SAP`: Add a new TCAP Service Access Point Configuration. Note: You cannot add a second TCAP Network SAP. The following error message will appear:

```
This operation on TCAPNSap is disable in LDF environment.
```

`Display timers`: Display and modify TCAP Timers configuration.

`Edit`: Modify an existing TCAP SAP configuration.

`Delete`: Delete a TCAP SAP.

`Delete unused dialogues`: Delete all unused dialogue control blocks.

`Delete unused invokes`: Delete all unused invoke control blocks.

Note: You cannot deactivate or activate Tcap Sap. This is now done automatically by the system when needed.

Timer Profile Tab

The Timer Profile tab allows to configure TCAP Timer Profiles for the TCAP Layer.

The following operations are supported for TCAP Timer Profiles:

`Add Timer Profile`: Add a new TCAP Timer Profile Configuration.

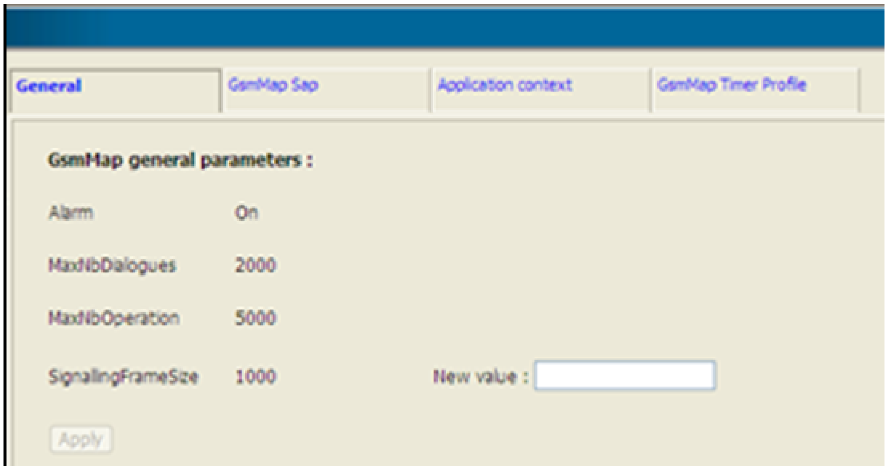
`Edit Timers`: Display and modify Timer Profiles and values.

`Delete`: Delete an existing TCAP Timer Profile.

Configuring the MAP Layer

Requirements: Log in to a WebCI session with a valid username and password. For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

The MAP window is used to Display, Add, Modify, Delete, Activate, and Deactivate the parameters used to define the MAP layer of the SS7 network. The following MAP provisioning tabs are available: General, GsmMap Sap, Application context, and GsmMap Timer Profile. Refer to the SS7 entities chapter of the *SDM System Configuration - Reference Manual* for more details on MAP parameters.



GsmMap general parameters :

Alarm On

MaxNbDialogues 2000

MaxNbOperation 5000

SignalingFrameSize 1000 New value :

Figure 33: Map Window

General Tab

The General tab allows to view and modify the MAP General configuration parameters that apply to the entire GsmMap Layer.

The following operation is supported for MAP General Parameters:

`Apply`: modify the Signalling Frame Size.

GSM Map Sap Tab

The GsmMap Sap tab allows to provision MAP Service Access Points (SAPs). This is the Service Access Point (SAP) of the GSM-MAP services to its users (i.e., HLR) and contains the SAP address (i.e., Sub-System number).

The following operations are supported for GSM Map Service Access Points:

`Add GsmMap SAP`: Add a new GSM Map Service Access Point Configuration.

`Display timers`: Display and modify GSM Map Timers Configuration.

`Edit`: Modify an existing GS Map SAP configuration.

`Activate`: Activate the Tcap Service Access Points (TCAPSAP).

`Delete`: Delete a TCAP SAP.

Application Context Tab:

The Application context tab allows to define the MAP services supported by the HLR, such as mobility management, location management, call handling etc...

The following operations are supported for GSM Map Application Contexts:

`Add application context`: Add a new GSM Map Application Context Configuration.

`Display timers`: Display and modify GSM Map Timers Configuration.

`Edit`: Modify an existing GSM Map Application Context Configuration.

`Delete`: Delete a GSM Map Application Context.

Timer Profile Tab

The Timer Profile tab allows to configure the GsmMap Timer Profiles.

The following operations are supported for GsmMap Timer Profiles:

`Add timer profile`: Add a new GsmMap Timer Profile Configuration.

`Edit Timers`: Display and modify Timer Profiles and values.

`Delete`: Delete an existing GsmMap Timer Profile.

Configuring the SS7 Stack Using the TUCL, M3UA & Protocols (SIGTRAN)

The ngHLR of the SDM can also use the SIGTRAN feature for SS7 communication via IP. This feature utilizes the TUCL, M3UA protocols and the Linux/SCTP stack (controlled by the OS kernel) to receive the SS7 messages through IP connections and then transport and route them to upper layers of the SS7: SCCP, TCAP, MAP.

The SDM supports the following for SS7 communication using the SIGTRAN feature:

- The ITU/ANSI networks
- The possibility to act as the client or the server (type of Association)
- A single local or remote IP address or multiple local or remote IP addresses
- Two modes:
- ASP – Application Server Process. In this mode, the SDM plays the role of an Application Server (AS) where the ASP is a process instance of the AS. The ASP contains an SCTP endpoint and is configured to process signaling traffic with an external Signalling Gateway node that takes care of translating MTP3 services coming from the VLR into services supported by SIGTRAN. This mode is used if the VLR does not support the SIGTRAN feature.
- SGP-Signalling Gateway Process. The SDM supports SIGTRAN communication with a Signalling Gateway node. In this mode, the SDM plays the role of a Client and initiates the establishement of the association with the external SGP.
- IPSP – IP Server Process. In this mode, the SDM plays the role of an IP Server or IP Client where the IPSP is a process instance of an IP-based application. In this context, the SDM uses M3UA in a point-to-point fashion and does not use the services of a Signalling Gateway node. SS7 communication is done over IP directly between the SDM using the SIGTRAN feature and the VLR that also supports the SIGTRAN feature.

The following sections cover all the provisioning information from the prerequisites to the procedures for provisioning a new system with new SS7 components using the SIGTRAN feature.

Once the initial SS7 configuration is loaded into the Single Board Computers (before system startup) and once the SIGTRAN feature is enabled within the system (at system installation), the SIGTRAN feature can be provisioned by the operator through the WebCI.

In order to operate, administer, and manage the components of a SIGTRAN network, a network operator needs to set and inspect certain values that characterize the configuration of the network components.

Collecting data prior to configuration

Collect all required information prior to configuration.

Collecting SS7 Point Code Data

The SS7 point codes are SS7 network addresses that uniquely identify every switch, Signal Transfer Point (STP). To communicate with the SS7 network, SS7 point codes must be obtained for the Tekelec SDM and for every SS7 network device that it will communicate with. The Tekelec ngHLR only supports one originating point code (OPC) and a minimum of one destination point code (DPC), one DPC per remote SS7 network device.

Collecting IP Addresses and Port Number

Local and Remote IP addresses must be defined to indicate the IP addresses that will be used by the Tekelec ngHLR and its peer nodes to communicate together using SIGTRAN. On the SDM system, two blades run SIGTRAN traffic in High Availability. A local IP address/mask and port number must be defined on each of these two blades, and the IP address and port number of the peers node must also be defined.

Collecting SS7 Route Data

An SS7 route must be defined for each Signalling End Point the Tekelec ngHLR wants to reach. There must be an SS7 route for each linkset. You must be ready to enter the following information about the SS7 route to be created:

- Destination Point Code (DPC)
- Originating Point Code (OPC)
- CombinedLinkset

Collecting Associations

An association refers to an SCTP association. The association provides the transport for the delivery of MTP3-User protocol data units and M3UA adaptation layer peer messages. An association must be created between the Tekelec ngHLR and each of its peer node. Since the Tekelec ngHLR works in High Availability, an IP association must be created for each of the system's blades running SIGTRAN traffic. Finally, in the case where the SDM communicates with one peer node using SIGTRAN, two SCTP associations must be created. The following information must be entered about each association:

- Remote IP Address(es) and Port
- Network (ITU)
- SCTSap

- PSP Type (SGP, IPsP)
- Associtation Type (Client or Server)

Collecting SS7 Subsystem Data

One route is defined for each destination subsystem that the SCCP layer may be used to access. The route defines the destination point code used to reach that subsystem as well as any backup point code which replicates the subsystem.

Collecting Concerned Point Code Data

Every remote SignallingPoint interested in knowing about the state changes of the Tekelec ngHLR node shall be configured. They will receive messages such as SSA (Subsystem Allowed), SSP (Subsystem Prohibited), and SSC (Subsystem Congested).

Collecting Global Title Data

All mobile subscriber terminals in a cellular network (e.g. GSM) are usually defined in a specific database, the HLR (i.e., Tekelec ngHLR). The addressing of an HLR node in the telecom network is usually based on the first, most significant half of a mobile subscribe number. When an HLR communicates over the SS7 signalling network, this address information has to be translated into a form that allows routing in the SCCP network. Some of the address information based on the global title series is called a Global Title (GT). A GT needs to be translated into a DPC by the SCCP in order to make it possible for the MTP to route the signalling messages through the SCCP network. The following information must be entered about the GTT to be created:

- Destination Point Code (DPC)
- Subsystem Number (SSN)
- Nature of Address (NA)
- Numbering Plan (NP)
- Digits of the Called or Calling Party Number
- Translation Type (TT)
- Address Indicator (Routing Indicator, GT Indicator, SSN Indicator, Dpc Indicator)
- Network Indicator (NI)

SS7 signaling configuration sequence using SIGTRAN

The SS7 logical node must be provisioned, modified or unprovisioned in specific sequences. Hereunder is a flow chart that provides an overview of these sequences for the configuration of the SS7 stack in the TUCL, M3UA and SCCP layers. Once all these steps have been followed, the TCAP and MAP layers must also be configured. For instructions on how to configure these last two layers, refer to *Configuring the TCAP layer* and *Configuring the MAP Layer* of this document.

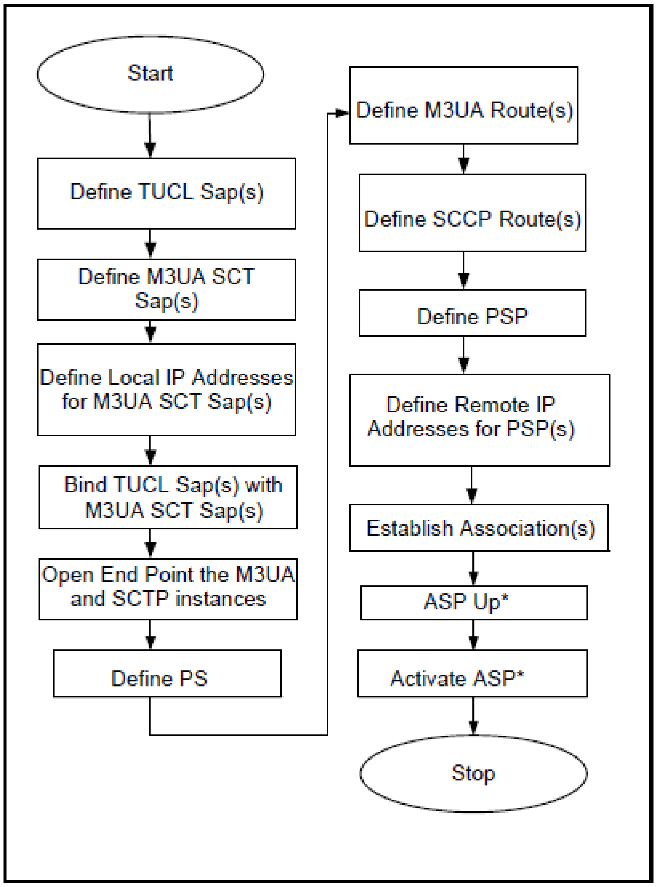

Start
Define TUCL Sap(s)
Define M3UA SCT Sap(s)
Define Local IP Addresses for M3UA SCT Sap(s)
Bind TUCL Sap(s) with M3UA SCT Sap(s)
Open End Point the M3UA and SCTP instances
Define PS
Define M3UA Route(s)
Define SCCP Route(s)
Define PSP
Define Remote IP Addresses for PSP(s)
Establish Association(s)
ASP Up*
Activate ASP*
Stop

Figure 34: SS7 Configuration Sequence When Using SIGTRAN

Note: The Activate PSP and ASP Up operations are done automatically if the Association has been configured as Client (in the M3UA window's PSP tab). In this case, this step can therefore be skipped.

However, for an Association that has been configured as Server, the activate PSP and ASP Up operations must be performed manually by the operator.

Note: The system supports SCTP multi-homing, which allows the Network Operator to configure the SCTP layer with different local/destination IP addresses and different routes in order to make the SS7/Diameter traffic travel from one node to another on different physical paths, through different networks.

Moreover, take note that the following steps are the same as the ones followed when configuring the SS7 Signaling stack using MTP2/SAAL and MTP3 protocols:

- Define Signaling Points (OPC and DPC)
- Define SCCP Route(s)

  For instructions on how to configure these components, refer to *Configuring SS7 Signaling Point Codes* and *Configuring SS7 Signaling Routes at the SCCP Layer*

  For instructions on the other steps, refer to *SIGTRAN configuration logic*

SIGTRAN configuration logic

The following logic must be followed to provision the Tekelec ngHLR with the SIGTRAN feature:

1. The Service Access Points (Sap) must be configured for each SIGTRAN layer: TUCL and M3UA.
2. For the TUCL layer, the Sap provider must be created.
3. For the M3UA layer, the SCTSap provider (using the previous TUCL Sap as provider) must be created.

   The list of local IP addresses (IP addresses of the Tekelec ngHLR) must be defined per SCTSap and the list of remote IP addresses (IP addresses of the peer nodes) that will be used for SIGTRAN must be defined per PSP.
4. For SCCP layer, the NSap user (using previous M3UA NSap provider) must be created.
5. The M3UA SCTSaps must be bound with the TUCL Saps by executing the Bind() operation and open-end-point between the M3UA and SCTP protocols must be executed with the OpenEndpoint() operation. Both operations are available in the M3UA layer's SCTSap.
6. The local and remote PS must be created.
7. A local route and remote M3UA route must be created for the PS.
8. The PSP (Peer Signalling Process) must be configured in the M3UA layer. When creating the PSP, the type must be defined (IPsP, SGP) as well as the association type (client or server), the reference to the Remote PS and the reference to the Remote IP address. Note that when the SGP type is selected, the association type can only be client.

   In the case where the association type is configured as "Server" or if it is the first time that the HLR service is started, the peer that is the client should bring the association up, if it doesn't, you can:
9. Establish the association by executing the EstablishAssociation() operation found in the PSP entity.
10. Set the applications to "ready" by executing the AspUp() operation found in the PSP entity.
11. Activate the applications by executing the ActivateAsp() operation found in the PSP entity.

    Note: If you configured the association as being client, the three steps above are done automatically.

The figure below shows the main logic that needs to be followed when provisioning the SIGTRAN feature.

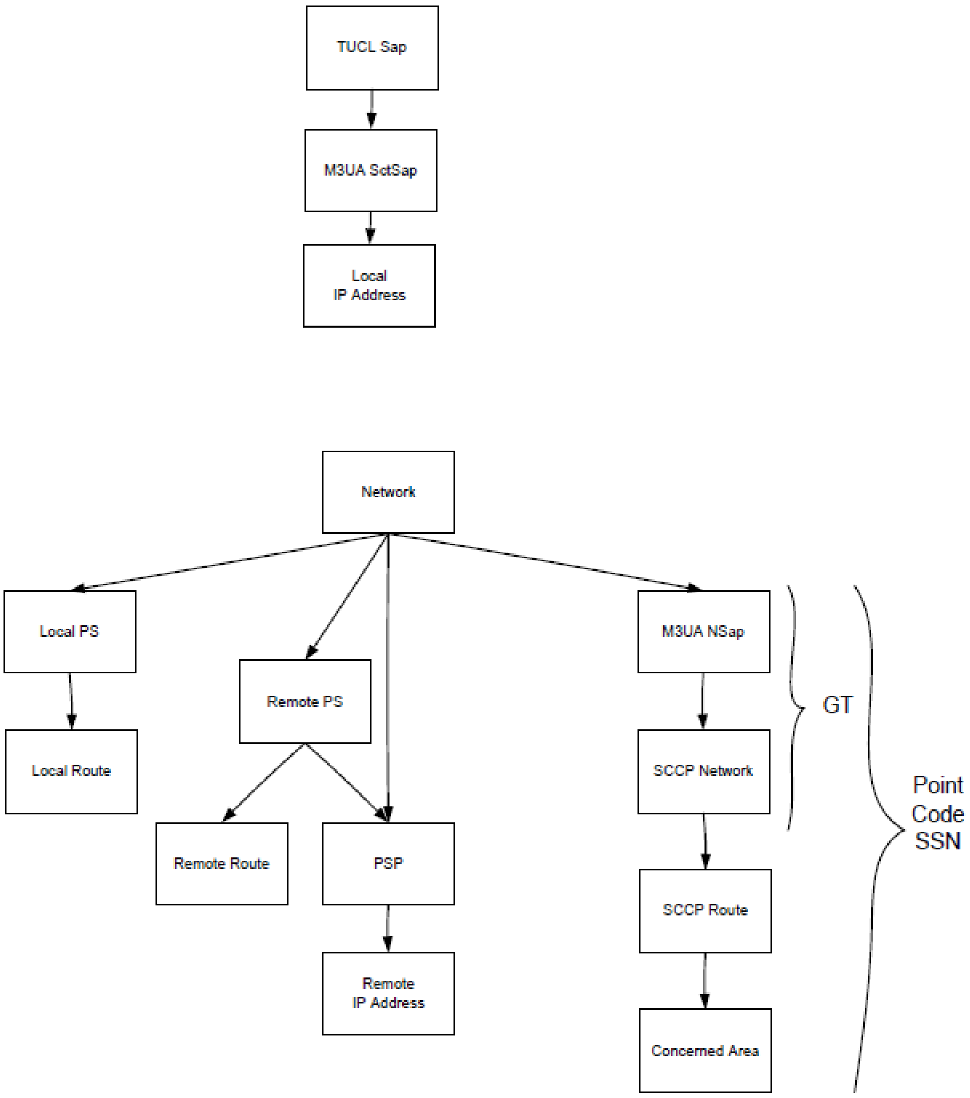


Figure 35: Provisioning Logic For The SIGTRAN (TUCL, M3UA) Protocols

Configuring and Binding Service Access Points (TSap, SCTSap)

The Interfaces used for SIGTRAN must be configured by following these steps:

1. The Service Access Points (Sap) must be configured for each SIGTRAN layer: TUCL and M3UA.

   This can be achieved from the WebCI's TUCL and M3UA windows. See description of windows below.
2. For the TUCL layer, the Sap provider must be created.
3. For the M3UA layer, the SCTSap user (using previous TUCL Sap provider) and NSap provider must be created.

The list of local IP addresses (IP addresses of the ngHLR) must be defined per SCTSap and the list of remote IP addresses (IP addresses of the peer nodes) that will be used for SIGTRAN must be defined per PSP. This can be achieved from the M3UA window (see description below).

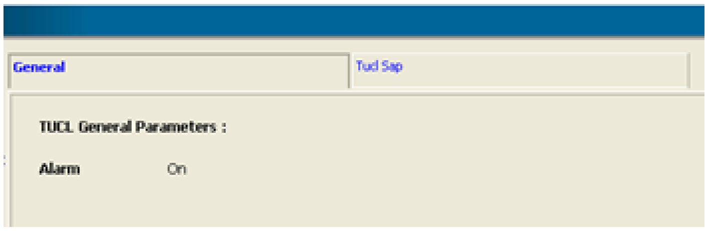
4. For the SCCP layer, the NSap user (using previous M3UA NSap provider) must be created. This can be achieved from the WebCI's SCCP window. For instructions on how to configure the NSap user, refer to section 4.1.15 Configuring SS7 Signaling Routes at the SCCP layer of this document.
5. The M3UA SCTSaps must be bound with the TUCL Saps by executing the Bind() operation and open-end-point between the M3UA and SCTP protocols must be executed with the OpenEndpoint() operation. Both operations are availableM3UA in the layer's SCTSap.

TUCL window

Requirements: Log in to a WebCI session with a valid username and password.

For help using the WebCI, refer to the section: "Using the WebCI" in both this document and the *SDM System Configuration – Reference Manual*.

The TUCL window is used to DISPLAY, ADD, MODIFY, and DELETE the parameters used to define the TUCL layer of the SS7 network using SIGTRAN. The following TUCL provisioning tabs are available: General, Tucl Sap. For more details on TUCL parameters, please refer to the *TUCL* section of the *SDM System Configuration - Reference Manual*.



TUCL General Parameters :

Alarm On

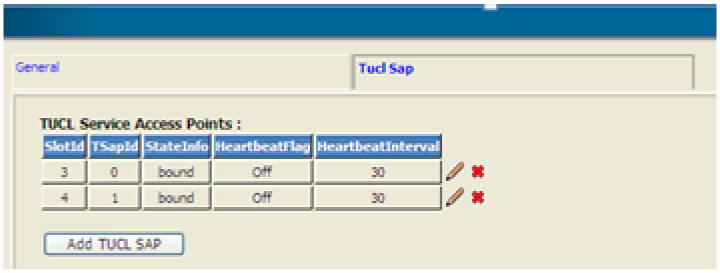
Figure 36: TUCL Window

General Tab

The General tab allows to view the TUCL General parameters.

Tucl Sap Tab

The Tucl Sap tab allows to provision TUCL Service Access Points (SAPs) on the slot on which runs the HLR service with SIGTRAN. More specifically, this window allows you to provision the Sap provider in the TUCL layer.



TUCL Service Access Points :

SlotId	TSapId	StateInfo	HeartbeatFlag	HeartbeatInterval
3	0	bound	Off	30
4	1	bound	Off	30

Figure 37: TUCL Sap Window

The following operations are supported for TUCL Service Access Points:

`Add TUCL SAP`: Add a new TUCL SAP. Note: You cannot add a TUCL Sap on a slot that does not exist. The following error message will appear:

```
Failed to create TuclSap, requested slot# do not have active TUCL layer
```

Important: A minimum of two TUCL SAPs should be configured on two different HLR Instances (on two different blades, for different SlotIds) in order to support High Availability failure.

✎ `Edit`: Modify an existing TUCL Sap definition.

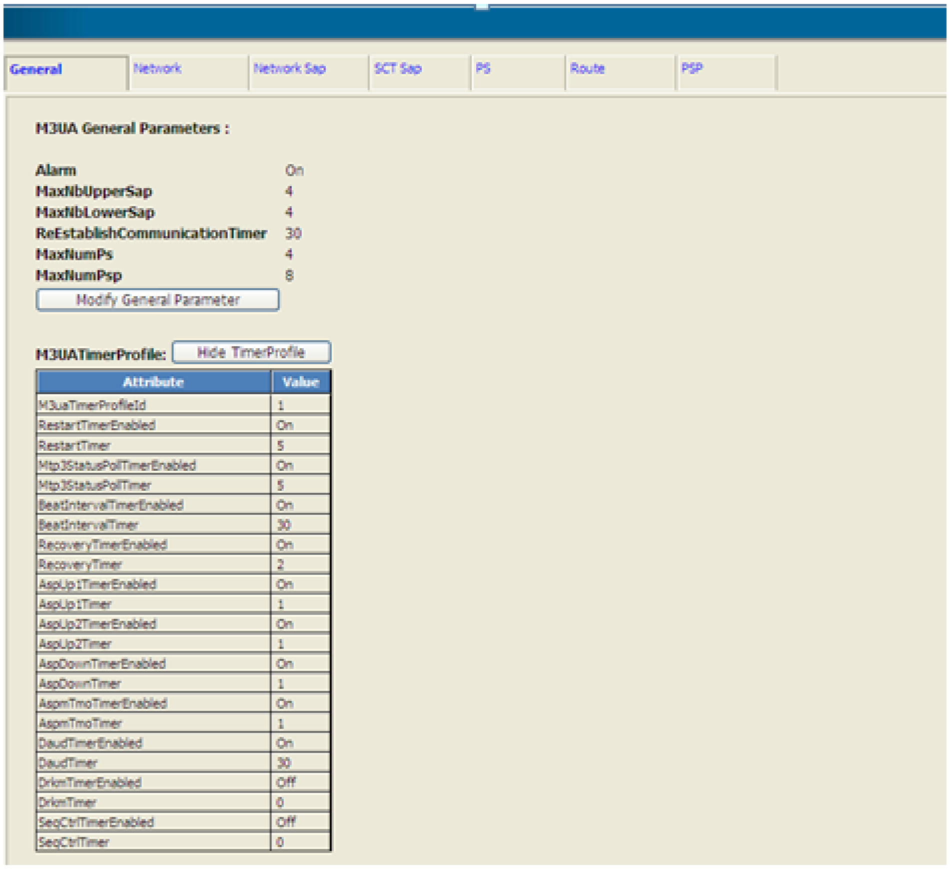
✖ `Delete`: Delete a TUCL SAP. Requirements: Before deleting the configuration of a TSap, the TSap must not be bound. The operation Unbind() must be executed for this TSap. Moreover, the M3UA SCTSap should also be deleted.

M3UA Window

Requirements: Log in to a WebCI session with a valid username and password.

For help using the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* .

The M3UA window is used to Display, Add, Modify, Delete, Activate, and Deactivate the parameters used to define the M3UA layer of the SS7 network using SIGTRAN. The following M3UA provisioning tabs are available: General, Network, Network Sap, SCT Sap, PS, Route, PSP. For more details on M3UA parameters, refer to the SS7 entities section of the *SDM System Configuration - Reference Manual* .



M3UA General Parameters :

Alarm	On
MaxNbUpperSap	4
MaxNbLowerSap	4
ReEstablishCommunicationTimer	30
MaxNumPs	4
MaxNumPsp	8

M3UATimerProfile:

Attribute	Value
M3uaTimerProfileId	1
RestartTimerEnabled	On
RestartTimer	5
Mtp3StatusPollTimerEnabled	On
Mtp3StatusPollTimer	5
BeatIntervalTimerEnabled	On
BeatIntervalTimer	30
RecoveryTimerEnabled	On
RecoveryTimer	2
AspUp1TimerEnabled	On
AspUp1Timer	1
AspUp2TimerEnabled	On
AspUp2Timer	1
AspDownTimerEnabled	On
AspDownTimer	1
AspmTmoTimerEnabled	On
AspmTmoTimer	1
DaudTimerEnabled	On
DaudTimer	30
DrkmTimerEnabled	Off
DrkmTimer	0
SeqCtrlTimerEnabled	Off
SeqCtrlTimer	0

Figure 38: M3UA Window

General Tab

The General tab allows to view and modify the M3UA General parameters.

The following operations are supported for M3UA General Parameters:

`Modify General Parameter`: Modify an existing M3UA General configuration.

`Display TimerProfile/Hide TimerProfile`: Display the Timer Profile parameters and their configured values/ Hide the Timer Profile parameters.

Network Tab

The M3UA window's Network tab allows to view the information of the network that SIGTRAN is using. This network is configured at installation of the system.

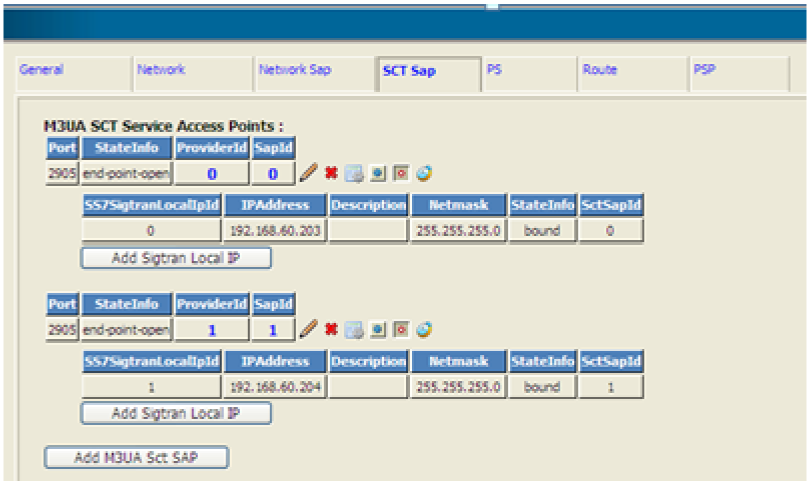
Note: Only one M3UA Network is defined. SIGTRAN runs only on ITU-T network for now.

Network Sap Tab

The Network Sap tab allows to view the M3UA Network Service Access Points (NSap) automatically created by system to define the interface between the SCCP and M3UA layers. One Network SAP is defined for each M3UA layer interface that the SCCP layer uses.

SCT Sap Tab

The SCT Sap tab allows to provision the SCT SAP in the M3UA layer and define the interface between the TUCL and M3UA layers. One SCT Sap is defined for each M3UA layer interface that the TUCL layer uses.



M3UA SCT Service Access Points :

Port	StateInfo	ProviderId	SapId
2905	end-point-open	0	0

SS7SigtranLocalIpId	IPAddress	Description	Netmask	StateInfo	SctSapId
0	192.168.60.203		255.255.255.0	bound	0

Port	StateInfo	ProviderId	SapId
2905	end-point-open	1	1

SS7SigtranLocalIpId	IPAddress	Description	Netmask	StateInfo	SctSapId
1	192.168.60.204		255.255.255.0	bound	1

Figure 39: M3UA SCT Sap Window

The following operations are supported for M3UA SCT SAP:

`Add M3UA Sct SAP`: Add a new M3UA SCT SAP and define the port.

*PROVISIONING NOTE: A M3UA's SCT Sap should be created for all existing instance(s) of TUCL Sap.

`Edit`: Display and modify M3UA SCT SAP and values associated with this SAP. Requirements: Before modifying the configuration of a SCTSap, the SCTSap must not be bound. The operation Unbind() must be executed for this SCTSap.

`Delete`: Delete an existing M3UA SCT SAP. Requirements: Before deleting the configuration of a SCTSap, the SCTSap must not be bound. The operation Unbind() must be executed for this SCTSap.

`Bind`: Bind and create a relation between the SCTSap user in the M3UA layer and its Sap provider in the TUCL layer.

`Unbind`: Delete the relation between the SCTSap user in the M3UA layer and its Sap provider in the TUCL layer. Note: This operation must be executed if you need to change anything in the configuration of the SCTSap user or provider.

`Open EndPoint`: Request to open an instance for this SCT Sap endpoint (this will locally bind this M3UA SCT Sap to its local IP interface).

`Add Sigtran Local IP`: Add local IP Addresses for a specific M3UA SCT Sap. The system supports multiple local IP addresses with the SCTP multi-homing functionality. One local IP address can be added at a time for a M3UA SCT Sap.

Local IP addresses cannot be deleted nor modified. You can only delete a local IP address by deleting its SCT Sap.

Configuring the PS

After defining the SAPs, the following must be configured:

The local and remote PS must be created in the M3UA layer.

To achieve this, you can provision the M3UA PS table in the M3UA window's PS tab.

PS Tab

The M3UA window's PS tab allows to define the PS (Peer Server) local and PS (Peer Server) remote for a PSP.

The following operations are supported for M3UA PS:

`Add M3UA Ps`: Add a new M3UA PS.

Note: Only one Local PS should be added. A Remote PS should be created for each destination route. Multiple PSPs can then be assigned to a PS. Multiple non-adjacent point codes and multiple alias point codes can also be configured.

`Delete`: Delete an M3UA PS. Requirements: Before deleting a PS, its associated Route and the PSPs referring to it must be deleted.

`Edit`: Modify an M3UA PS. Requirements: Before modifying a PS, you must manually deactivate the Application Server Process by deactivating the PSP. To do so, you must execute the AspDown() operation for the PSP to which the PS you wish to modify refers to.

Configuring Route(s)

After defining the PS and PSP, the following steps must be followed:

1. The M3UA Routes must be defined by following the steps below:
2. The Signaling Point Codes (DPC & OPC) must be defined.

   To achieve this, provision the MTP3 Signaling Points table in the MTP3 window's Signaling Points tab. Refer to section 0
3. Configuring SS7 Signaling Point Codes of this document.
4. A local route and remote route must be created for the PS.

   To achieve this, provision the M3UA Route table in the M3UA window's Route tab.

Route Tab

The M3UA window's Route tab allows to configure the M3UA Route and specify the destination signaling points that are accessible from the Signaling Point (SP) being configured. One route is required for each remote signaling point/network/cluster that is to be accessible from the SP being configured (DPC). Routes are used to route outgoing messages to the appropriate signaling IP associations. Each route is assigned to one IP association which may be used to reach that destination.

The following operations are supported for M3UA Route:

`Add M3UA Route`: Add a new M3UA Route. NOTE: One Route should be created for the OPC referring to the Local PS. Also, a Route should be created per DPC, referring to the Remote PSs. The SS7 components are added in a defined order to provide validation and sanity checking. Each PS should have a corresponding Route: one for the Local PS and one Route per remote PS.

`Delete`: Delete an M3UA Route.

For instructions on how to open a tab and on how to perform the different operations available from that tab, refer to *Web Craft Interface (WebCI)* of this document and "Operations available" from the *SDM System Configuration – Reference Manual* .

- The SCCP Routes must be defined. To achieve this, follow the same steps as described in *Configuring SS7 Signaling Routes at the SCCP Layer* of this document.

Configuring the PSP

After defining the SAPs, the following must be configured:

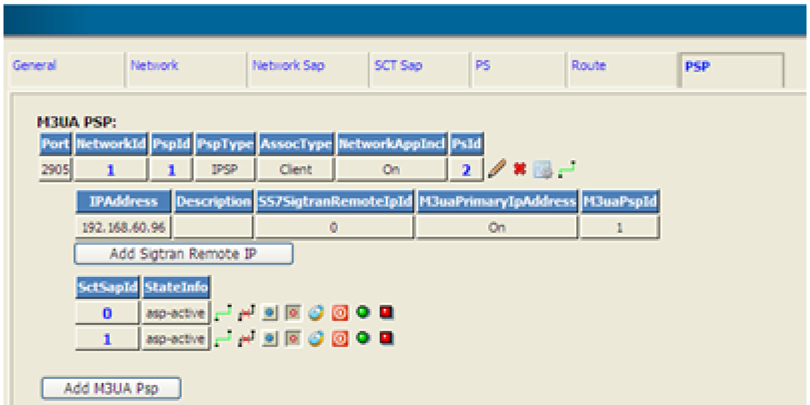
The PSP (Peer Signalling Process) must be configured in the M3UA layer.

When creating the PSP, the type must be defined (IPsP, SGP) as well as the association type (client or server), the reference to the Remote PS and the reference to the Remote IP address.

To achieve this, you can provision the M3UA PSP table in the M3UA window's PSP tab.

PSP (Peer Signalling Process) Tab

The PSP tab allows to create the IP associations between the Tekelec ngHLR and the peer nodes. It is used to define with which peer node the Tekelec ngHLR communicates with using Sigtran.



M3UA PSP:

Port	NetworkId	PspId	PspType	AssocType	NetworkAppInd	PsId
2905	1	1	IPSP	Client	On	2

IPAddress	Description	SS7SigtranRemoteIpId	M3uaPrimaryIpAddress	M3uaPspId
192.168.60.96		0	On	1

SctSapId	StateInfo
0	asp-active
1	asp-active

Figure 40: M3UA PSP Window

The following operations are supported for M3UA PSP:

`Add M3UA Psp`: Add a new M3UA PSP and define the remote port. NOTE: If the SDM only needs to communicate with one peer node to run SIGTRAN traffic, then an association must be established with the PSP through at least one of the end-points running on each slot and represented by the M3UA SCTSAP. If, for example, the SDM needs to communicate with another peer node, a second Remote PS, Remote Route and PSP must be added. One more Remote PSs should be created for each PSP. Multiple PSs can be assigned to a PSP. Multiple non-adjacent point codes and multiple alias point codes can be configured. The associations can be established through the same end-points used by the first PSP. The same logic applies to any scenario with multiple peer nodes running SIGTRAN traffic.

`Edit`: Modify an existing M3UA PSP. Requirements: Before modifying a PSP (IP association), you must firstly make sure that the Application Server process is down. You must terminate the association between the Tekelec ngHLR and the remote peer (PSP). To do so, you must execute the TerminateAssociation() operation.

Delete: Delete an M3UA PSP. Requirements: Before deleting a PSP, all its associations with the M3UA SCTSAPs must be terminated by executing the TerminateAssociation() operation.

Establish Association: Establish the association between the Tekelec ngHLR and the remote peer (PSP) through an SctSap.

Terminate Association: Terminate the association between the Tekelec ngHLR and the remote peer (PSP).

ASP Up: Indicate to the peer that the Application Server process is up and that the SIGTRAN applications are ready to receive traffic.

ASP Down: Indicate to the peer that the Application Server process is down and that the SIGTRAN applications are no longer ready to receive traffic.

Inhibit Psp: the PSP Association is not available to carry traffic.

Uninhibit Psp: the PSP Association is available to carry traffic.

Activate ASP: The ASP is active and can receive and process traffic.

Deactivate ASP: The ASP is deactivated and cannot receive nor process traffic.

Add Sigtran Remote IP. Add remote IP Addresses for a specific M3UA PSP. The system supports multiple remote IP addresses with the SCTP multi-homing functionality. One remote IP address can be added at a time for a M3UA PSP. When defining multiple remote IP addresses, one and only one remote IP address must be defined as the 'Primary' IP address (only one primary remote IP address must be defined for each association). For this, the 'M3uaPrimaryIpAddress' parameter has been implemented in the Sigtran Remote IP Address table. This indicates to the Tekelec ngHLR which IP address to use when connecting with the peer.

Provisioning TIP: The first remote IP Address defined must be the primary address (IP address to use when connecting with the peer).

Remote IP addresses cannot be deleted nor modified. You can only delete a remote IP address by deleting its PSP.

The status of each PSP association is available per M3UA SCT Sap in the PspState table.

Establishing Association and Activating ASP

In the case where the association type is configured as "Server" or if it is the first time that the HLR service is started, the peer that is the client should bring the association up, if it doesn't, you can:

- Establish the association by executing the EstablishAssociation() operation found in the PSP entity.
- Set the applications to "ready" by executing the AspUp() operation found in the PSP entity.
- Activate the applications by executing the ActivateAsp() operation found in the PSP entity.

Note: If you configured the association as being client, the three steps above are done automatically.

Chapter 5

HLR Features Configuration

Topics:

This chapter contains information pertaining to the configuration of HLR Features.

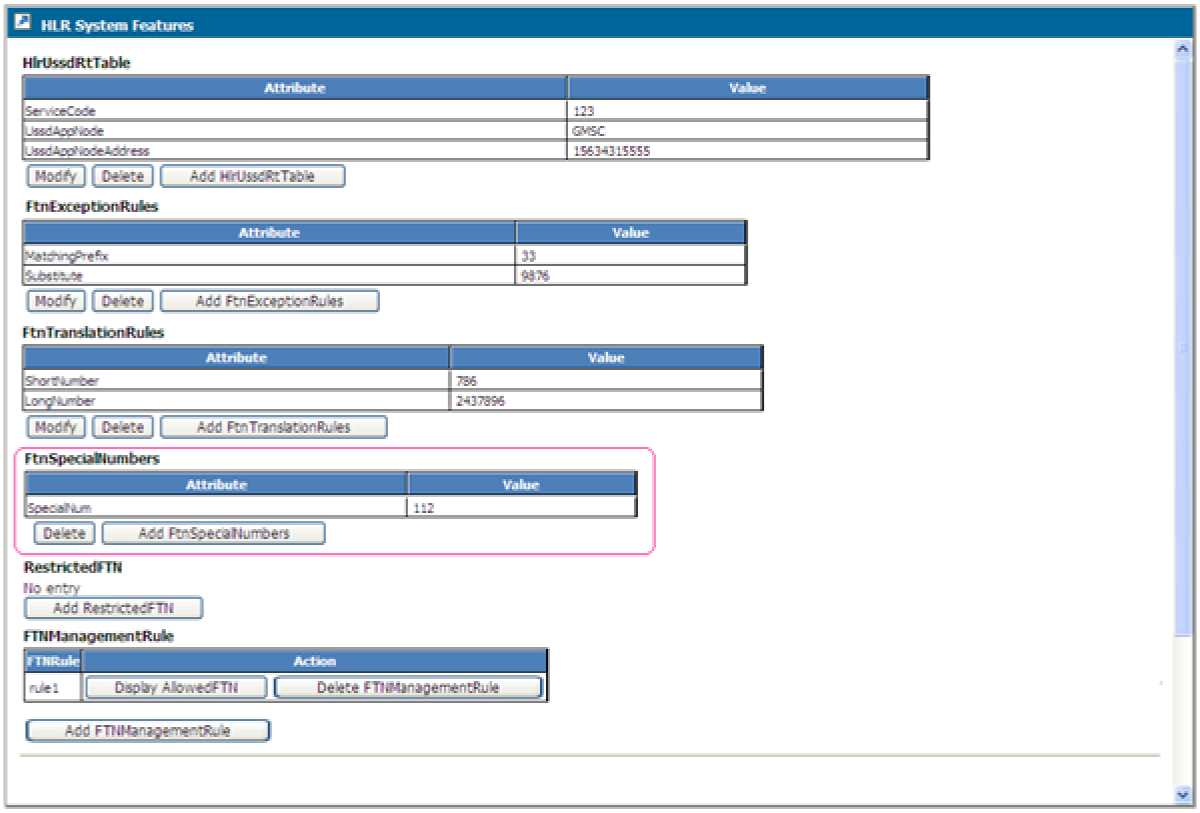
Provisioning Forward-To-Number rules for FTN Digits Analysis

This section describes how to provision FTN rules in the Tekelec ngHLR's database that will be used during FTN Digits Analysis upon receiving a RegSS with a FTN from one of its subscribers. Refer to the "FTN Digits Analysis" section of the *SDM Product Description* for more details on the functionality of this feature.

Defining FTN special numbers

The Network Operator can define special numbers (e.g. 911, 112, etc.) in the database and when the FTN provided in the RegSS message matches exactly one of these special numbers provisioned in the database, the Tekelec ngHLR refuses the RegSS message and doesn't store the FTN number in the database.

To define special numbers in the database, the Network Operator must provision the FtnSpecialNumbers table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu.



HlrUssdRtTable

Attribute	Value
ServiceCode	123
UssdAppNode	GMSC
UssdAppNodeAddress	15634315555

FtnExceptionRules

Attribute	Value
MatchingPrefix	33
Substitute	9876

FtnTranslationRules

Attribute	Value
ShortNumber	786
LongNumber	2437896

FtnSpecialNumbers

Attribute	Value
SpecialNum	112

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action
rule1	Display AllowedFTN Delete FTNManagementRule

Figure 41: Provisioning Special Numbers

In addition to provisioning the FtnSpecialNumbers table with new entries, the following operation is also available:

Delete. One entry at a time can be deleted from the FtnSpecialNumbers table.

Defining FTN short number translation rules on RegSS

The Short Number Translation on RegSS feature allows the operator to configure short numbers that can be translated into a full 3GPP-compliant international format FTN.

With this, subscribers may provide a short number (e.g. voice mail access number) or a national format as a "Forward-To Number" (FTN) when activating or registering their Call Forward service

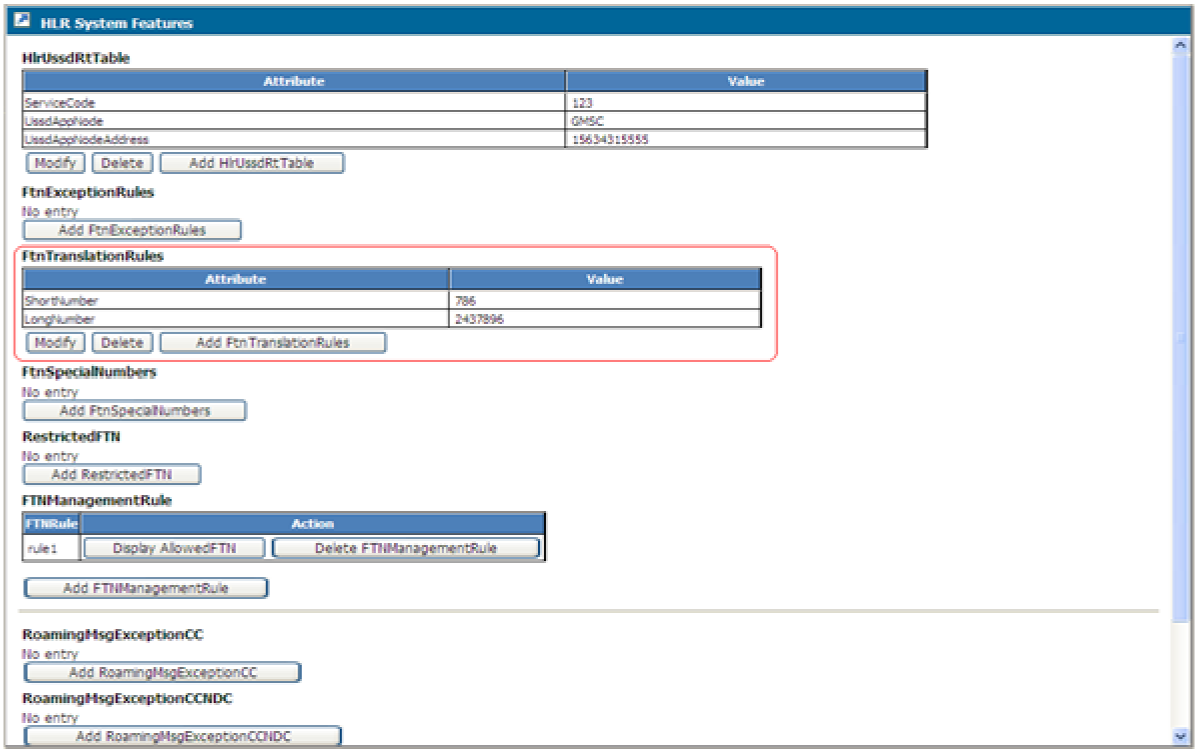
Short FTN's received in Register Supplementary Service (RegSS) messages are applied as a set of predefined and configurable rules and converted to a long number in E.164 format.

The long number is then used for all Call Forwarding services throughout the system.

Refer to the "Short Number translation on RegSS" section of the *SDM Product Description* for a more detailed description of the feature. Refer to the "HLR FTN Provisioning" section of the *SDM System Configuration – Reference Manual* for more details on the FtnTranslationRules entity and its parameters.

To achieve this, the operator must provision the FtnTranslationRules table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu. Prerequisite: The FTN Translation Rule feature must be enabled. Verify that the FtnTranslationOn parameter in the HlrConfig table is set to 'On'. Refer to *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* of this document for instructions on how to modify parameters in the HlrConfig table.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.



HlrUssdRtTable

Attribute	Value
ServiceCode	123
UssdAppNode	GMSC
UssdAppNodeAddress	15634315555

FtnExceptionRules

No entry

FtnTranslationRules

Attribute	Value
ShortNumber	786
LongNumber	2437896

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action	
rule1	Display AllowedFTN	Delete FTNManagementRule

RoamingMsgExceptionCC

No entry

RoamingMsgExceptionCCNDC

No entry

Figure 42: Provisioning Short Number Translation Rules

In addition to provisioning the FtnTranslationRules table with new entries, the following operation is also available:

Delete. One entry at a time can be deleted from the FtnTranslationRules table.

Modify. The LongNumber can be modified for each ShortNumber entry.

Note: Only the LongNumber parameter can be modified. If you wish to modify the key parameter ShortNumber, you must delete it and add a new ShortNumber as part of a new entry.

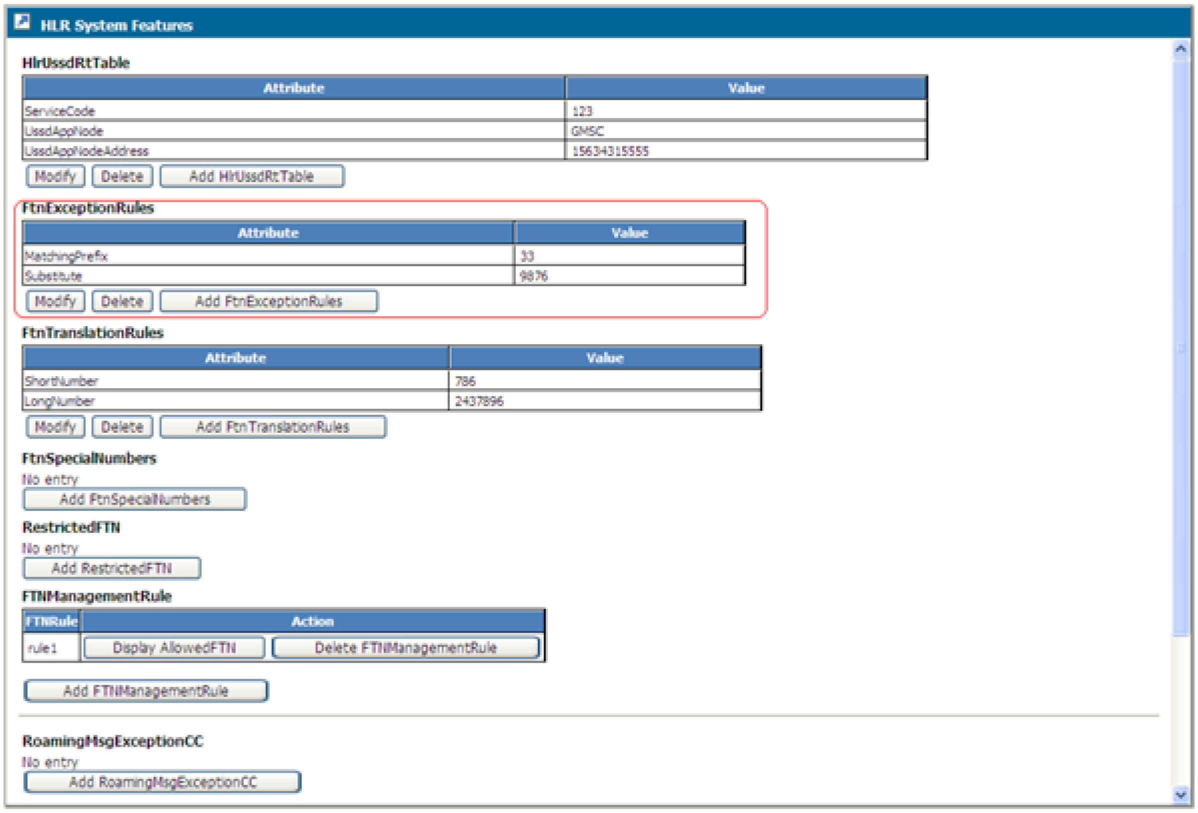
Defining FTN exception rules

The operator can provision some exception rules in the FTN formats and replace some prefixes with a substitute number that will ensure that the Tekelec ngHLR stores the FTN in the correct international format.

Refer to the "FTN Digits Analysis" section in the *SDM Product Description* for a description of the FTN Digits Analysis implemented in the Tekelec ngHLR and for details on when these exception rules are applied.

To achieve this, the operator must provision the FtnExceptionRules table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu. Prerequisite: The FTN Translation Rule feature must be enabled. Verify that the FtnTranslationOn parameter in the HlrConfig table is set to 'On'. Refer to *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* for instructions on how to modify parameters in the HlrConfig table.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.



HlrUssdRtTable

Attribute	Value
ServiceCode	123
UssdAppNode	GMSC
UssdAppNodeAddress	15634315555

FtnExceptionRules

Attribute	Value
MatchingPrefix	33
Substitute	9876

FtnTranslationRules

Attribute	Value
ShortNumber	786
LongNumber	2437896

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action
rule1	Display AllowedFTN Delete FTNManagementRule

RoamingMsgExceptionCC

No entry

Figure 43: Provisioning FTN Exception Rules

In addition to provisioning the FtnExceptionRules table with new entries, the following operation is also available:

Delete. One entry at a time can be deleted from the FtnExceptionRules table.

Modify. The Substitute number can be modified for each Prefix entry.

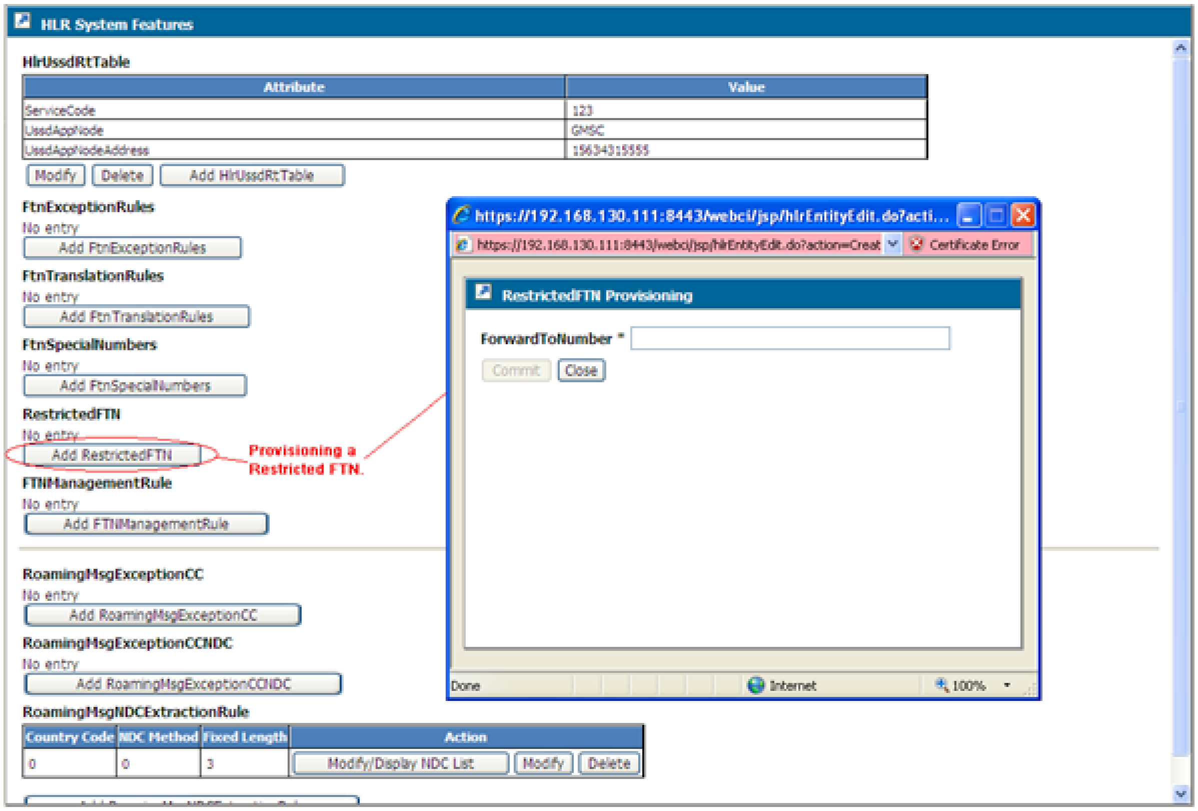
Note: Only the Substitute parameter can be modified. If you wish to modify the key parameter MatchingPrefix, you must delete it and add a new MatchingPrefix as part of a new entry.

Defining a Global FTN "black-list" (FTN Restrictions) for the ngHLR

The operator can choose to globally restrict some FTNs (for all subscribers) by defining a global list of restricted FTNs (black-list) in the Tekelec ngHLR configuration.

To achieve this, the operator must provision the RestrictedFTN table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.



HLR System Features

HlrUssdRtTable

Attribute	Value
ServiceCode	123
UssdAppNode	GMSC
UssdAppNodeAddress	15634315555

FtnExceptionRules

No entry

FtnTranslationRules

No entry

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

No entry

RoamingMsgExceptionCC

No entry

RoamingMsgExceptionCCNDC

No entry

RoamingMsgNDCExtractionRule

Country Code	NDC Method	Fixed Length	Action
0	0	3	Modify/Display NDC List Modify Delete

https://192.168.130.111:8443/webci/jsp/hlrEntityEdit.do?acti...

https://192.168.130.111:8443/webci/jsp/hlrEntityEdit.do?action=Creat

RestrictedFTN Provisioning

ForwardToNumber *

Provisioning a Restricted FTN.

Figure 44: Provisioning The HLR Restricted FTN Table

In addition to provisioning the RestrictedFTN table with a new entry, the following operation is also available:

Delete. On entry at a time can be deleted from the RestrictedFTN table.

Defining FTN Management Rules with FTN “white-list”

To allow the operator to better control the registration of the FTN(s) for each subscriber, the operator can define different lists of allowed FTN(s) (white-list), where each list corresponds to a “FTN Management Rule”, and can also assign each subscriber with one “FTN Management Rule” in its subscriber profile.

To achieve this, the operator must provision the following tables in the order presented below. These tables can be found in the WebCI’s HLR System Features window, which can be opened by extending the HLR folder from the WebCI’s menu.

1. The FTNManagementRule table must be provisioned to define a rule.

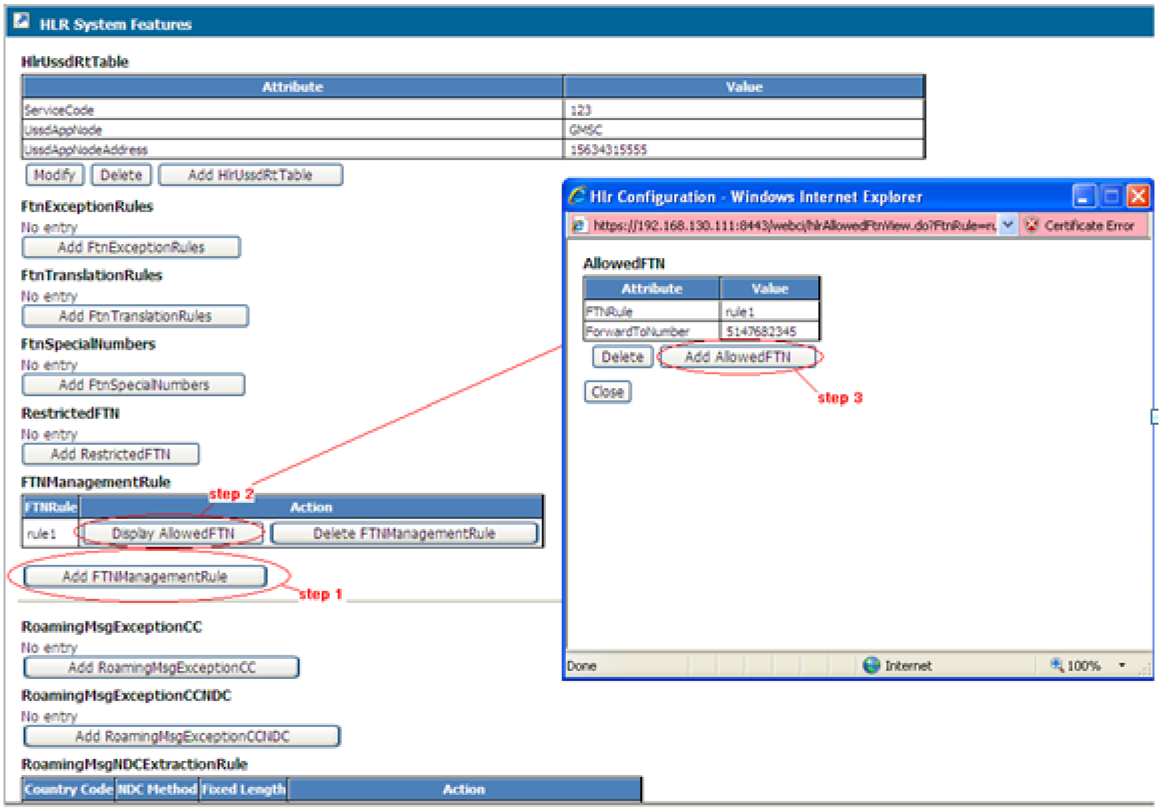
   This step can be repeated to define several rules.

2. Display the AllowedFTN table.

   NOTE: The button that allows to display this table only appears once at least one rule has been provisioned.

3. The AllowedFTN table must be provisioned to define an allowed FTN for a specific rule.

NOTE: A list of allowed FTNs can be defined for each rule. To do so, simply repeat this step by defining a different allowed FTN for the same rule.



HLR System Features

HlrUssdRtTable

Attribute	Value
ServiceCode	123
UssdAppNode	GMSC
UssdAppNodeAddress	15634315555

FtnExceptionRules

No entry

FtnTranslationRules

No entry

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action	
rule1	Display AllowedFTN	Delete FTNManagementRule

RoamingMsgExceptionCC

No entry

RoamingMsgExceptionCCNDC

No entry

RoamingMsgNDCExtractionRule

Country Code	NDC Method	Fixed Length	Action

Hlr Configuration - Windows Internet Explorer

https://192.168.130.111:8443/webci/hlrAllowedFtnView.do?FtnRule=ru

AllowedFTN

Attribute	Value
FTNRule	rule1
ForwardToNumber	5147682345

Figure 45: Provisioning FTN Management Rules With Allowed FTNs

Once rules have been defined with each a list of allowed FTNs, the operator can provision subscriber profiles that refer to a specific FTN Management rule defined in this table. To achieve this, the operator must specify the name of the rule in the Subscriber Profile's FTNRule parameter. When the Tekelec ngHLR receives a RegSS message from one of its subscribers, it will verify if a FTNRule is defined for that subscriber and if so will check if the FTN provided in the RegSS message matches one of the FTNs in the white-list and either accept or refuse the RegSS message. Refer to the *SDM Subscriber Provisioning – User Guide* for instructions on how to provision a subscriber profile using XML files. Refer to the *SDM Subscriber Provisioning – Reference Manual* for a description of the Subscriber Profile entity and the FTNRule parameter. *Refer to the SDM Troubleshooting, Monitoring, Maintenance – User Guide* for instructions on how to modify a Subscriber Profile from the WebCI and provision the FTNRule parameter.

In addition to provisioning the FTNManagementRule and AllowedFTN tables with new entries, the following operation is also available:

Delete. The following can be deleted:

a) The Delete button for the AllowedFTN table allows to delete one "allowed FTN" at a time from the list of allowed FTNs provisioned for a specific FTN Management rule.
b) The Delete button for the FTNManagementRule table allows to delete one FTN rule at a time.

Prerequisite: Prior to being able to delete a FTN Management Rule, all Subscriber Profiles that refer to it must be modified. There must be no subscriber profiles that refer to this FTN

Management rule. The FTNRule parameter in the Subscriber Profile table must be set to "Not Defined" (the default value).

Note: Deleting a FTN Management rule automatically deletes all allowed FTNs provisioned for that rule.

Provisioning CAMEL

The SDM supports CAMEL Phase 3. This section describes how to provision CAMEL at system level (HLR application). To provision the system with CAMEL functionalities, the following tables must be provisioned in the order presented hereby:

1. The Default Call Handling Override feature can be enabled (set to 'Continue' or 'Release') by modifying the DchOverride value.

   To do so, modify the Camel Config table.

   By default, it is set to 'Normal', which means that the DCH override feature is disabled. For more information on this feature, refer to the "System default call handling (DCH) override" section of the *SDM Product Description*.

2. The Camel Server Addresses must be defined along with the setting of the different Notification requests.

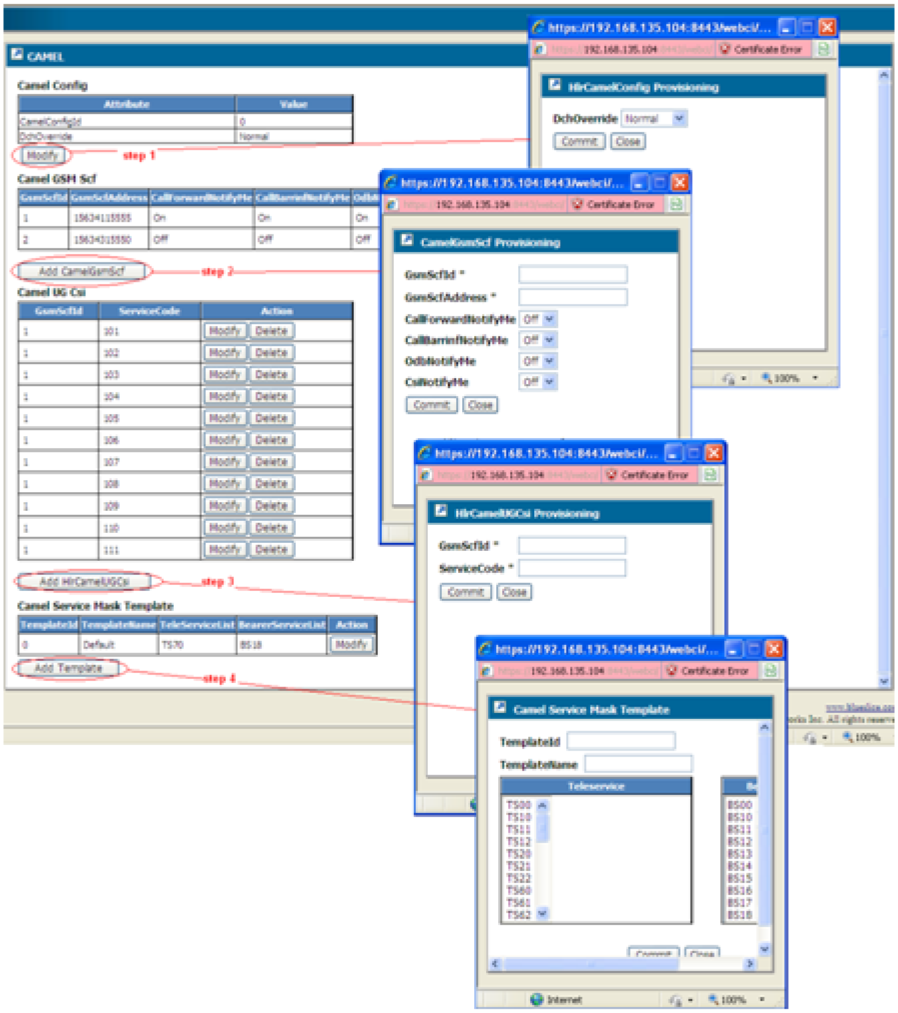
   This can be achieved by provisioning the Camel GSM Scf table from the CAMEL window, which can be accessed from the WebCI's HLR folder.

3. The USSD service codes must be defined and linked to a specific GsmScf address (already defined in the previous step).

   Note: these USSD service codes are applied to all subscribers. To achieve this, open the CAMEL window from the WebCI's HLR folder and provision the Camel UGCsi table.

4. One or several TS/BS Mask templates must be provisioned one at a time by defining a unique template identifier and by selecting the TeleService(s)/Bearer Service(s) the Tekelec ngHLR will need to suppress when applying this TS/BS Mask template.

   Templates are referenced in the subscriber profile during subscriber provisioning. Refer to the "Enhanced CAMEL handling" section of the *SDM Product Description* for a description of the CAMEL handling logic implemented in the Tekelec ngHLR and the use of these TS/BS Mask templates. To achieve this, open the CAMEL window from the WebCI's HLR folder and provision the Camel Service Mask Template.



CAMEL

Camel Config

Attribute	Value
CamelConfigId	0
OchOverride	Normal

Modify — step 1

Camel GSM Scf

GsmScfId	GsmScfAddress	CallForwardNotifyMe	CallBarrinNotifyMe	OdbN
1	15634115555	On	On	On
2	15634315550	Off	Off	Off

Add CamelGsmScf — step 2

Camel UG Csi

GsmScfId	ServiceCode	Action
1	101	Modify Delete
1	102	Modify Delete
1	103	Modify Delete
1	104	Modify Delete
1	105	Modify Delete
1	106	Modify Delete
1	107	Modify Delete
1	108	Modify Delete
1	109	Modify Delete
1	110	Modify Delete
1	111	Modify Delete

Add HlrCamelUGCsi — step 3

Camel Service Mask Template

TemplateId	TemplateName	TeleServiceList	BearerServiceList	Action
0	Default	TS70	BS18	Modify

Add Template — step 4

HlrCamelConfig Provisioning

OchOverride: Normal

CamelGsmScf Provisioning

GsmScfId *

GsmScfAddress *

CallForwardNotifyMe: Off

CallBarrinNotifyMe: Off

OdbNotifyMe: Off

CsiNotifyMe: Off

HlrCamelUGCsi Provisioning

GsmScfId *

ServiceCode *

Camel Service Mask Template

TemplateId

TemplateName

Teleservice	Be
TS00 TS10 TS11 TS12 TS20 TS21 TS22 TS60 TS61 TS62	BS00 BS10 BS11 BS12 BS13 BS14 BS15 BS16 BS17 BS18

https://192.168.135.104:8443/webci/...
https://192.168.135.104:8443/webci/
Certificate Error
Commit
Close
Internet
100%

Figure 46: Camel GsmScf Provisioning Window

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to Web Craft Interface (WebCI) in both this document and the *SDM System Configuration – Reference Manual* document.

Note: Further CAMEL provisioning can be done on a per-subscriber basis when provisioning the subscribers profiles. Refer to the *SDM Subscriber Provisioning – Reference Manual* for information on the different parameters that can be provisioned for CAMEL handling from a subscriber's profile and to the *SDM Subscriber Provisioning – User Guide* for instructions on how to provision a subscriber profile through XML files or on how to edit it from the WebCI.

Provisioning Roaming Welcome Notifications

This section describes how to provision the Roaming Welcome Notification feature. The roaming welcome messages feature allows the ngHLR to notify a server when it receives a MAP Location_Update or MAP Location_Update_for_GPRS message, with a country code different from the previously registered one.

For a description of the feature and the conditions that need to be met for the Tekelec ngHLR to send a notification to the server, refer to the "Roaming Welcome Notification" section of the *SDM Product Description* .

For more details on the how the Tekelec ngHLR provides an XML interfaces for sending external notification when a subscriber is successfully roaming in a different country, please refer to the *ID-0020 SDM Roaming Welcome Message XML Interface* description document.

Setting roaming welcome notification exceptions for CCs, CC-NDCs and the NDC extraction rule

The Tekelec ngHLR notifies a server when it receives a MAP Location_Update or MAP Location_Update_for_GPRS message with:

- A country code (CC) different from the previously registered one.
- A country and National Destination Code (CC-NDC) different from the previously registered one.
- An IMSI different from the previously registered one.

Prior to being able to send these notifications, the operator must enable the feature and configure the Tekelec ngHLR with the type of change that should trigger a notification. To achieve this, the operator must provision the "RoamingMsgOn" parameter in the HlrConfig table with one of the following values:

- Off (The Roaming Welcome Notification feature is disabled)
- Notify on CC changes or IMSI change (The Roaming Welcome Notification feature is enabled and notifications are sent when the CC is different from the previously registered one)
- Notify on CC-NDC changes or IMSI change (The Roaming Welcome Notification feature is enabled and notifications are sent when the CC-NDC is different from the previously registered one)

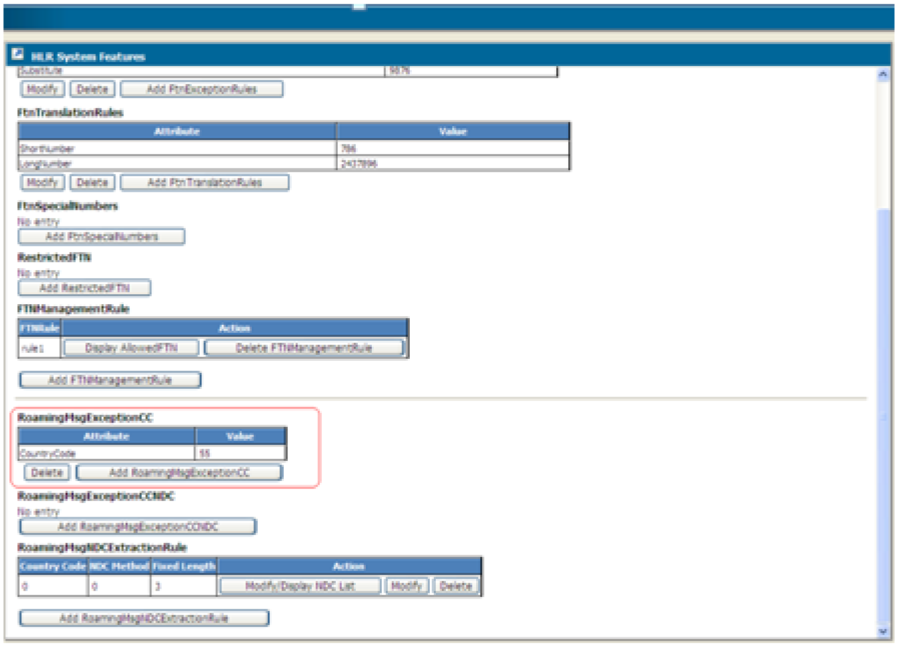
Refer to *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* in this document for details on how to set the value (modify) for the "RoamingMsgOn" parameter in the HlrConfig table. Refer to the *SDM System Configuration – Reference Manual* for more details on the HlrConfig entity and its parameters, values and default values.

Now in the cases where the feature is not disabled, the operator can provision a list of CCs and CC-NDCs that are an exception to the roaming welcome notification service. This means, for example, that when the Tekelec ngHLR is set to "Notify on CC changes" the Tekelec ngHLR will never send a notification for the CCs in this list.

Provisioning a List of CCs as Exception

To provision a list of CCs that are an exception to the roaming welcome notification service, you must provision the RoamingMsgExceptionCC table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.



Substitute	9876

FtnTranslationRules

Attribute	Value
ShortNumber	786
LongNumber	2437896

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action
rule1	Display AllowedFTN Delete FTNManagementRule

RoamingMsgExceptionCC

Attribute	Value
CountryCode	55

RoamingMsgExceptionCCNDC

No entry

RoamingMsgNDCExtractionRule

Country Code	NDC Method	Fixed Length	Action
0	0	3	Modify/Display NDC List Modify Delete

Figure 47: Provisioning A List Of CCs As An Exception To The Roaming Welcome Notification

In addition to provisioning the RoamingMsgExceptionCC table with a new entry, the following operation is also available:

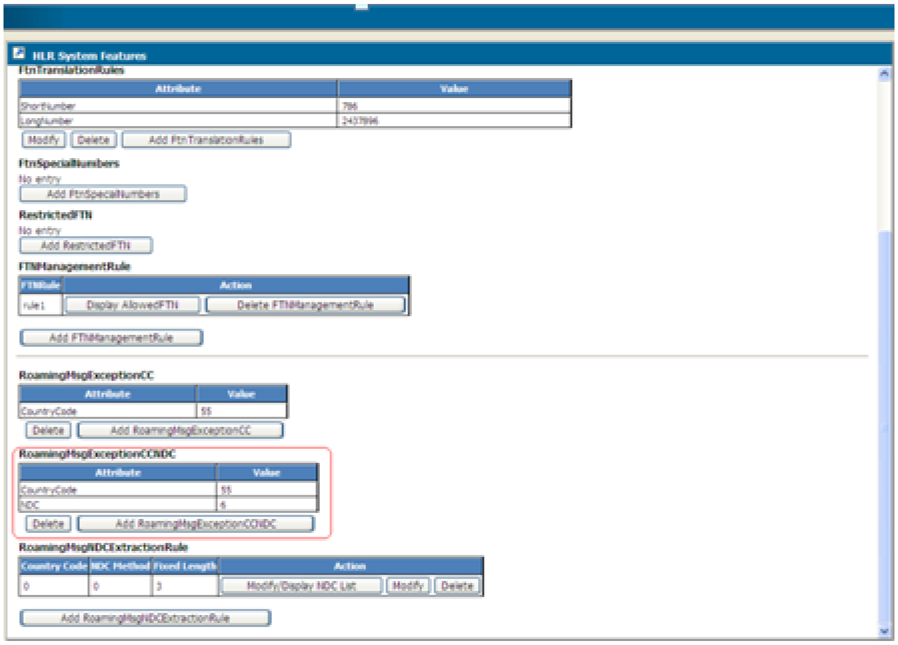
Delete. One entry at a time can be deleted from the RoamingMsgExceptionCC table.

Provisioning a list of CC-NDCs as exception

To provision a list of CC-NDCs that are an exception to the roaming welcome notification service, you must provision the RoamingMsgExceptionCCNDC table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu.

Prerequisite **to provision the RoamingMsgExceptionCCNDC table:** Prior to adding a RoamingMsgExceptionCCNDC entry, the CC must already be defined in the RoamingMsgExceptionCC table. Refer to section above to know how to provision the RoamingMsgExceptionCC table.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.



FtnTranslationRules

Attribute	Value
ShortNumber	786
LongNumber	2437896

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action
rule1	

RoamingMsgExceptionCC

Attribute	Value
CountryCode	55

RoamingMsgExceptionCCNDC

Attribute	Value
CountryCode	55
NDC	6

RoamingMsgNDCExtractionRule

Country Code	NDC Method	Fixed Length	Action
0	0	3	

Figure 48: Provisioning A List Of CC-NDCs As An Exception To The Roaming Welcome Notification

In addition to provisioning the RoamingMsgExceptionCCNDC table with a new entry, the following operation is also available:

Delete. One entry at a time can be deleted from the RoamingMsgExceptionCCNDC table.

It is important to note that the XML notifications can also be turned On/Off on a per subscriber (Primary IMSI) basis. Of course, it can only be turned On if it is enabled at system level, in the RoamingMsgOn parameter of the HlrConfig entity. To provision this feature on a per-subscriber basis, the operator can set the "SubsRoamingMsgOn" parameter to On/Off in subscriber profiles. Refer to the *SDM Subscriber Provisioning – User Guide* for instructions on how to provision subscriber profiles using XML files. Refer to the *SDM Subscriber Provisioning – Reference Manual* for details on the SubsRoamingMsgOn parameter in the SubscriberProfile entity. Refer to the *SDM Troubleshooting, Monitoring, Maintenance – User Guide* document for instructions on how to modify the Subscriber Profile of a subscriber from the WebCI.

Provisioning a list of CC-NDCs as exception

To provision a list of CC-NDCs that are an exception to the roaming welcome notification service, you must provision the RoamingMsgExceptionCCNDC table located in the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu.

Prerequisite to provision the RoamingMsgExceptionCCNDC table: Prior to adding a RoamingMsgExceptionCCNDC entry, the CC must already be defined in the RoamingMsgExceptionCC table. Refer to section above to know how to provision the RoamingMsgExceptionCC table.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to the section: "Using the WebCI" in both this document and the SDM System Configuration – Reference Manual document.

In addition to provisioning the RoamingMsgExceptionCCNDC table with a new entry, the following operation is also available:

Delete. One entry at a time can be deleted from the RoamingMsgExceptionCCNDC table.

It is important to note that the XML notifications can also be turned On/Off on a per subscriber (Primary IMSI) basis. Of course, it can only be turned On if it is enabled at system level, in the RoamingMsgOn parameter of the HlrConfig entity. To provision this feature on a per-subscirber basis, the operator can set the "SubsRoamingMsgOn" parameter to On/Off in subscriber profiles. Refer to the SDM Subscriber Provisioning – User Guide for instructions on how to provision subscriber profiles using XML files. Refer to the SDM Subscriber Provisioning – Reference Manual for details on the SubsRoamingMsgOn parameter in the SubscriberProfile entity. Refer to the SDM Troubleshooting, Monitoring, Maintenance – User Guide document for instructions on how to modify the Subscriber Profile of a subscriber from the WebCI.

Provisioning NDC Extraction Rule

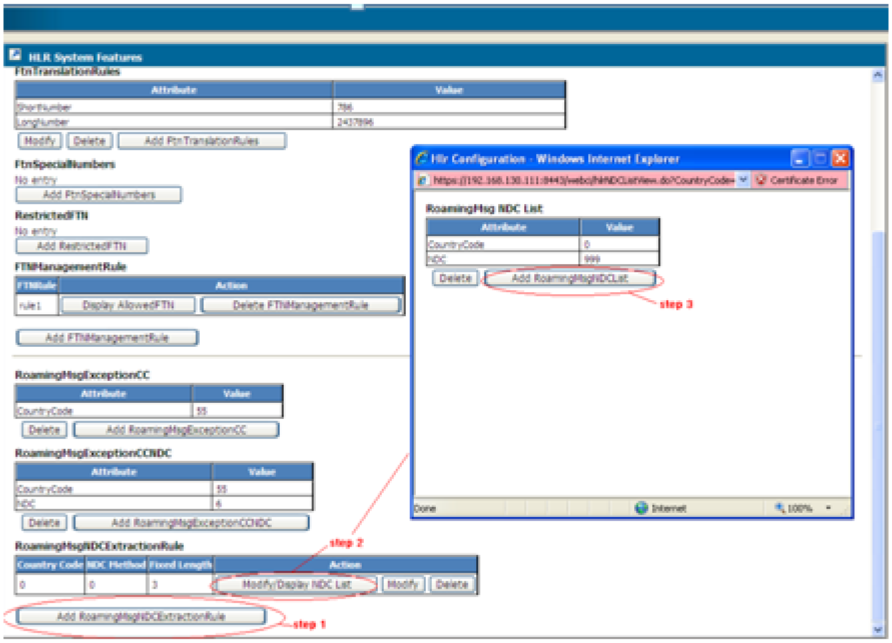
In the case where the Tekelec ngHLR is set to "Notify on CC-NDC changes", the Tekelec ngHLR extracts the CC as per the ITU assignment rules and verifies in the RoamingMsgNDCExtractionRule entity which method is defined for this CC in order to extract the NDC from the VLR GT (e.164 global title).

The operator can define for a specific CC the method that the Tekelec ngHLR needs to use to extract the NDC. For a description of the NDC extraction rule and each method that can be used by the Tekelec ngHLR, refer to the "XML Notifications on NDC change or IMSI change" section of the *SDM Product Description.*

To achieve this, the operator must provision the following from the WebCI's HLR System Features window, which can be opened by extending the HLR folder from the WebCI's menu:

1. The RoamingMsgNDCExtractionRule table must be provisioned first to define for a specific CC the method that the Tekelec ngHLR needs to use to extract the NDC.
2. The RoamingMsgNDCList table must be displayed by clicking on the Modify/Display NDC List button.
3. The RoamingMsgNDCList table must be provisioned to define a list of shared country codes and their corresponding NDC list in which roaming welcome messages are sent if the CC-NDC changes. NOTE: This table only needs to be provisioned for the CC for which the roaming message NDC extracting rule is the NDC list method.

   For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



FtnTranslationRules

Attribute	Value
ShortNumber	786
LongNumber	2437896

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

FTNRule	Action
rule1	Display AllowedFTN Delete FTNManagementRule

RoamingMsgExceptionCC

Attribute	Value
CountryCode	55

RoamingMsgExceptionCCNDC

Attribute	Value
CountryCode	55
NDC	6

RoamingMsgNDCExtractionRule

Country Code	NDC Method	Fixed Length	Action
0	0	3	Modify/Display NDC List Modify Delete

RoamingMsg NDC List

Attribute	Value
CountryCode	0
NDC	999

Figure 49: Provisioning NDC Extraction Method

In addition to provisioning the RoamingMsgNDCExtractionRule and RoamingMsgNDCList tables with new entries, the following operations are also available:

Delete. The following can be deleted:

Each entry of the RoamingMsgNDCExtractionRule table can be deleted one at a time.

Note: Deleting an entry in this table will also delete the list of NDCs provisioned for it in the case where it had been provisioned with the NDC method.

Each entry of the RoamingMsgNDCList table can be deleted one at a time.

Modify. Each entry in the RoamingMsgNDCExtractionRule table can be modified one at a time.

Provisioning USSD application nodes for the routing of USSD messages

This section describes how to provision the USSD Application Nodes to which the Tekelec ngHLR may have to route USSD messages to.

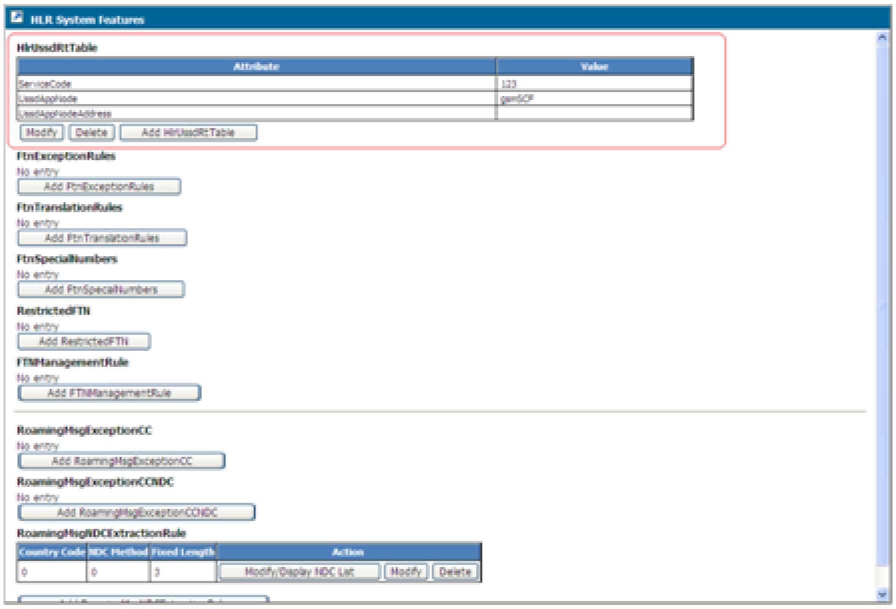
This can be achieved by provisioning the HlrUssdRtTable from the HLR System Features window, which can be accessed from the WebCI's HLR folder.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

For details on the USSD table parameters, refer to the “HLR USSD Routing Table” section of the “HLR entities” chapter in the *SDM System Configuration - Reference Manual* .

The operations available when provisioning the HlrUssdRtTable are as follows: Add, Modify, Delete.

Requirements when adding an entry in the HlrUssdRtTable: In the case where you want to add a USSD Routing Table entry with a UssdAppNode = gsmSCF, do not enter the Application Node Address when defining the entry. In addition to this, you must add a HlrCamelUGCsi entry and a CamelGsmScf entry (in which you will have to enter the Gsm Scf Address). Refer to *Provisioning CAMEL* for instructions on the provisioning of the CamelGsmScf and HlrCamelUGCsi tables.



HLR System Features

HlrUssdRtTable

Attribute	Value
ServiceCode	123
UssdAppNode	gsmSCF
UssdAppNodeAddress	

FtnExceptionRules

No entry

FtnTranslationRules

No entry

FtnSpecialNumbers

No entry

RestrictedFTN

No entry

FTNManagementRule

No entry

RoamingMsgExceptionCC

No entry

RoamingMsgExceptionCCNDC

No entry

RoamingMsgNDCExtractionRule

Country Code	NDC Method	Fixed Length	Action
0	0	3	Modify/Display NDC List Modify Delete

Figure 50: HLR USSD Routing Table

Roaming controls

This section describes firstly how to set roaming controls and secondly how to calculate the list of Nodes (VLR/GMSC) affected by specific changes made to this roaming control data.

Setting Roaming Controls (Operator Controlled PLMN, Roaming Restrictions and Service Screening Restrictions)

The Tekelec ngHLR offers to the Network Operator, the capability of controlling some of the Tekelec ngHLR's behaviour when a subscriber is roaming. It offers to the Network Operators the ability to customize some features or services on a per roaming PLMN basis.

Currently it consists in giving the operator the ability to:

Define roaming PLMNs as a group of Node ranges (VLR/GMSC address range).

Define Service Screening Templates allowing to Control individual subscriber services like BAOC override mask, Camel Data, etc

Create OCPLMN Templates in order to:

Create "allowed" ("white-listed") PLMN-IMSI combinations (roaming restrictions), by assigning to each OCPLMN Template a list of roaming PLMNs and then defining a list of "allowed IMSIs" for each of those roaming PLMNs.

The Tekelec ngHLR only accepts Update Locations coming from one of these “allowed” PLMN-IMSI combinations defined in the system.

Assign a Service Screening Template to each of the OCPLMN Templates’ roaming PLMN.

In the case where the PLMN-IMSI combination is “allowed” for the UL received and the roaming service screening feature is enabled, the Tekelec ngHLR retrieves the correct Service Screening Template (based on the OCPLMN Template assigned to the subscriber and on the roaming PLMN from which the UL was received) and applies it against the provisioned Subscriber’s services. The Update Location continues with thus tailored Subscriber Profile, as modified by the service screening rules.

Each subscriber can have a different OCPLMN Template assigned to it, by provisioning the Subscriber Profile with the name of the OCPLMN Template. For more information on the ‘OCPLMNTemplateName’ parameter from the Subscriber Profile that can be set to refer to one of these templates, refer to the *SDM Subscriber Provisioning - Reference Manual* and for instructions on how to provision the Subscriber Profile from the WebCI, refer to the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

When receiving an Update Location for a subscriber, the Tekelec ngHLR will use the OCPLMN Template assigned to that subscriber in order to identify the roaming PLMN and apply the roaming restrictions and service screening restrictions defined for that PLMN.

The WebCI’s Roaming Controls window allows the operator to set all the roaming controls described above (PLMN Definitions, Service Screening Templates Definitions and OCPLMN Templates definitions). To achieve this, follow the steps described below:

Prerequisite: By default, the roaming restrictions (PLMN-IMSI selection) and Service Screening restrictions features are disabled unless you purchased the features. Contact the Tekelec’s Sales team to purchase one or both of them. Both of these features can independently be enabled/disabled dynamically from the WebCI, by setting the Hlr Roaming Controls Config table’s ‘RoamRestrictEnable’ and/or ‘RoamServiceScreeningEnable’ parameters to ‘1’ (enabled) or ‘0’ (disabled).

1. Define the roaming PLMNs with a list of Node Ranges (VLR/GMSC address ranges) by following these steps:

   Click on the `Add Plmn` button of the Plmn Definitions table. One entry can be provisioned at a time, so in order to define multiple roaming PLMNs, simply provision the Plmn Definitions table with a new entry one after the other until all roaming PLMNs are defined.

   One Node range (VLR/GMSC range) can be defined at a time, by clicking on the `Add VLR` button available for a specific roaming PLMN. Simply repeat this as many times as the number of Node ranges you wish to define for a roaming PLMN.

   A default PLMN is created at system start up. This default PLMN doesn’t have any VLR/GMSC nodes associated to it.

2. Optional step that is only required if you want to assign Service Screening Templates to the OCPLMN Templates’ roaming PLMNs.

   The Service Screening Templates are used by the OCPLMN Templates in order to customize the Subscriber Profile based on the PLMN where the subscriber is roaming.

   a) Define Service Screening Templates by clicking on the `Add Service Screening Template` button located under the Service Screening Templates Definitions table.

      At system start-up a Service Screening Template with Name = “Not Defined” and Id = 0 is created without customization of any services. This template is used as default for the creation of any OCPLMN Templates.

b) Add service customization for the defined Service Screening Templates (other than the Service Screening Template = 'Not Defined').

By default, the Service Screening Template is created without any BAOC customization (empty BAOC BSG List) and without any Camel Data customization (empty CSI key list to suppress) or any other service customization.

In order to add customization of some services (CSI Key To Suppress from O-CSI, BAOC per BSG, Camel – max Camel Version Allowed, ODB (All Outgoing, All Outgoing Intl, Premium), TeleServices(TS91, TS92), BearServices (BS1F, BS17), Other services - CLIP, CLIR, COLP, COLR, CW, HOLD, MPTY, REGSUBSCRIPTION, CFB, CRNRc, CFNRy) for a Service Screening Template, you must add them individually, one at a time, by clicking on the corresponding buttons (**Add CSI, Add BSG, Add TS, Add BS, Add SS, Add ODB**) available for each Service Screening Template defined in the Service Screening Templates Definitions table.

3. Create OCPLMN Templates by provisioning the OCPLMN Template Definitions table.

a) Define OCPLMN Templates by clicking on the **Add OCPLMN Template** button located at the top of the OCPLMN Templates Definitions table.

At system start-up, an OCPLMN Template with OCPLMN Template Name = "Not Defined" is created by the system. The Template is used as default for all new subscribers. It is created for the purpose to denote that the subscriber does not have any Roaming restrictions or Service Screening to be applied. By using OCPLMN template = "Not Defined, the feature can be turned OFF on a per subscriber basis. The "Not Defined OCPLMN Template" cannot have any PLMNs assigned to it.

b) Assign roaming PLMNs to the defined OCPLMN Templates. To achieve this, click on the `Add Plmn` button available for the OCPLMN Template for which you wish to add a roaming PLMN. When assigning a roaming PLMN to an OCPLMN Template, the following can optionally also be defined for that roaming PLMN:

1. a Service Screening Template (among the ones defined in the Service Screening Templates Definitions (see step 2)). Only one Service Screening Template can be assigned per roaming PLMN.
2. the type of node to which the roaming and service screening restrictions apply to.

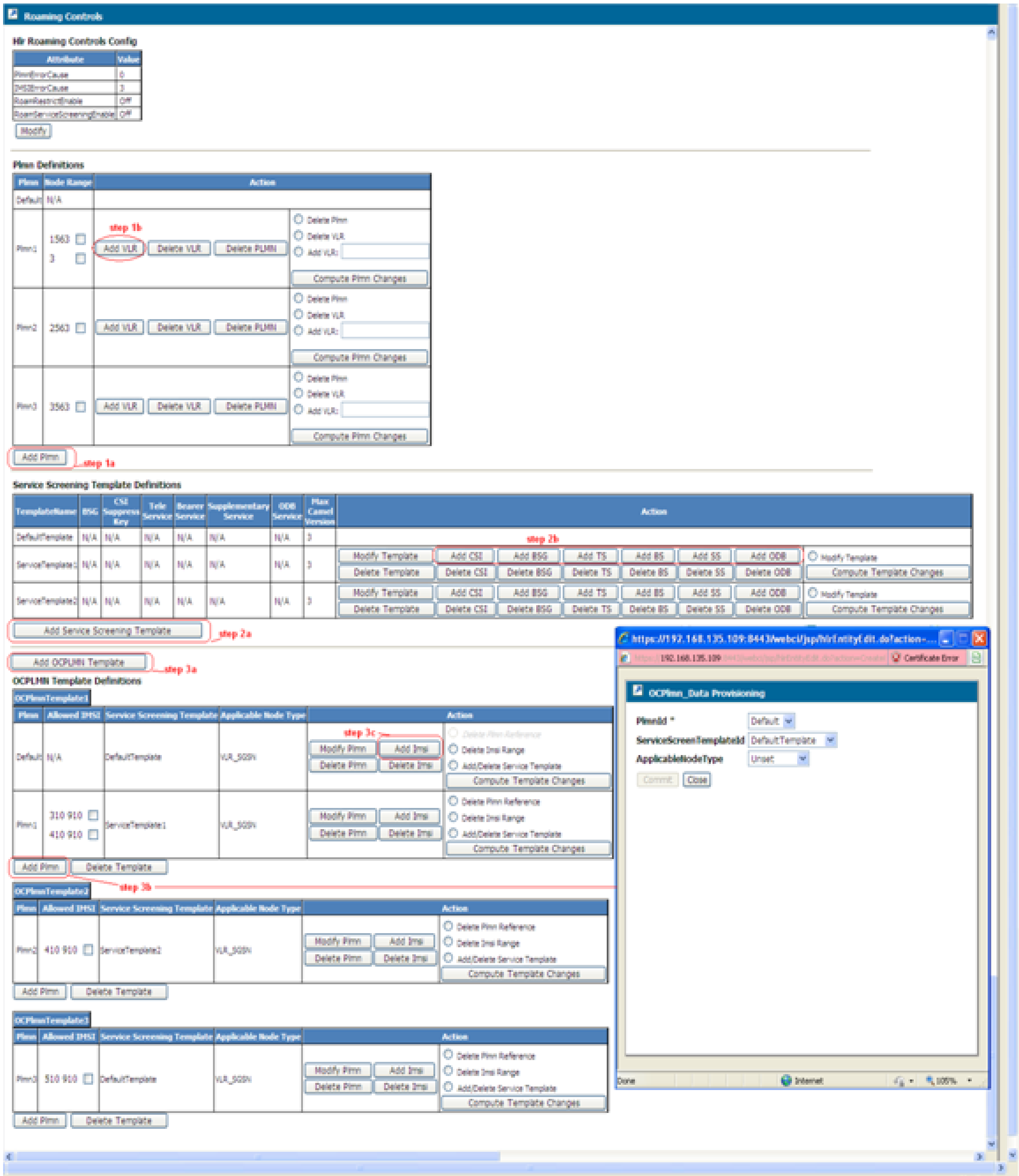
Only the PLMNs that are already defined in the Plmn Definitions table (see step 1) can be assigned to an OCPLMN Template. You can assign a list of roaming PLMNs to one single OCPLMN Template. Simply repeat this step for the same OCPLMN Template.

Note: That roaming PLMNs cannot be assigned to the "Not Defined" OCPLMN Template.

Each OCPLMN Template must have a "Default PLMN" and therefore the first PLMN that is to be assigned to each OCPLMN Template must be the "Default PLMN". If a VLR/GMSC is not found in any of the PLMNs defined for the used OCPLMN Template, it is considered as belonging to the "default PLMN".

c) Define roaming restrictions ("allowed" PLMN-IMSI combinations), by defining a list of "Allowed IMSIs" for each roaming PLMN assigned to an OCPLMN Template. One "Allowed IMSI" range can be defined at a time by clicking on the `Add Imsi` button available for a specific roaming PLMN. Simply repeat this as many times as the number of "allowed IMSIs" you wish to define for that roaming PLMN.

By default, the "Allowed IMSI" is set to 'N/A', which means that no IMSIs are allowed for the roaming PLMN.



Roaming Controls

Hlr Roaming Controls Config

Attribute	Value
PlmnErrorCause	0
IMSIErrorCause	3
RoamRestrictEnable	Off
RoamServiceScreeningEnable	Off

Plmn Definitions

Plmn	Node Range	Action	
Default	N/A		
Plmn1	1563 □ 3 □	Add VLR Delete VLR Delete PLMN	○ Delete Plmn ○ Delete VLR ○ Add VLR: Compute Plmn Changes
Plmn2	2563 □	Add VLR Delete VLR Delete PLMN	○ Delete Plmn ○ Delete VLR ○ Add VLR: Compute Plmn Changes
Plmn3	3563 □	Add VLR Delete VLR Delete PLMN	○ Delete Plmn ○ Delete VLR ○ Add VLR: Compute Plmn Changes

Service Screening Template Definitions

TemplateName	BSG	CSI Suppress Key	Tele Service	Bearer Service	Supplementary Service	ODB Service	Max Camel Version	Action	
DefaultTemplate	N/A	N/A	N/A	N/A	N/A	N/A	3		
ServiceTemplate1	N/A	N/A	N/A	N/A	N/A	N/A	3	Modify Template Add CSI Add BSG Add TS Add BS Add SS Add ODB Delete Template Delete CSI Delete BSG Delete TS Delete BS Delete SS Delete ODB	○ Modify Template Compute Template Changes
ServiceTemplate2	N/A	N/A	N/A	N/A	N/A	N/A	3	Modify Template Add CSI Add BSG Add TS Add BS Add SS Add ODB Delete Template Delete CSI Delete BSG Delete TS Delete BS Delete SS Delete ODB	○ Modify Template Compute Template Changes

OCPLMN Template Definitions

OCPlmnTemplate1

Plmn	Allowed IMSI	Service Screening Template	Applicable Node Type	Action	
Default	N/A	DefaultTemplate	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes
Plmn1	310 910 □ 410 910 □	ServiceTemplate1	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes

OCPlmnTemplate2

Plmn	Allowed IMSI	Service Screening Template	Applicable Node Type	Action	
Plmn2	410 910 □	ServiceTemplate2	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes

OCPlmnTemplate3

Plmn	Allowed IMSI	Service Screening Template	Applicable Node Type	Action	
Plmn3	510 910 □	DefaultTemplate	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes

https://192.168.135.109:8443/webci/jsp/hlrEntityEdit.do?action-...

OCPlmn_Data Provisioning

PlmnId * Default

ServiceScreenTemplateId DefaultTemplate

ApplicableNodeType Unset

Figure 51: Operator Controlled PLMN Definition

Notice from this figure that the OCPLMN Templates allow the operator to define different “allowed IMSIs” for the same PLMN (Plmn1) as long as they belong to different templates. A subscriber’s profile can be provisioned to refer to either one of the OCPLMN Templates defined here. So, it is possible to have different group of subscribers with different restrictions in the same PLMN. To do so, simply create a specific OCPLMN Template with the same PLMN (but different restrictions) and assign them to specific group of Subscribers. Note that if a subscriber’s profile doesn't refer to any OCPLMN Template (default scenario), then it is always allowed and there are no PLMN nor service restrictions for that subscriber.

Refer to the *SDM Subscriber Provisioning – User Guide* for instructions on how to provision subscribers in bulk with the OCPlmnTemplateName referring to an OCPLMN template. Refer to the *SDM Subscriber Provisioning – Reference Manual* for details on the OCPlmnTemplateName parameter. Refer to the *SDM Troubleshooting, Monitoring, Maintenance – User Guide* for instructions on how to modify a subscriber profile and provision the OCPlmnTemplateName.

TIPs to help you provision the tables and setting the PLMN-IMSI restrictions:

The Node Range list may consist of one or more specific Node Ranges.

This restricts the PLMN to allow only some Node Ranges. Only in the case of the 'Default PLMN', the Node Range list is empty (N/A), which means that for all Node Ranges the roaming Allowed/Not Allowed verification will be done based on the Allowed IMSI defined for the 'Default PLMN' assigned to the subscriber's OCPLMN Template.

The "Allowed IMSIs list" may:

d) be empty (N/A) – this means that the "PLMN is NOT allowed ".

Any calls coming from any Node Range defined for that PLMN will be blocked.

Or

e) have a list of one or more specific IMSI ranges.

This only allows certain subscribers (IMSIs) to make calls from any Node Range defined for that PLMN.

Or

f) have a MCC=000 and MNC=000 as IMSI ranges.

This allows ALL subscribers (IMSIs) to make calls from any Node Range defined for that PLMN.

The following operations are also available from the Roaming Controls window:

Modify. The following is available in order to make modifications:

g) The **Modify** button located beneath the Hlr Roaming Controls Config table allows you to enable/disable the Roaming Restrictions and/or the Service Screening Restrictions and also allows you to modify the default PLMN/IMSI error causes configuration.

h) The **Modify Template** button, located in the Action column of the Service Screening Template Definitions table for each Service Screening Template, allows you to modify the ServiceScreenTemplateName and the MaxCamelVersion.

Delete. The following is available in order to make deletions:

i) The **Delete PLMN** button, located in the Action column of the Plmn Definitions table for each roaming PLMN, allows you to delete the corresponding roaming PLMN (other than the default PLMN).

Note: The Deletion of a PLMN cascades down to the VLR/GMSC address ranges and it un-assigns the roaming PLMN from the OCPLMN Templates to which it had been assigned to.

j) The **Delete Plmn** button, located in the Action column for each OCPLMN Template's roaming PLMN, allows to un-assign a roaming PLMN to an OCPLMN Template.

Note1: The deletion of a roaming PLMN also deletes the "Allowed IMSIs" that were defined for it and un-assigns its Service Screening Template.

k) The **Delete VLR** button, located in the Action column of the Plmn Definitions table for each roaming PLMN, allows you to delete one Node range at a time for a specific PLMN.

l) The **Delete Imsi** button, located in the Action column for each OCPLMN Template's roaming PLMN, allows you to delete one "Allowed IMSI range" at a time for a specific OCPLMN Template's roaming PLMN.

m) The **Delete Template** button, located in the Action column of the Service Screening Template Definitions table for each Service Screening Template, allows you to delete a Service Screening Template and all of its customized services.

Take note that a Service Screening template cannot be deleted if it is assigned to at least one roaming PLMN.

n) The **Delete Template** button, located beneath each OCPLMN Template, allows you to delete a PLMN from the OCPLMN Template.

All the Plmns of an OCPLMN Template, except the "default Plmn", can be deleted one by one regardless of whether the OCPLMN Template is assigned to subscribers or not. The "default Plmn" of the OCPLMN Template can be deleted, only if the template is not assigned to any subscriber since the deletion of the "Default Plmn" is equivalent to a deletion of the OCPLMN Template as a whole.

o) The deletion of an OCPLMN Template cascades to its roaming restrictions and service screening restrictions.

p) Delete TS/Delete BS/Delete BSG/Delete ODB/Delete CSI/Delete SS.

These operations are available for each Service Screening Template and allow to delete individually the customized services defined for that template.

Calculating VLR/SGSN Nodes Affected by a Roaming Configuration Change

This section describes how the Network Operator can request for the Tekelec ngHLR to calculate the list of VLR/SGSN nodes that would be affected by a specific roaming configuration change. The Tekelec ngHLR can calculate the list of affected VLR/SGSN nodes for one roaming configuration change at a time.

The Network Operator can then use this list of affected VLR/SGSN nodes and include it in the NodeNumberSubset entity's list of nodes, to which a MAP_RESET message will be sent to when executing the 'Map Reset' operation (SendMapReset() Option=Node Number Subset). For further instructions on the 'Map Reset' operation, refer to *MAP Reset* in this document.

In order to request the calculation of the affected VLR/SGSN nodes and then feed that list to the NodeNumberSubset entity's list of nodes for the MAP Reset, the Roaming Controls window must be accessed from the WebCI and from there, the following steps must be followed:

Note: For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document.

Prerequisite: The roaming configuration data must be provisioned prior to being able to calculate which VLR/SGSN nodes would be affected by a change in the roaming configuration. Refer to the previous sections for instructions on how to configure roaming data.

1. Select the change for which you wish to have the list of affected VLR/SGSN nodes calculated.

Note that only a single change can be evaluated at a time.

The configuration changes are evaluated separately via three operations, which are inserted in the Plmn Definitions, OCPlmn Template Definitions and Service Screening Template tables, as shown in the figure below. Here are the types of roaming configuration changes for which the Tekelec ngHLR can calculate the list of affected VLR/SGSN nodes and the operation that executes this calculation:

Compute Plmn Changes: The user must select one of the actions using the radio buttons.

Delete Plmn: The PlmnId is taken directly from the corresponding row.

Delete Node Range: Select the desired Node Range, using the check boxes in the 'Node Range' column of the corresponding Plmn row. Only one Node Range can be selected at a time.

Add Node Range: The value of the new Node Range must be entered in the adjacent text box.

Compute OCPlmn Template Changes: The user must select one of the actions using the radio buttons.

Delete Plmn Reference: The PlmnId is taken directly from the corresponding row.

Delete Imsi: Select the desired Imsi, using the check boxes in the 'Allowed Imsi' column of the corresponding Plmn row. Only one Imsi can be selected at once.

Add/Delete Service Template Reference: The only value required is the action (Add/Delete), the actual value of the service template is irrelevant.

Compute Service Screening Template Changes: The user must select one of the actions using the radio buttons.

Modify Service Template: The ServiceScreenTemplateId is taken directly from the corresponding row.

2. Click on the compute button that corresponds to the roaming change you selected.

   Example: If you select the 'Delete Plmn' roaming change, you must click on the 'Compute Plmn Changes' button.

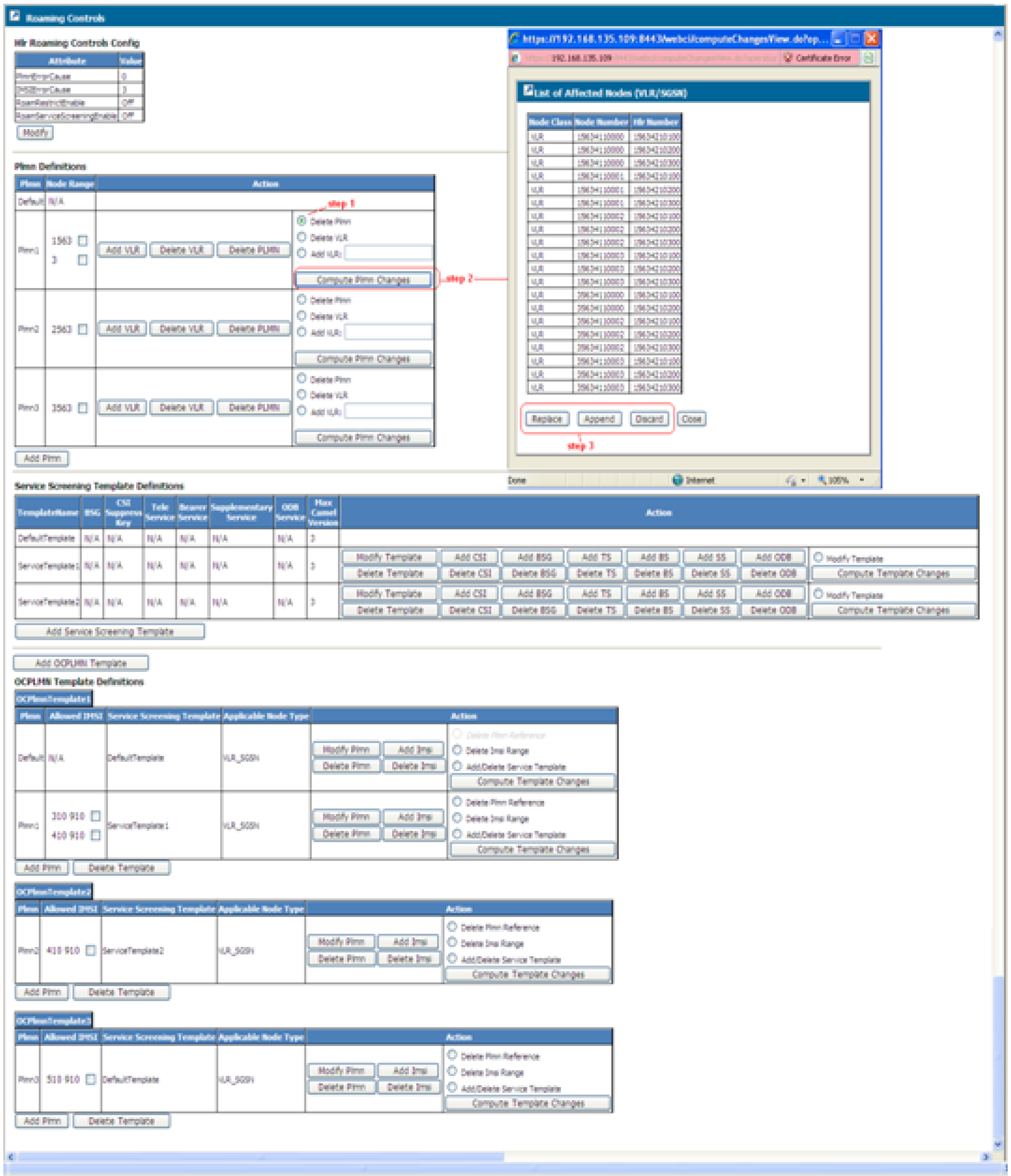
3. A pop-up window will appear with the list of affected VLR/SGSN nodes calculated by the Tekelec ngHLR.

   This window offers you the choice to take the following action:

   a) 'Discard': this operation discards the list of affected nodes.
   b) 'Append': this operation appends the list of affected nodes to the NodeNumberSubset table's list of nodes (nodes to which the Tekelec ngHLR will send a MAP_RESET message upon the execution of the 'Map Reset' operation).
   c) 'Replace': this operation replaces the NodeNumberSubset entity's list of nodes with the list of affected VLR/SGSN nodes calculated by the Tekelec ngHLR.

   The steps described above can be repeated as many times as desired for a different roaming configuration change. The actions taken in step 3 are cumulative, which means that if you repeat this procedure multiple times and append each list of affected VLR/SGSN nodes calculated, the NodeNumberSubset entity's list of nodes will include all of these lists of affected VLR/SGSN nodes calculated.

   After performing this procedure, you can display and edit the NodeNumberSubset table's list of nodes as desired. This list of nodes will be all the nodes to which a MAP_RESET message will be sent upon execution of the 'Map Reset' operation with option=Node Number Subset. For instructions on how to achieve this, refer to the MAP Reset" section of this document.



Roaming Controls

Hlr Roaming Controls Config

Attribute	Value
PlmnErrorCause	0
IMSIErrorCause	3
RoamRestrictEnable	Off
RoamServiceScreeningEnable	Off

Pmn Definitions

Plmn	Node Range	Action	
Default	N/A		
Plmn1	1563 □ 3 □	Add VLR Delete VLR Delete PLMN	● Delete Plmn ○ Delete VLR ○ Add VLR: Compute Plmn Changes
Plmn2	2563 □	Add VLR Delete VLR Delete PLMN	○ Delete Plmn ○ Delete VLR ○ Add VLR: Compute Plmn Changes
Plmn3	3563 □	Add VLR Delete VLR Delete PLMN	○ Delete Plmn ○ Delete VLR ○ Add VLR: Compute Plmn Changes

step 1

step 2

https://192.168.135.109:8443/webci/computeChangesView.do?op...

List of Affected Nodes (VLR/SGSN)

Node Class	Node Number	Hlr Number
VLR	15634110000	15634210100
VLR	15634110000	15634210200
VLR	15634110000	15634210300
VLR	15634110001	15634210100
VLR	15634110001	15634210200
VLR	15634110001	15634210300
VLR	15634110002	15634210100
VLR	15634110002	15634210200
VLR	15634110002	15634210300
VLR	15634110003	15634210100
VLR	15634110003	15634210200
VLR	15634110003	15634210300
VLR	25634110000	15634210100
VLR	25634110000	15634210200
VLR	25634110002	15634210100
VLR	25634110002	15634210200
VLR	25634110002	15634210300
VLR	25634110003	15634210100
VLR	25634110003	15634210200
VLR	25634110003	15634210300

step 3

Service Screening Template Definitions

TemplateName	BSG	CSI Suppress Key	Tele Service	Bearer Service	Supplementary Service	ODB Service	Max Camel Version	Action
DefaultTemplate	N/A	N/A	N/A	N/A	N/A	N/A	3	
ServiceTemplate1	N/A	N/A	N/A	N/A	N/A	N/A	3	Modify Template Add CSI Add BSG Add TS Add BS Add SS Add ODB ○ Modify Template Delete Template Delete CSI Delete BSG Delete TS Delete BS Delete SS Delete ODB Compute Template Changes
ServiceTemplate2	N/A	N/A	N/A	N/A	N/A	N/A	3	Modify Template Add CSI Add BSG Add TS Add BS Add SS Add ODB ○ Modify Template Delete Template Delete CSI Delete BSG Delete TS Delete BS Delete SS Delete ODB Compute Template Changes

OCPLMN Template Definitions

OCPlmnTemplate1

Plmn	Allowed IMSI	Service Screening Template	Applicable Node Type	Action	
Default	N/A	DefaultTemplate	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes
Plmn1	310 910 □ 410 910 □	ServiceTemplate1	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes

OCPlmnTemplate2

Plmn	Allowed IMSI	Service Screening Template	Applicable Node Type	Action	
Plmn2	410 910 □	ServiceTemplate2	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes

OCPlmnTemplate3

Plmn	Allowed IMSI	Service Screening Template	Applicable Node Type	Action	
Plmn3	510 910 □	DefaultTemplate	VLR_SGSN	Modify Plmn Add Imsi Delete Plmn Delete Imsi	○ Delete Plmn Reference ○ Delete Imsi Range ○ Add/Delete Service Template Compute Template Changes

Figure 52: Calculating VLR/SGSN Nodes Affected By A Roaming Configuration Change

Setting Restrictions on the Version of MAP Messages (MAP Policing) and on the SRI-ack, ATI-ack and PSI Messages

The MAP Policing feature allows the operator to control, on a per-node and per-Application Context (AC) basis, the maximum AC version to be used in any MAP transaction. For a more detailed description of the MAP Policing feature and the Tekelec ngHLR's behavior, refer to the "Map Policing (Manual Configuration of Maximum MAP Version)" and "MAP Reset" sections of the *SDM Product Description* . For a description about the tables to provision, each of their parameters and values supported, refer to the "MAP Policing" section of the *SDM System Configuration – Reference Manual*.

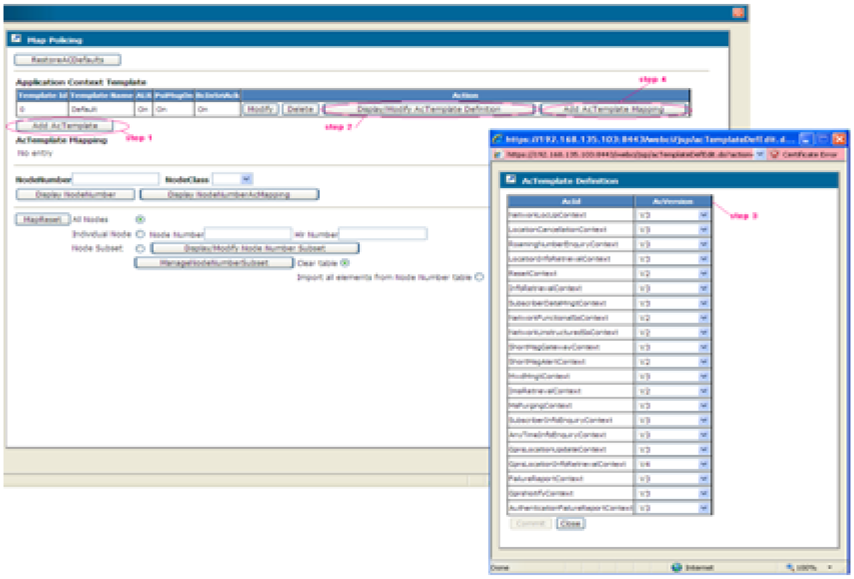
To achieve this, the operator must follow the steps below, from the WebCI's Map Policing window, which can be opened from the HLR folder.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

Prerequisite: The MAP Policing feature must be enabled. The MapPolicingOn parameter in the HlrConfig table allows to enable/disable this feature. Refer to the *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* in this document for instructions on how to enable/disable the MAP Policing feature.

1. The Application Context Template table must be provisioned to define a template.

   It can also be used to provision the following features for each template definition: ALR Suppression (to include/exclude the ALR information in the reply), Optional PSI (to send or not the PSI message), Addition of GSM-BC and BS in SRI-ack (to include/exclude the GSM-BC and BS information in the SRI-ack).
2. The AC Template Definition table must be displayed.
3. The AC Template Definition table must be provisioned to define a default maximum MAP version, per Application Context (AC) for a specific template.
4. In order to add control of the maximum AC version to be used on a per-node basis, the AC Template Mapping table must be provisioned to associate a Node Range to the template for which you just defined a default maximum MAP version for each AC.



Template Id	Template Name	ALR	PsiPlugIn	BcInfoInAck
0	Default	On	On	On

AcId	AcVersion
NetworkLocUpContext	v3
LocationCancellationContext	v3
RoamingNumberEnquiryContext	v3
LocationInfoRetrievalContext	v3
ResetContext	v2
InfoRetrievalContext	v3
SubscriberDataMngtContext	v3
NetworkFunctionalSsContext	v2
NetworkUnstructuredSsContext	v2
ShortMsgGatewayContext	v3
ShortMsgAlertContext	v2
MwdMngtContext	v3
ImsiRetrievalContext	v3
MsPurgingContext	v3
SubscriberInfoEnquiryContext	v3
AnyTimeInfoEnquiryContext	v3
GprsLocationUpdateContext	v3
GprsLocationInfoRetrievalContext	v4
FailureReportContext	v3
GprsNotifyContext	v3
AuthenticationFailureReportContext	v3

Figure 53: Provisioning MAP Policing

Blocking MAP Transactions Based on the Node Address and the AC

The MAP Policing feature also allows the operator to block certain MAP transactions based on the node address and the AC, by setting the maximum MAP version to "NotSupported" in an AC Template. That template must then be associated to a Node Range that covers the desired node address.

Other Operations

In addition to provisioning the Application Context Template, Ac Template Definition and Ac Template Mapping tables with new entries, the following operations are also available:

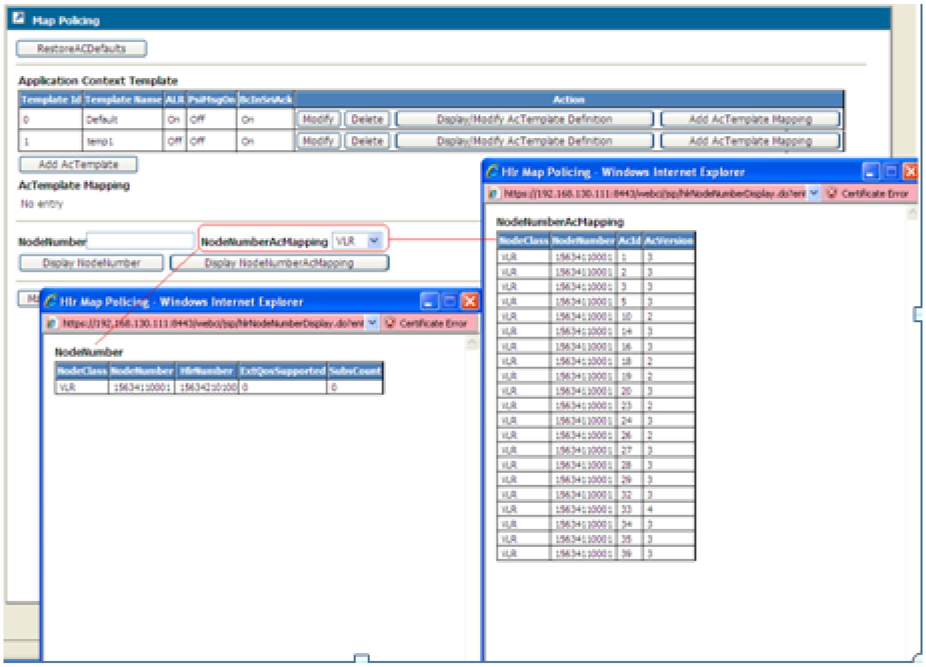
Display NodeNumber.* The Node Number table is dynamic and contains a list of all the nodes for which an "Update Location" message has been received. This table is used internally by the NodeNumberAcMapping table.

The operator can view the content of the Node Number table by displaying it from the WebCI's Map Policing window.

Display NodeNumberAcMapping.* During a MAP transaction, the ngHLR proceeds with MAP Version Fallback when needed, and dynamically stores the last negotiated MAP version for a given AC, to be used for subsequent transactions. These values are stored in the "Node Number AC Mapping" table, dynamically managed by the ngHLR. If a specific template is associated to the desired node, the values from this template are stored in this dynamic table; otherwise the values are taken from the "Default Template'.

The operator can view the content of the Node Number AC Mapping table by displaying it from the WebCI's Map Policing window.

*The WebCI offers the possibility to specify the NodeNumber and/or the NodeClass to narrow the list displayed by the WebCI in the Node Number and Node Number AC Mapping tables.



Application Context Template

Template Id	Template Name	ALR	PsiMsgOn	ScInSriAck	Action
0	Default	On	Off	On	Modify Delete Display/Modify AcTemplate Definition Add AcTemplate Mapping
1	temp1	Off	Off	On	Modify Delete Display/Modify AcTemplate Definition Add AcTemplate Mapping

AcTemplate Mapping

No entry

NodeNumber

NodeNumberAcMapping VLR

https://192.168.130.111:8443/webci/jsp/hlrNodeNumberDisplay.do?ent

NodeNumber

NodeClass	NodeNumber	HlrNumber	ExtQosSupported	SubsCount
VLR	15634110001	15634210100	0	0

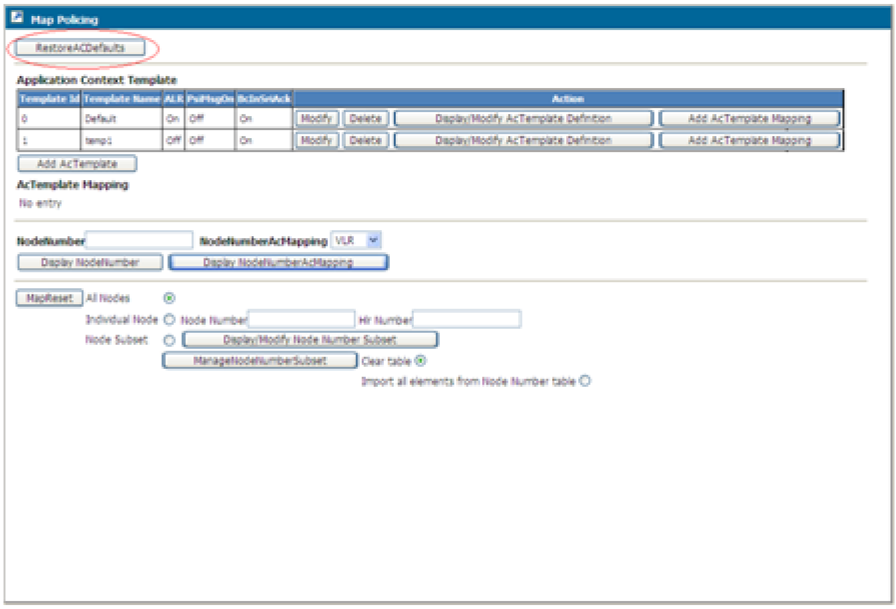
https://192.168.130.111:8443/webci/jsp/hlrNodeNumberDisplay.do?ent

NodeNumberAcMapping

NodeClass	NodeNumber	AcId	AcVersion
VLR	15634110001	1	3
VLR	15634110001	2	3
VLR	15634110001	3	3
VLR	15634110001	5	3
VLR	15634110001	10	2
VLR	15634110001	14	3
VLR	15634110001	16	3
VLR	15634110001	18	2
VLR	15634110001	19	2
VLR	15634110001	20	3
VLR	15634110001	23	2
VLR	15634110001	24	3
VLR	15634110001	26	2
VLR	15634110001	27	3
VLR	15634110001	28	3
VLR	15634110001	29	3
VLR	15634110001	32	3
VLR	15634110001	33	4
VLR	15634110001	34	3
VLR	15634110001	35	3
VLR	15634110001	39	3

Figure 54: Displaying Node Number And Node Number AC Mapping Tables For MAP Policing

Restore ACDefaults. The operator can restore the MAP versions stored in the Node Number AC Mapping dynamic table back to the original maximum values, which were defined as a template in the AC Template Definition table.



Application Context Template

Template Id	Template Name	ALR	PsiMsgOn	BcInSriAck	Action			
0	Default	On	Off	On	Modify	Delete	Display/Modify AcTemplate Definition	Add AcTemplate Mapping
1	temp1	Off	Off	On	Modify	Delete	Display/Modify AcTemplate Definition	Add AcTemplate Mapping

AcTemplate Mapping

No entry

NodeNumber NodeNumberAcMapping VLR

All Nodes ●

Individual Node ○ Node Number Hlr Number

Node Subset ○

Clear table ●

Import all elements from Node Number table ○

Figure 55: Restore AC Defaults

MAP Reset

The operator can force the Tekelec ngHLR to send a MAP_RESET message to VLRs or SGSNs in order to inform them that a failure occurred. The MAP_RESET message indicates to the remote node that it should refresh all of the subscriber data previously received by the Tekelec ngHLR. Refer to the “MAP Reset” section of the *SDM Product Description* for a more detailed description of the MAP Reset service.

To achieve this, the operator must follow the steps below, from the WebCI’s Map Policing window, which can be opened from the HLR folder.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

WARNING

WARNING: The ‘Map Reset’ operation must only be executed during low traffic periods, otherwise it could affect the performance of the system.

Prerequisite: The MAP Policing feature must be enabled. The MapPolicingOn parameter in the HlrConfig table allows to enable/disable this feature. Refer to the *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* in this document for instructions on how to enable/disable the MAP Policing feature.

1. Select one of the three options for which you wish the Tekelec ngHLR to send a MAP Reset message:

Option 1: **All Nodes.** The Tekelec ngHLR sends a MAP Reset message to all nodes from the complete list of nodes stored in the database (in the Node Number entity).

Option 2: **An individual node.** When selecting this option, you must also specify the Node Number and Hlr Number.

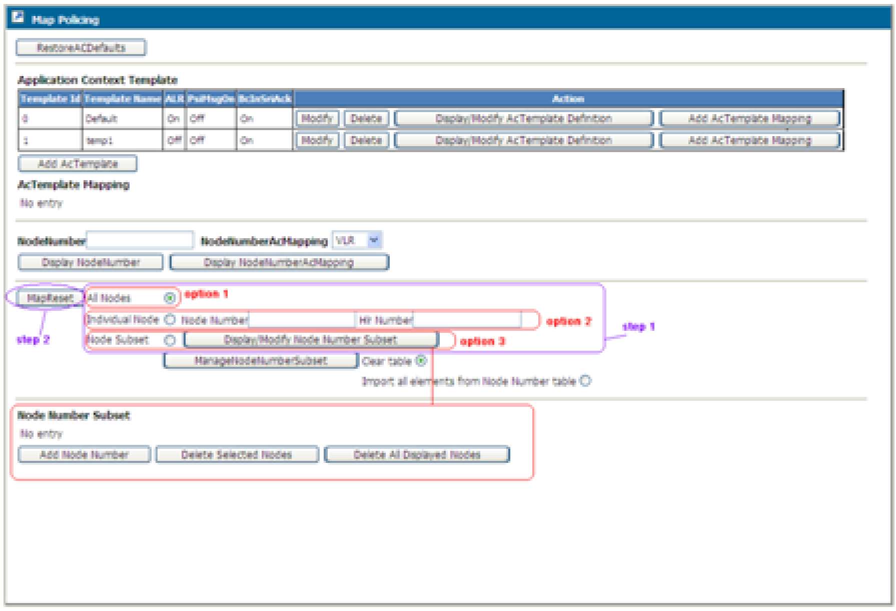
Option 3: **Node Subset.** This allows the operator to force the Tekelec ngHLR to send a MAP Reset message to a series of specific nodes that can be defined in the Node Number Subset table. When selecting this option, you must follow these steps:

Display the Node Number Subset table by clicking on the Display/Modify Node Number Subset button.

Provision the Node Number Subset table to define the Nodes for which you wish the Tekelec ngHLR to send a MAP Reset message to.

2. Execute the Map Reset operation by clicking on the MapReset button.

   This Map Reset operation will be executed as per the option selected previously.



Application Context Template

Template Id	Template Name	ALR	PsiMsgOn	BcInSriAck	Action			
0	Default	On	Off	On	Modify	Delete	Display/Modify AcTemplate Definition	Add AcTemplate Mapping
1	temp1	Off	Off	On	Modify	Delete	Display/Modify AcTemplate Definition	Add AcTemplate Mapping

AcTemplate Mapping

No entry

NodeNumber NodeNumberAcMapping VLR

All Nodes ●

Individual Node ○ Node Number Hlr Number

Node Subset ○

Clear table ●

Import all elements from Node Number table ○

Node Number Subset

No entry

Figure 56: Executing A MAP Reset

Other Operations

In addition to provisioning the Node Number Subset table with new entries, the following operations are also available:

ManageNodeNumberSubset. This operation has been implemented to provide you with an easier and faster way to provision the Node Number Subset table. The ManageNodeNumberSubset operation is used to clear the NodeNumberSubset entity or to import all elements from the NodeNumber entity.

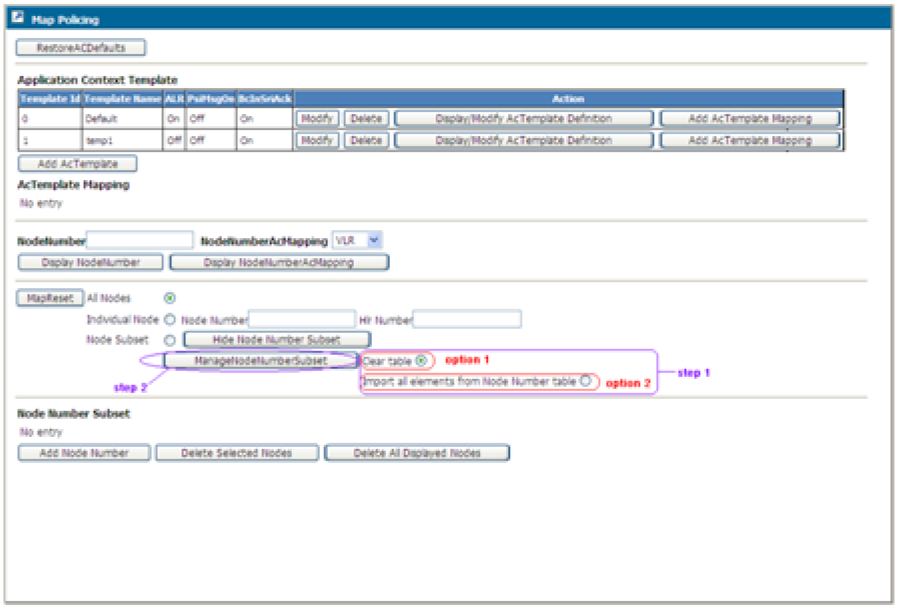
The following steps must be followed to execute this operation:

Select one of the two following options:

Option 1: Clear table.

Option 2: **Import all elements from Node Number table.** This option will provision the Node Number Subset table with all the entries of the Node Number table.

Execute the ManageNodeNumberSubset operation by clicking on the ManageNodeNumber button.



Application Context Template

Template Id	Template Name	ALR	PsiMsgOn	BcInSriAck	Action
0	Default	On	Off	On	Modify Delete Display/Modify AcTemplate Definition Add AcTemplate Mapping
1	temp1	Off	Off	On	Modify Delete Display/Modify AcTemplate Definition Add AcTemplate Mapping

AcTemplate Mapping

No entry

NodeNumber NodeNumberAcMapping VLR

All Nodes ●

Individual Node ○ Node Number Hr Number

Node Subset ○

Clear table ●

Import all elements from Node Number table ○

Node Number Subset

No entry

Figure 57: Managing Node Number Subset Table For The MAP Reset Feature

Provisioning the Tekelec ngHLR for MT-SMS Routing

The Tekelec ngHLR can reply to a SRI_SM message with either the MSC address at which the subscriber is currently registered (normal 3GPP-defined call flow) or with an alternative E.164 GT address, for redirection of MT-SMS to a SMS Relay (server/router) of the Home PLMN of the destination subscriber. Refer to the "SRI-SM Routing to SMS Relay" sections in the *SDM Product Description* for a detailed description of this feature and in the *SDM System Configuration – Reference Manual* for a description of the entities to provision, each of their parameters and values supported.

The operator can define a list of Destination Router addresses to which the MT-SMS request message will be routed if the feature is enabled. These Destination Router addresses can be assigned to each MT-SMS Routing Template, which defines the routing trigger as well as an exception list that contains the GT addresses for which any MT_SMS request originating from any of these addresses will not be rerouted.

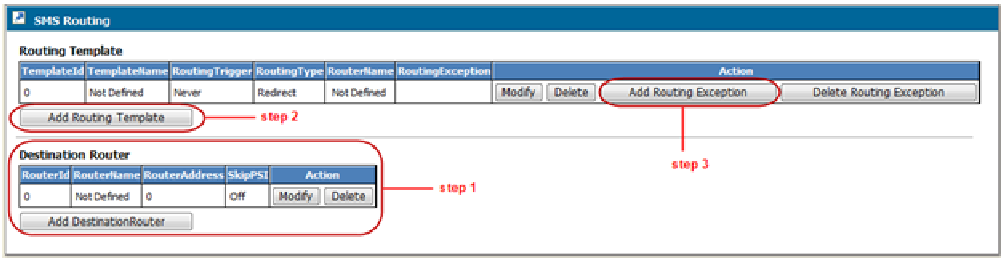
To achieve this, the operator must provision the following from the WebCI Routing window, which can be opened by extending the HLR folder from the WebCI menu:

1. The Destination Router table must be provisioned first to define the Destination Router address(es) to which the MT-SMS request will be routed in the case where the Flexible MT-SMS Rerouting (SmsRouting and SmsRelay) feature is activated.

   Refer to *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* for instructions on how to activate and deactivate the MT-SMS Redirection functionality (one of the two possible functionalities of the Flexible MT-SMS Rerouting feature).

Note: To provision a list of SMS Relay addresses, repeat this step for each SMS Relay address to provision.

2. MT-SMS Templates can be defined and Destination Router addresses can be assigned to these templates by provisioning the Routing Template table.



Routing Template

TemplateId	TemplateName	RoutingTrigger	RoutingType	RouterName	RoutingException	Action
0	Not Defined	Never	Redirect	Not Defined		Modify Delete Add Routing Exception Delete Routing Exception

Add Routing Template

Destination Router

RouterId	RouterName	RouterAddress	SkipPSI	Action
0	Not Defined	0	Off	Modify Delete

Add DestinationRouter

Figure 58: Provisioning the MT-SMS Routing functionalities (Redirect and Relay)

Note: The first Routing Template entry must be added with a TemplateId=1, the second Routing Template entry to be added must be created with a TemplateId=2 and so on (following an order from 1 to n). This way, the TemplateId can be deducted as per the logic used in the following examples (considering that the first entry in the table is the default entry and has a TemplateId=0):

a) the second entry in the MT-SMS Routing Template table has a TemplateId=1
b) the third entry in the MT-SMS Routing Template table has a TemplateId=2
c) the fourth entry in the MT-SMS Routing Template table has a TemplateId=3
d) the fifth entry in the MT-SMS Routing Template table has a TemplateId=4.

Each MT-SMS Routing Template entry must be identifiable by a unique TemplateId and TemplateName.

Note: If you wish for the Tekelec ngHLR to always redirect the MAP_SRI_FOR_SM message to an SMS Relay, you must provision the SMS Redirect Trigger attribute to the 'Always' value. By default, the Routing Trigger is set to 'Never', in which case the Tekelec ngHLR will never redirect the MAP_SRI_FOR_SM message for a subscriber associated with this template.

3. A list of GT addresses from which reception fo an MT-SMS request will not trigger the redirection, can be defined by provisioning Routing Exception entries for each MT-SMS Routing Template created.

Note:

- No exceptions can be provisioned for the default Routing Template.
- To provision a list of GT addresses prefixes for one single template, repeat this step for the same template and add different GT addresses prefixes each time.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual*(this document gives more details on these tables and each of their parameters and values supported).

For details on the SubscriberProfile entity and the SmsTemplateName parameter, refer to the *SDM Subscriber Provisioning - Reference Manual*. For instructions on how to provision a subscriber profile in bulk, refer to the *SDM Subscriber Provisioning – User Guide* . For instructions on how to modify a subscriber profile from the WebCI, refer to the *SDM Troubleshooting, Monitoring, Maintenance – User Guide* .

Note:

This feature can also be configured for each subscriber by specifying an SmsTemplateName (WebCi) or SmsTemplateId (CLI) in the subscriber profile. This template refers to the corresponding template defined in the SMS Redirect Template table.

Other Operations

In addition to provisioning the Destination Router and the Routing Template tables with new entries, the following operations are also available from the WebCI Routing window:

- Delete. The following can be deleted:
  - One entry at a time in the Destination Router table. Prerequisite: The Routing templates that refer to the Destination Router to delete must first be deleted.
  - One MT-SMS Routing template at a time can be deleted in the Routing Template table. NOTE: Deleting a Routing template also deletes any GT addresses provisioned as exceptions for that template.
  - One Orig Address can be deleted at a time for a template. Select the address to delete in the scroll down list and then click the Delete Routing Exception button.
- Modify. Each entry in the Destination Router and Routing Template tables can be modified.

Provisioning Routing Controls for GSM/IMS Router capabilities

Use this procedure to provision the Tekelec ngHLR for GSM/IMS routing capabilities.

The Tekelec ngHLR can be configured to behave as a GSM/IMS Router in order to relay SRI, SRI-LCS, ATI and MT-SMS messages or redirect SRI, SRI-LCS and MT-SMS messages to one of the following nodes:

- Destination Router (in the GSM Network)
- External HLR (in the GSM Network)
- External TAS (in the IMS Network)

For more information about the Tekelec ngHLR's GSM/IMS Routing capabilities, refer to the *GSM/IMS Router* section in the *SDM Product Description*.

The step-by-step procedure in this section demonstrates how to configure the following Routing Controls from the SDM's WebCI:

- Define a list of Destination Router addresses (used if mobile device is HLR or SIP registered) and/or a list of SIP TAS Gt (used if mobile device is TAS registered).
- Define various Routing Templates, which specify how the Tekelec ngHLR will process the MAP messages:
  - Define Routing Type (Relay or Redirect)
  - Define Routing Trigger
  - Define Default Action
  - Associate one of the Destination Router addresses

- Define a list of Originator SMS-GMSC as exceptions and from which no MAP SRI-for-SM shall ever be routed.
- Define an IMSI for each of a subscriber's MSISDNs in the IMSIForRedirectRouting table. This step is very important in the cases where the Tekelec ngHLR doesn't know the IMSI of the subscriber. This can occur in the following cases:
  - there is no full subscriber profile provisioned in the Tekelec ngHLR for the subscriber (e.g., only MSISDNs)
  - the subscriber is not registered.

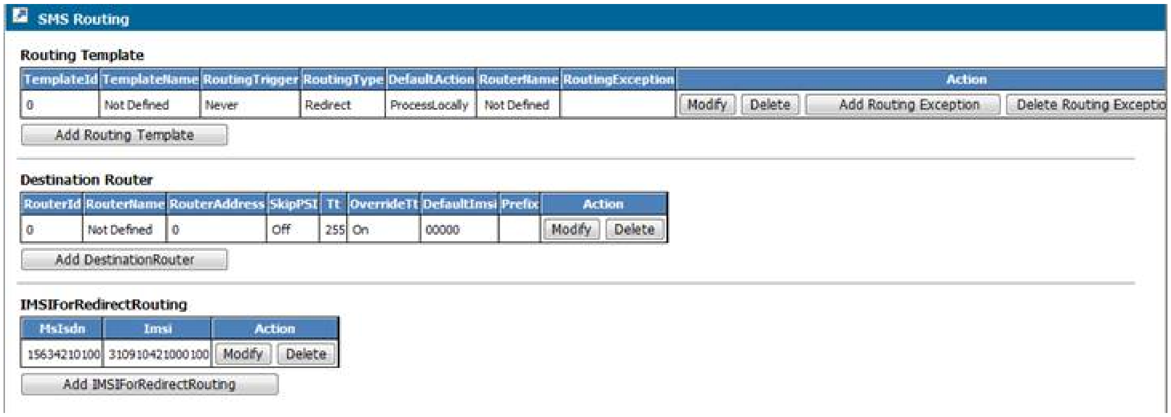
  In order to return the mandatory IMSI parameter in the MAP SRI MT-SMS Ack message, the Tekelec ngHLR first reads the IMSI provisioned in the IMSIForRedirectRouting table and if no IMSI is provisioned, it returns the default IMSI configured in the DestinationRouter or SipTasGt table. This behavior ensures that the MAP Forward SM contains the necessary information to correctly identify the subscriber.

For further assistance on the other components that need to be provisioned in the Tekelec ngHLR in order to successfully configure it with the GSM/IMS Router capabilities (e.g., activate/deactivate the routing functionalities, associate a routing template to a MSISDN or HLR Service Profile (only for the MT-SMS routing)), please refer to the *Provisioning Information* sub-section of the *GSM/IMS Router* section in the *SDM Product Description*.

Use these steps to configure the routing controls for the GSM/IMS Router from the WebCI.

1. From the WebCI main menu, go to **HLR ➤ Routing Controls**.

   The SMS Routing window displays.



SMS Routing

Routing Template

TemplateId	TemplateName	RoutingTrigger	RoutingType	DefaultAction	RouterName	RoutingException	Action
0	Not Defined	Never	Redirect	ProcessLocally	Not Defined		Modify Delete Add Routing Exception Delete Routing Exceptio

Destination Router

RouterId	RouterName	RouterAddress	SkipPSI	Tt	OverrideTt	DefaultImsi	Prefix	Action
0	Not Defined	0	Off	255	On	00000		Modify Delete

IMSIForRedirectRouting

MsIsdn	Imsi	Action
15634210100	310910421000100	Modify Delete

Figure 59: Provisioning Routing Functionalities

2. In the Destination Router table, define one or more Destination Router address(es).

   The MAP request message (SRI, SRI-LCS, ATI, or MT-SMS) will be routed to this address if the corresponding MAP Routing functionality is activated.

   a) Provision a Destination Router.

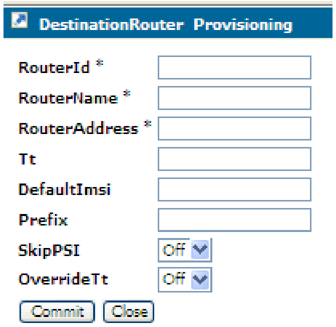
      - To add a Destination Router, click **Add DestinationRouter**.

        Repeat this step for each address to provision.
      - To modify an existing Destination Router, click **Modify** next to the existing Destination Router.

- To delete a Destination Router, click **Delete** in the Destination Router table.

  Note: The Routing Templates that refer to the Destination Router to be deleted must be deleted first.

b) Enter the required router information and commit.



DestinationRouter Provisioning

RouterId *	
RouterName *	
RouterAddress *	
Tt	
DefaultImsi	
Prefix	
SkipPSI	Off
OverrideTt	Off

3. Provision the Routing Template table.

Each Routing Template table entry represents a Routing Template. The table includes one Routing Template with TemplateId=0. This template is the default template and cannot be updated or deleted.

a) Provision a Routing template.

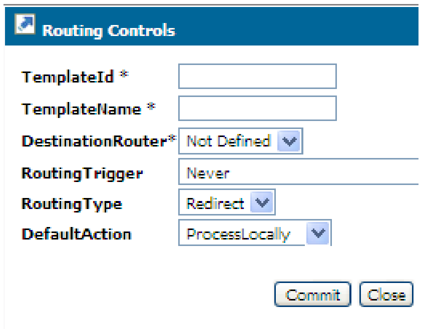
- To add a Routing Template, click **Add Routing Template**.
- To modify a Routing Template, click **Modify** next to the existing Routing Template.
- To delete a Routing Template, click **Delete**.

  Delete one Routing Template at a time. Deleting the template also deletes any Gt addresses provisioned as exceptions for that template.

b) Specify the Routing Template ID, Routing Template Name, and Destination Router.

- TemplateID - Each Routing Template must be identifiable by a unique TemplateId and TemplateName. The templates must be added with sequential TemplateIds where the first added template after the default template must have TemplateId=1, the second added template must have TemplateId=2, and so on (1-n).

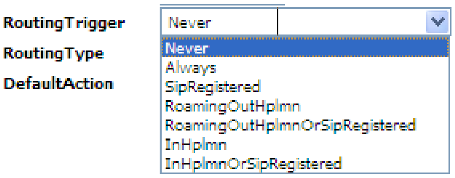
  Note: Routing templates can also be configured for each subscriber by specifying a SriTemplateId and SmsTemplateId in the MSISDN table (for any of the routing functionalities) and/or a SmsTemplateId in the HLR service profile's SubscriberProfile table (only supported for the for MT-SMS Routing functionality). The Routing Template refers to the corresponding template in the Routing Template table. When the Tekelec ngHLR receives a message, it checks the MSISDN table for an SmsTemplateId value before checking the Subscriber Profile table.



TemplateId *	
TemplateName *	
DestinationRouter*	Not Defined
RoutingTrigger	Never
RoutingType	Redirect
DefaultAction	ProcessLocally

c) Optionally, change the Routing Trigger, Routing Type, and Default Action.

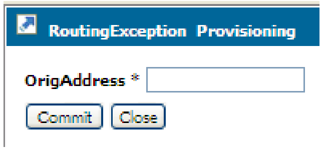
Note: When provisioning the Routing Trigger, set the attribute to Always if the Tekelec ngHLR shall always reroute the message requests to the Destination Router. By default, the Routing Trigger is set to Never, in which case the Tekelec ngHLR will never reroute the message requests for a subscriber associated with this template.



d) Provision a Routing Exception for MT-SMS Routing.

A Routing Exception is a list of Gt addresses from which the reception for an SRI MT-SMS request will not trigger a redirection. This list can be created for each Routing Template except for the default Routing Template. To provision a list of these Gt address prefixes for one single template, repeat this step for the same template and add different Gt addresses prefixes each time.

- To add a Routing Exception, click **Add Routing Exception** next to the Routing Template. Once the RoutingException Provisioning pop-up window opens (as shown below), enter the address of an Originator SMS-GMSC (Orig Address), and then commit.



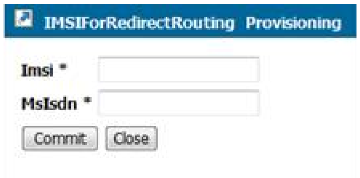
OrigAddress *	

- To delete a Routing Exception, select the Orig Address to be deleted in the scroll down list and click **Delete Routing Exception**.

Note: Routing Exceptions can only be defined for the MT-SMS routing functionality.

4. Provision a subscriber IMSI (instead of the default IMSI) for MT-SMS message routing in the IMSIFOrRedirectRouting table.

- To add a subscriber IMSI, click **Add IMSIForRedirectRouting**, enter an IMSI and MSISDN value, and commit.



- To modify an existing IMSI value, click **Modify**.

  The MSISDN value cannot be modified.
- To delete the IMSI and MSISDN values, click **Delete**.

Provisioning GSM Bearer Capabilities

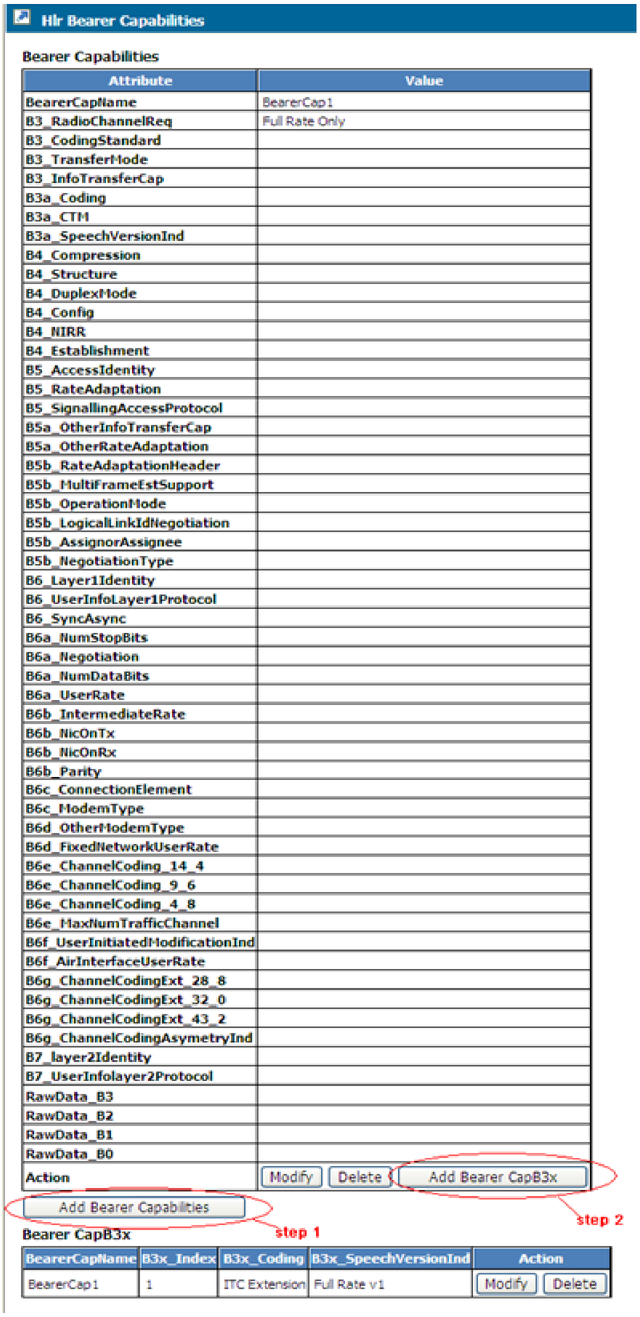
The operator can define Bearer Capabilities in order for the Tekelec ngHLR to communicate them to the VLR through the Provide Roaming Number message. For a description of the GSM Bearer Capabilities feature, refer to the *SDM Product Description*.

To achieve this, the operator must provision the following from the WebCI's Bearer Capabilities window, which can be opened by extending the HLR folder from the WebCI's menu:

The Bearer Capabilities table must be provisioned.

Note: Multiple Bearer Capability entries can be defined, to do so, simply repeat this operation and make sure to give a different Bearer Capability name to each different entry.

The Bearer Cap3Bx table can optionally be provisioned.



Bearer Capabilities

Attribute	Value
BearerCapName	BearerCap1
B3_RadioChannelReq	Full Rate Only
B3_CodingStandard	
B3_TransferMode	
B3_InfoTransferCap	
B3a_Coding	
B3a_CTM	
B3a_SpeechVersionInd	
B4_Compression	
B4_Structure	
B4_DuplexMode	
B4_Config	
B4_NIRR	
B4_Establishment	
B5_AccessIdentity	
B5_RateAdaptation	
B5_SignallingAccessProtocol	
B5a_OtherInfoTransferCap	
B5a_OtherRateAdaptation	
B5b_RateAdaptationHeader	
B5b_MultiFrameEstSupport	
B5b_OperationMode	
B5b_LogicalLinkIdNegotiation	
B5b_AssignorAssignee	
B5b_NegotiationType	
B6_Layer1Identity	
B6_UserInfoLayer1Protocol	
B6_SyncAsync	
B6a_NumStopBits	
B6a_Negotiation	
B6a_NumDataBits	
B6a_UserRate	
B6b_IntermediateRate	
B6b_NicOnTx	
B6b_NicOnRx	
B6b_Parity	
B6c_ConnectionElement	
B6c_ModemType	
B6d_OtherModemType	
B6d_FixedNetworkUserRate	
B6e_ChannelCoding_14_4	
B6e_ChannelCoding_9_6	
B6e_ChannelCoding_4_8	
B6e_MaxNumTrafficChannel	
B6f_UserInitiatedModificationInd	
B6f_AirInterfaceUserRate	
B6g_ChannelCodingExt_28_8	
B6g_ChannelCodingExt_32_0	
B6g_ChannelCodingExt_43_2	
B6g_ChannelCodingAsymetryInd	
B7_layer2Identity	
B7_UserInfolayer2Protocol	
RawData_B3	
RawData_B2	
RawData_B1	
RawData_B0	
Action	Modify Delete Add Bearer CapB3x

Bearer CapB3x

BearerCapName	B3x_Index	B3x_Coding	B3x_SpeechVersionInd	Action
BearerCap1	1	ITC Extension	Full Rate v1	Modify Delete

Figure 60: Provisioning Bearer Capabilities

It is important to note that the operator can associate a BC to each of the subscriber's MSISDN by specifying a Bearer Capability Name for the subscriber profile's BearerCapName parameter.

The operator can associate BC information, defined in the GsmBearerCapabilities table, to each MSISDN for which you wish the Tekelec ngHLR to send BC information. The Tekelec ngHLR sends the Provide Roaming Number message with the correct BC information if it is associated to its MSISDN. If no BC information is associated to the subscriber's MSISDN, the Tekelec ngHLR won't send any BC information in the PRN message.

For details on the MSISDN entity and the BearerCapName parameter, refer to the "MSISDN" section of the *SDM Subscriber Provisioning - Reference Manual* . For instructions on how to provision a subscriber profile in bulk, refer to the *SDM Subscriber Provisioning – User Guide* . For instructions on how to modify a subscriber profile from the WebCI, refer to the *SDM Troubleshooting, Monitoring, Maintenance – User Guide*.

Other Operations

In addition to provisioning the Bearer Capabilities and BearerCapB3x tables with new entries, the following operations are also available:

Delete. The following can be deleted:

One entry at a time in the Bearer Capabilities table. Prerequisite: If one or several subscriber profile's MSISDN have been associated to the BC definition you wish to delete, by specifying its BearerCapName when provisioning each of these subscriber profiles, this BC definition cannot be deleted without first un-provisioning the BearerCapName in each subscriber profile that refers to it. One entry at a time in the Bearer CapB3x table.

One entry at a time in the Bearer CapB3x table.

Modify. Each entry in the Bearer Capabilities and BearerCapB3x tables can be modified.

Provisioning the Subscriber Signaling Router (SSR)

The Subscriber Signaling Router (SSR) is one of the Tekelec ngHLR's multiple functionalities. The Tekelec ngHLR supports the SSR function in order to be able to redirect some SS7 messages to an alternate HLR address, using the following rules:

- Based on an individual IMSI or MSISDN number.
- Based on IMSI of MSISDN number range.
- Based on absence of subscriber.
- Based on message type (SAI/ATI override)

For a detailed description of this feature, refer to the "Subscriber Signaling Router (SSR)" section in the *SDM Product Description* .

The SSR fulfills its role when it is authorized by the Tekelec *Customer Care Center* and activated by the Network Operation, using the ActivateSSR() operation, as well as provisioned properly in the Tekelec ngHLR.

This section describes how to:

- provision the SSR properly.
- activate the SSR.

Note: The configuration of the SSR can be done even if the SSR is not authorized.

Here are the steps to follow when provisioning the SSR:

Note: For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference*

Manual document (this document gives more details on these tables and each of their parameters and values supported).

1. Create SSR Template(s) by provisioning the SSR Template table.

   Each SSR Template will have a set of rules that must be followed by the SSR to know what to block, which messages to forward and where.

2. Associate SSR Templates (one at a time) with one of the following: an IMSI Prefix, an MSISDN Prefix or a subscriber.

   When messages are sent for a subscriber that meets one of those criterias, the associated SSR Template will be followed by the SSR when analyzing which action to take. To achieve this, you must provision an entry in either one of the following tables:

   SSRPerMSISDNRangeData, SSRPerIMSIRangeData and SSRPerSubData.

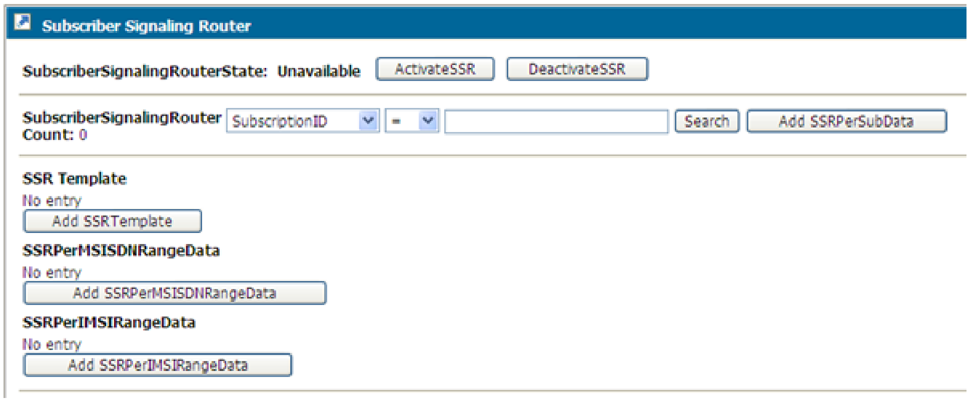
   For the SSRPerSubData table, the Subscription with SubscriptionID has to be created before being able to provision an entry in this table.

   Here are the steps to follow when activating/deactivating the SSR:

   Note: For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

3. The activation/deactivation can only be done when the feature is authorized.

   By default, the SSR function is unauthorized. You must communicate with the Tekelec *Customer Care Center* to request authorization of the SSR. Once the SSR is authorized, the HlrConfig entity's SubscriberSignalingRouterState parameter will be set to 'Deactivated'. This means that the SSR is available, but deactivated and it can now be activated. To do so, simply click on the **ActivateSSR** button. To later deactivate it, if needed, simply click on the **DeactivateSSR** button.



SubscriberSignalingRouterState: Unavailable

SubscriberSignalingRouter
Count: 0

SSR Template
No entry

SSRPerMSISDNRangeData
No entry

SSRPerIMSIRangeData
No entry

Figure 61: Provisioning/Activating The Subscriber Signaling Router

Other Operations

In addition to provisioning the SSRPerMSISDNRangeData, SSRPerIMSIRangeData, SSRPerSubData tables with new entries and activating/deactivating the SSR, the following operations are also available:

Delete. The following can be deleted:

- SSR Templates can be deleted one at a time.
- SSRPerMSISDNRangeData entries can be deleted one at a time.
- SSRPerIMSIRangeData entries can be deleted one at a time.
- SSRPerSubData entries can be deleted one at a time.

Note: All SSR data table (SSRPerSubData, SSRPerMSISDNRangeData, SSRPerISIRangeData) entries associated to a SSR template have to be deleted prior to deleting the SSR template (the template can only be delete if no SSR data is associated to it).

Modify. SSR Templates can be modified one at a time.

UpdateTimeStamp. The TimeStamp of each SSR template can be refreshed to the current time by clicking on the UpdateTimeStamp button located in the SSR Template table.

Provisioning/Modifying the Enhanced Control Of SCCP Routing Configuration

The Enhanced Control Of SCCP Routing feature can be provisioned by configuring through the WebCI the following parameters in the Tekelec ngHLR's Enhanced Control of SCCP Routing table:

- FilteringCallingPartyCheck
- FilteringPrefix
- PrefixStrip
- PrefixStripMsIsdnLength

For a detailed description of this feature, refer to the "Enhanced Control Of SCCP Routing (phase1)" section in the *SDM Product Description* .

The Tekelec ngHLR fulfills the role of the Enhanced Control Of SCCP Routing feature when:

it is authorized by the Tekelec *Customer Care Center* and activated by the Network Operator, using the ActivateFeature() operation

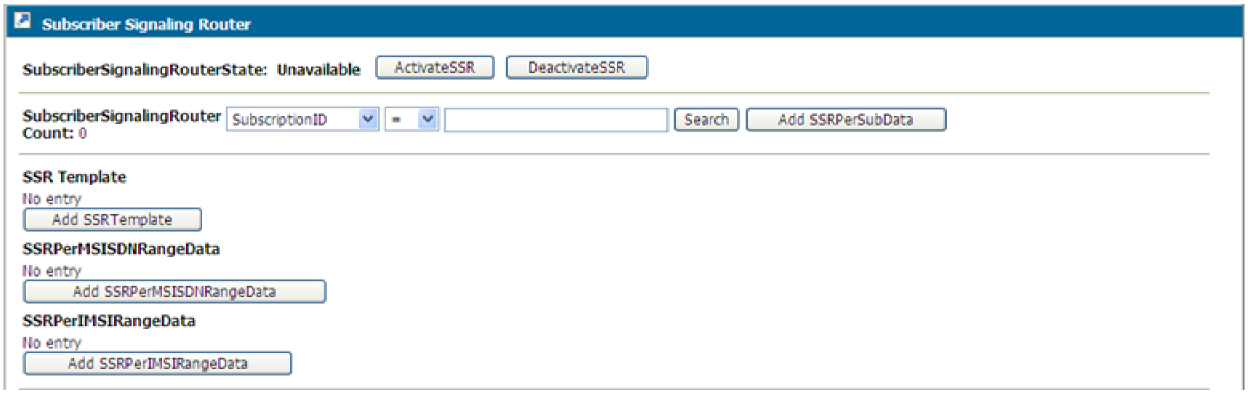
it is provisioned properly in the Tekelec ngHLR's EnhancedControlOfSccpRoutingConfig[ ] entity.

This section describes how to provision the EnhancedControlOfSccpRoutingConfig[ ] entity from the WebCI. For instructions on how to activate the feature, refer to *Viewing Activation Status of HLR Features and Activating/deactivating Them Individually* in this document.

Note: The configuration of the Enhanced Control Of SCCP Routing feature can be done even if it is not authorized (unavailable).

Note: For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

1. Open the window that can be accessed from the HLR Configuration's EnhSccpRouting tab.
2. Provision the Enhanced Control Of Sccp Routing table.



Subscriber Signaling Router

SubscriberSignalingRouterState: Unavailable

SubscriberSignalingRouter Count: 0

SSR Template

No entry

SSRPerMSISDNRangeData

No entry

SSRPerIMSIRangeData

No entry

Figure 62: Provisioning/Modifying The Enhanced Control Of SCCP Routing

Other Operations

In addition to provisioning the Enhanced Control of SCCP Routing table with new entries, the following operations are also available:

Modify. Enhanced Control of SCCP Routing data can be modified dynamically during running time of the system.

Provisioning PDN Context Templates

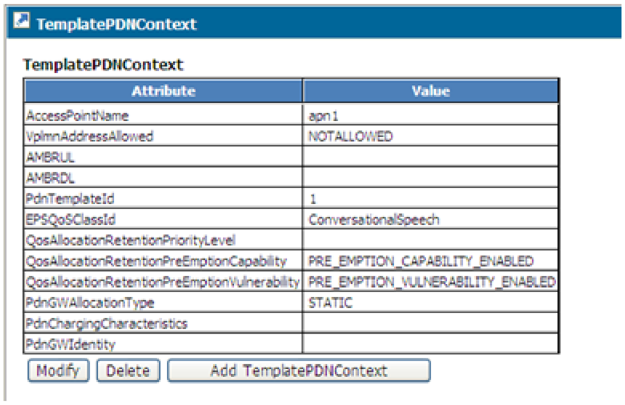
The PDN Context Templates must be configured prior to being able to define the PDN Context for a LTE-HSS subscriber. The PDN Context Templates can be defined from the WebCI's TemplatePDNContext table and once provisioned, each PDN Context Template can be linked to a subscriber profile.

The WebCI's TemplatePDNContext table can be accessed by first opening the HLR folder from the WebCI's left menu and then by opening the TemplatePDNContext window. Entries can be provisioned/edited dynamically, which means that the LTE HSS doesn't need to be restarted when adding/removing/updating entries in this entity.

Note: The PDN template can be modified on the fly without an LTE-HSS restart. However, modifying a PDN Template Id can result in a very high number of IDR sent by the LTE HSS over the network. One IDR will be sent for each subscriber registered in an MME/SGSN using the modified template in its subscriber profile. If 1 Million subscribers are using the PDN Template being modified, and these 1 Million subscribers are registered in several MMEs, upon modification of such PDN Template, the LTE HSS will send 1 Million IDR messages.

For a detailed description of each parameter, refer to the "PDN Context Template Configuration" section in the *SDM System Configuration-Reference Manual* .

Note: For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



TemplatePDNContext

TemplatePDNContext

Attribute	Value
AccessPointName	apn1
VplmnAddressAllowed	NOTALLOWED
AMBRUL	
AMBRDL	
PdnTemplateId	1
EPSQoSClassId	ConversationalSpeech
QosAllocationRetentionPriorityLevel	
QosAllocationRetentionPreEmptionCapability	PRE_EMPTION_CAPABILITY_ENABLED
QosAllocationRetentionPreEmptionVulnerability	PRE_EMPTION_VULNERABILITY_ENABLED
PdnGWAllocationType	STATIC
PdnChargingCharacteristics	
PdnGWIdentity	

Figure 63: Provisioning PDN Context Templates

Chapter 6

SIP Application Configuration

Topics:

This chapter describes the configuration of the SIP application.

Introduction

Depending on the Fixed Mobile Convergence (FMC) deployment used by the Network Operator, the SIP Server and only some or all of the following SIP functionalities need to be configured:

- SIP Registrar
- SIP Redirect Server
- SIP User Agent (RegClient)

Configuring SIP Application

The SIP application is usually configured at installation by the Tekelec *Customer Care Center*. The SIP functionalities are independent from each other, which means that they can be enabled/disabled individually at installation. During running-time of the system, the Network Operator can view the SIP configuration information and edit some SIP configuration parameters.

The WebCI allows you to view/edit the Server Configuration, Sip Security, Sip Registrar, Sip Redirect and Sip User Agent configuration tables and their attributes. This chapter describes how to view/edit this information from the WebCI.

For details on the parameters used to configure the SIP application, refer to the “SIP Entities” section in the *SDM System Configuration - Reference Manual* .

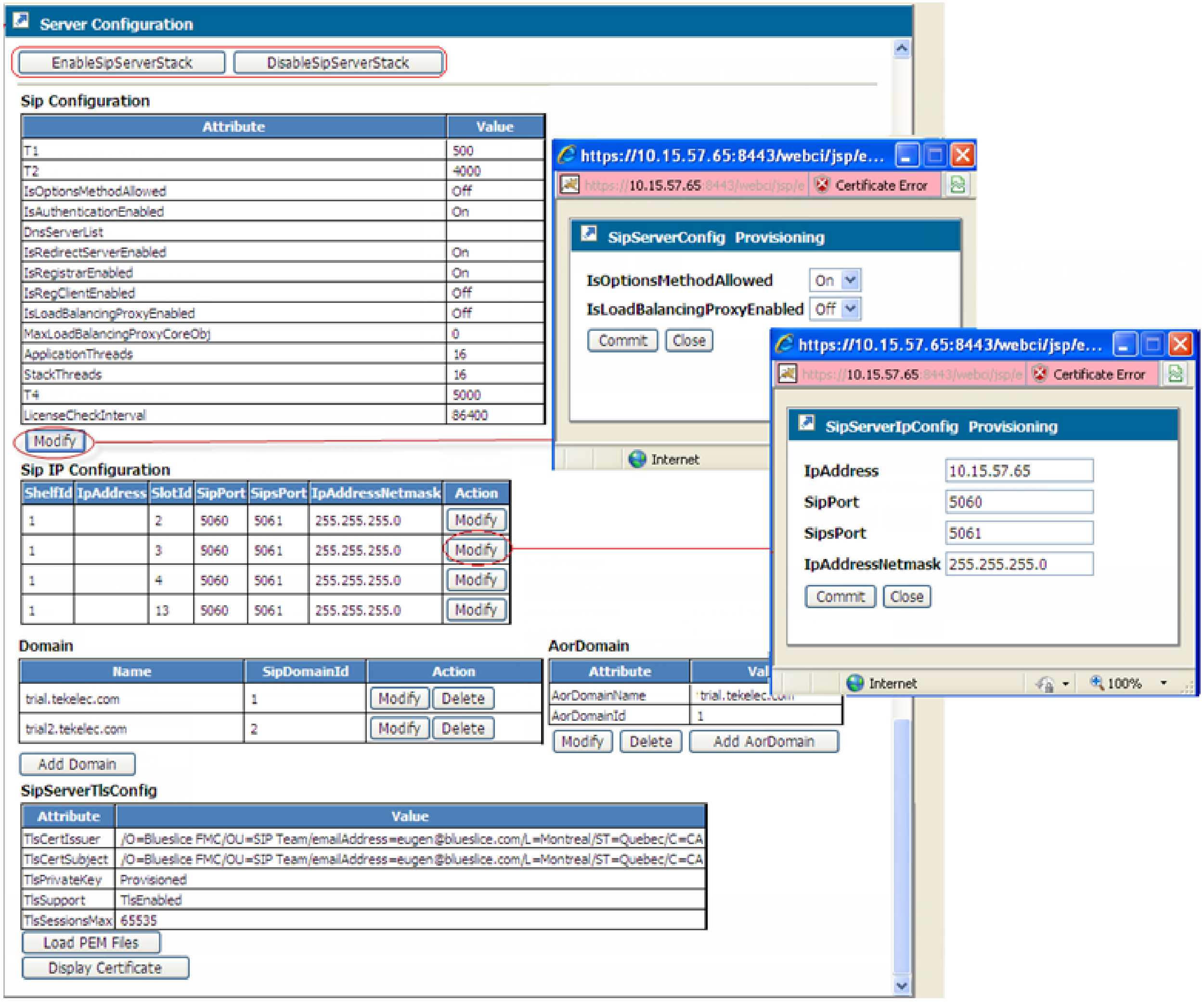
The operator can view all of the SIP configuration information from the WebCI’s SIP folder, by opening one of the following windows, depending on the SIP functionality’s configuration information desired:

- Server Configuration
- Security
- Registrar
- Redirect
- User Agent (RegClient)
- User Portability
- SIP Tas

  Some of the SIP configuration information can be edited, by clicking on the **Modify** buttons. To modify some SIP configuration data that cannot be edited by clicking on the Modify buttons, contact the Tekelec *Customer Care Center*.

Viewing and editing SIP server configuration

The WebCI’s Server Configuration window displays the Sip Configuration, Sip IP Configuration, Domain tables, Sip Server TLS Configuration and corresponding LoadPEMFiles() and DisplayCertificate() operations as well as the EnableSipServerStack/DisableSipServerStack operations.



Sip Configuration

Attribute	Value
T1	500
T2	4000
IsOptionsMethodAllowed	Off
IsAuthenticationEnabled	On
DnsServerList	
IsRedirectServerEnabled	On
IsRegistrarEnabled	On
IsRegClientEnabled	Off
IsLoadBalancingProxyEnabled	Off
MaxLoadBalancingProxyCoreObj	0
ApplicationThreads	16
StackThreads	16
T4	5000
LicenseCheckInterval	86400

Sip IP Configuration

ShelfId	IpAddress	SlotId	SipPort	SipsPort	IpAddressNetmask	Action
1		2	5060	5061	255.255.255.0	Modify
1		3	5060	5061	255.255.255.0	Modify
1		4	5060	5061	255.255.255.0	Modify
1		13	5060	5061	255.255.255.0	Modify

Domain

Name	SipDomainId	Action
trial.tekelec.com	1	Modify Delete
trial2.tekelec.com	2	Modify Delete

AorDomain

Attribute	Val
AorDomainName	trial.tekelec.com
AorDomainId	1

SipServerTlsConfig

Attribute	Value
TlsCertIssuer	/O=Blueslice FMC/OU=SIP Team/emailAddress=eugen@blueslice.com/L=Montreal/ST=Quebec/C=CA
TlsCertSubject	/O=Blueslice FMC/OU=SIP Team/emailAddress=eugen@blueslice.com/L=Montreal/ST=Quebec/C=CA
TlsPrivateKey	Provisioned
TlsSupport	TlsEnabled
TlsSessionsMax	65535

SipServerConfig Provisioning

IsOptionsMethodAllowed: On

IsLoadBalancingProxyEnabled: Off

SipServerIpConfig Provisioning

IpAddress: 10.15.57.65

SipPort: 5060

SipsPort: 5061

IpAddressNetmask: 255.255.255.0

Figure 64: Displaying/Editing The SIP Server Configuration

SIP configuration table

The Sip Configuration table displays the following:

- SIP Server’s configuration data
- On/Off flags (IsRedirectServerEnabled, IsRegistrarEnabled, IsRegClientEnabled) that indicate the enabled/disabled status of the SIP functionalities supported by the SIP Server.
- On/Off flag (IsOptionsMethodAllowed) that indicates whether the Options Method is allowed or not.
- The 3rd party registration initial retransmission interval for non-INVITE messages over UDP, for the ‘SRI Router’ feature.
- Configuration information about the ‘Improved SIP traffic distribution’ feature:
  - On/Off flag (IsLoadBalancingProxyEnabled) that indicates the enabled/disabled status of the feature.
  - The maximum number of SIP INVITE messages (MaxLoadBalancingProxyCoreObjects parameter) that can be simultaneously proxied by one single SIP Stack at one given moment.

For more details on this feature, refer to the “Improved SIP traffic distribution” section of the *SDM Product Description* manual.

The following data can be modified by the Network Operator during running-time of the system, which means that no system restart is required:

- On/Off flag (IsOptionsMethodAllowed) that indicates whether the Options Method is allowed or not.
- On/Off flag (IsLoadBalancingProxyEnabled) that indicates the enabled/disabled status of the feature.

SIP IP configuration table

The Sip IP Configuration table displays the following traffic access data of the blades on which run each SIP Server (integrated in HLR service):

- IP address
- Port
- IP address netmask
- Shelf and slot location of the blade

The following data can be modified by the Network Operator during running time of the system, which means that no system restart is required:

- IpAddress
- SipPort
- SipsPort
- IpAddressNetmask

Domain table

The Domain table displays the Domain Name of the SIP Server. The data can be modified by the Network Operator but cannot be edited during the system’s running-time without the need to restart the HLR services*:

Note: *IMPORTANT: Take note that when editing this information, in order for the new value to be committed and used by the HLR, the Network Operator must manually perform the following:

1. Stop all the HLR services that run the SIP Server.
2. Start all the HLR services that run the SIP Server.

Stopping and starting the HLR services will affect traffic, so make sure to perform this during down time if necessary. Refer to section “Starting and Stopping Services on a blade” of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for more information on how to stop a service.

For the ‘SRI Router’ feature to work correctly, the following SIP domains must be provisioned in the “Domain” entity before the Hlr service is started:

1. Request-URI domain
2. TO URI domain

To allow this, multiple entries can be provisioned in this table. Simply add an entry (by clicking on the ‘Add Domain’ button beneath the Domain table) with the ‘Request-URI domain’ and then separately add another entry with the ‘TO URI domain’.

If the SIP domain list is changed by the user, the Hlr service needs to be restarted.

AorDomain table

The AorDomain table displays the following:

- Domain Name of the AoR.
- ID of the AoR Domain Name

The following data can be modified by the Network Operator during running-time of the system without the need to restart the HLR services:

- Domain Name of the AoR

SIP Server TLS table

The Sip Server TLS Configuration table displays the following TLS configuration data:

- TLS Certificate Issuer
- TLS Certificate Subject
- TLS Certificate PEM
- TLS Private Key PEM
- TLS Private Key
- TLS Support (TLS encryption over SIP enabled or disabled)
- Maximum number of sessions opened simultaneously

Call the Tekelec Customer Care Center to edit TLS configuration and enable the TLS Support.

Other Operations

In addition to viewing/editing the Server Configuration, SIP IP Configuration and Domain tables, the following operations are also available:

DisableSipServerStack

This operation can be executed when the system is part of a Geo-redundant deployment and in the case where it has failed and you wish the system to respond with “503 Service Unavailable” in order to indicate to the SIP Client Application that it needs to route all the SIP transactions from the troubled site to the healthy site. When this operation is executed, the SIP Server performs the following:

EnableSipServerStack

Raises the Sip Server Stack Disabled critical alarm (alarmId: 8044) with the following description: SipServer - stack is Disabled, by OAM request received (manual operation)"

Answers to INVITE, OPTIONS and REGISTER valid SIP messages with “503 Service Unavailable”.

Note that the state established by this operations is not persistent.

This operation can be executed after the DisableSipServerStack () operation. When this operation is executed, the SIP Server performs the following:

Clears the SipServerStackDisabled alarm (alarmed:8044).

Answers to SIP INVITE, OPTIONS and REGISTER messages as per the usual (it no longer sends a 503 error code).

For details on these operations, refer to the section that describes the Handling of SS7 and SIP abnormal failure cases feature in the SDM Product Description.

Load PEM Files

This operation can be executed to load a TLS certificate and private key from the following known PEM files onto the database: `/tmp/cacert.pem and /tmp/cakey.pem`.Take note that in this release, multiple certificates are not supported, only one certificate and private key can be loaded.

At system startup, a certificate & a private key are provisioned and stored by default in the `/tmp/cacert.pem and /tmp/cakey.pem` files.

If the Network Operator chooses to use them, he must simply load them onto the system by performing the LoadPEMFiles() operation (see instructions below).

Otherwise, if the Network Operator chooses to use another certificate/private key, he must follow these steps:

1. Connect to the system's active System Controller blade and store the certificate/private key onto the database's PEM files: `/tmp/cacert.pem and /tmp/cakey.pem`.
2. Load the certificate/private key by performing the LoadPEMFiles() operation

In order to perform the LoadPEMFiles() operation, simply follow these steps from the WebCI's Server Configuration window (refer to the previous figure):

Prerequisite: Store the TLS certificate and private key into the database in the following well known PEM files: `/tmp/cacert.pem and /tmp/cakey.pem`

1. Click on the `Load PEM Files` button located underneath the SipServerTlsConfig table.
2. The following message will appear: "You are about to perform LoadPEMFiles, Continue?". Click on `Ok` to continue or `Cancel` if you wish to abort.
3. The PEM files will be invoked and loaded on the system. The following message will appear to inform you that the operation was successfully completed: "

```
The SIP TLS pem files have been successfully installed.
```

Display Certificate

This operation can be executed to display the details of the Certificate. Simply click on the `Display Certificate` button located underneath the SipServerTlsConfig table in the WebCI's Server Configuration window (refer to the previous figure). When the Display Certificate window opens, it will display the TLS Certificate and Private Key. Click on the `Close` button to exit.

If you wish to delete or modify the TLS Certificate and Private key, you must contact the Tekelec Customer Care Center and the Hlr service will need to be restarted.

Viewing/Editing SIP Security Configuration

The WebCI's Security window displays the SIP Security Configuration data.

The following data can be modified by the Network Operator:

- NonceValidityDuration
- GlobalRealm*
- DigestDomain*

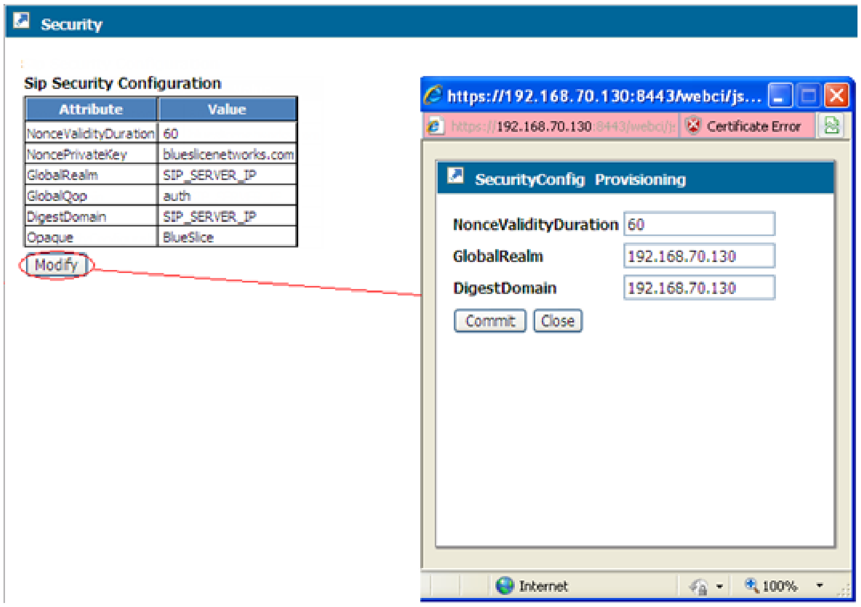
Important: Take note that when editing this information, in order for the new value to be committed and used by the HLR, the Network Operator must manually perform the following:

1. Stop all the HLR services that run the SIP Server.
2. Start all the HLR services that run the SIP Server.

Stopping and starting the HLR services will affect traffic, so make sure to perform this during down time if necessary. Refer to section "Starting and Stopping Services on a blade" of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for more information on how to stop a service.

For more details on these tables and their parameters, refer to the "SIP Security" section in the *SDM System Configuration – Reference Manual* .

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to the section: "Using the WebCI" in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).


Security
https://192.168.70.130:8443/webci/js...
https://192.168.70.130:8443/webci/j
Certificate Error
Internet
100%

Sip Security Configuration

Attribute	Value
NonceValidityDuration	60
NoncePrivateKey	bluesl icenetworks.com
GlobalRealm	SIP_SERVER_IP
GlobalQop	auth
DigestDomain	SIP_SERVER_IP
Opaque	BlueSlice

Modify

SecurityConfig Provisioning

NonceValidityDuration 60

GlobalRealm 192.168.70.130

DigestDomain 192.168.70.130

Commit Close

Figure 65: Displaying/Editing The SIP Security Configuration

Viewing/Editing SIP Registrar Configuration

Depending on the Network Operator's network architecture and needs, the SDM can play the role of a SIP Registrar as part of its SIP application capabilities.

The WebCI's Registrar window displays the Registrar Configuration table from the Configuration tab and the RegistrationBinding table from the RegistrationBinding tab. Simply opening the Registrar window will automatically display the Configuration tab.

To view the Registration Bindings, click on the Registration Binding tab. Note that you can also view the RegistrationBindings of a specific Address Of Record, to do so, please refer to the "Viewing/Editing

SIP Subscriber profiles (Address Of Records)" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

The Registrar Configuration table displays the following:

1. SIP Registrar configuration data:
2. The maximum Registrar Clients supported
3. The maximum contacts supported per Address of Record.
4. The minimum/maximum/default Registration duration
5. The Registration Binding Expiry Timestamp activation
6. The Registration Binding Cleanup activation/time

   The RegistrationBinding table displays the following:

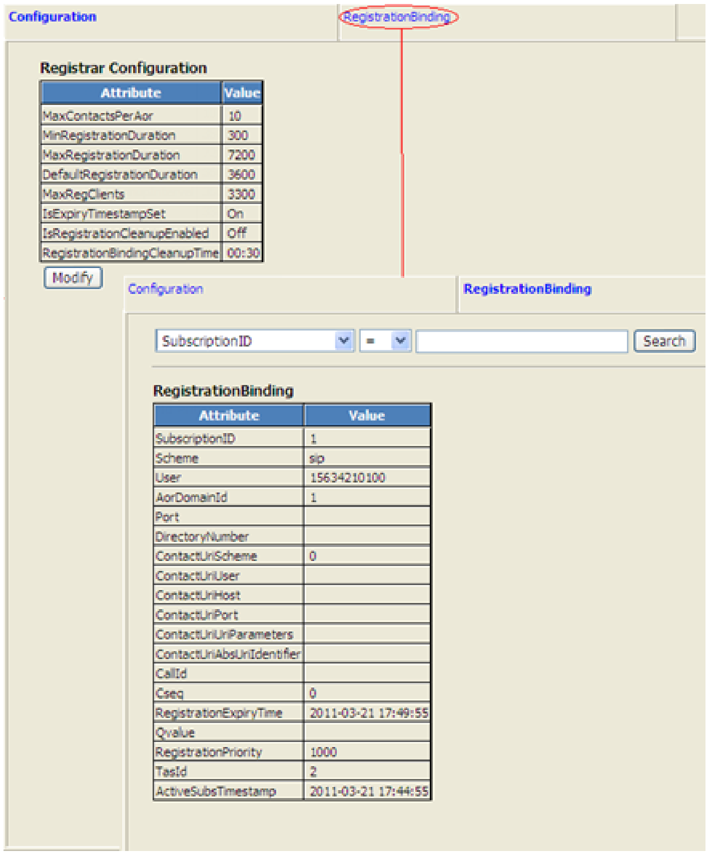
7. All or a list of specific SIP subscriber's RegistrationBindings that are driven by the system.

   The Network Operator can specify and limit the display of the RegistrationBindings using the Search engine. Refer to Displaying SIP UaRegistrationBinding for step-by-step instructions on how to use the WebCI's search engine.

   For more details on these tables and their parameters, refer to the "SIP Registrar" section in the *SDM System Configuration – Reference Manual* .

   For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

   Important: This Table Is NOT GEO-replicated So The Network Operator Must Update This Table On Both GEO Sites



Registrar Configuration

Attribute	Value
MaxContactsPerAor	10
MinRegistrationDuration	300
MaxRegistrationDuration	7200
DefaultRegistrationDuration	3600
MaxRegClients	3300
IsExpiryTimestampSet	On
IsRegistrationCleanupEnabled	Off
RegistrationBindingCleanupTime	00:30

RegistrationBinding

Attribute	Value
SubscriptionID	1
Scheme	sip
User	15634210100
AorDomainId	1
Port	
DirectoryNumber	
ContactUriScheme	0
ContactUriUser	
ContactUriHost	
ContactUriPort	
ContactUriUriParameters	
ContactUriAbsUriIdentifier	
CallId	
Cseq	0
RegistrationExpiryTime	2011-03-21 17:49:55
Qvalue	
RegistrationPriority	1000
TasId	2
ActiveSubsTimestamp	2011-03-21 17:44:55

Figure 66: Displaying/Editing The SIP Registrar Configuration

Viewing/Editing SIP Redirect Configuration

Depending on the Network Operator’s network architecture and needs, the SDM can play the role of a SIP Redirect Server as part of its SIP application capabilities.

The Network Operator can display or modify the SIP Redirect Server configuration, by displaying or editing the RedirectConfig table. Simply opening the Redirect window will automatically display the data provisioned in the RedirectConfig table.

The operation that applies to the RedirectConfig table and that can be executed during running time of the system (without a restart of the HLR services required) is as follows:

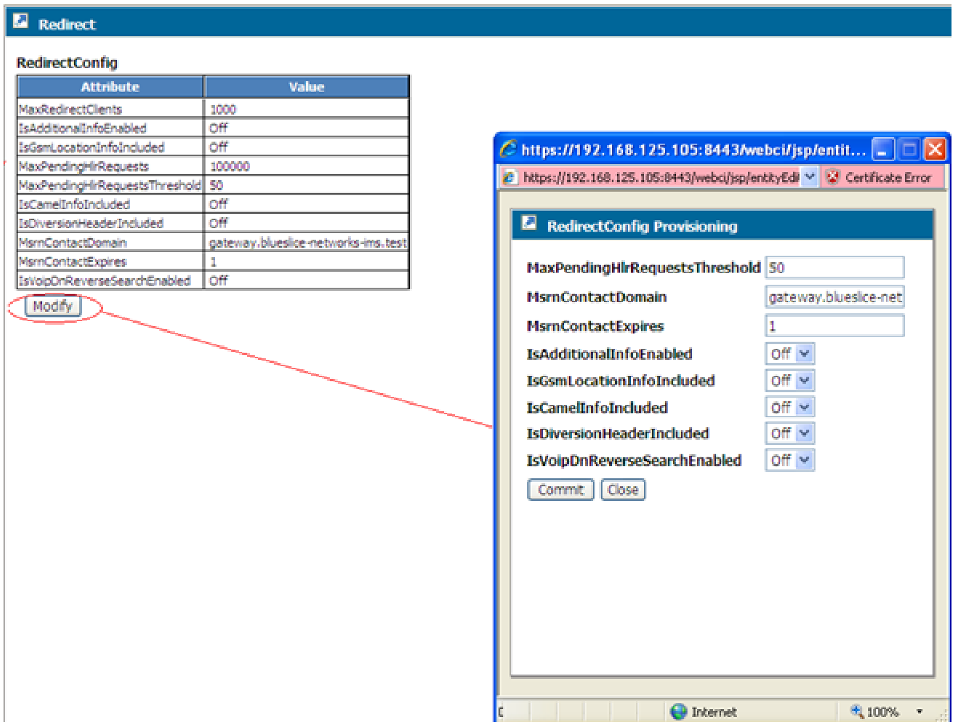
Modify. The following parameters can be modified:

1. MaxPendingHlrRequestsThreshold
2. MsrnContactDomain
3. MsrnContactExpires
4. IsAdditionalInfoEnabled
5. IsGsmLocationInfoIncluded

6. IsCamelInfoIncluded
7. IsDiversionHeaderIncluded
8. IsVoipDnReverseSearchEnabled

Refer to the “SIP Redirect Server section” of the *SDM System Configuration - Reference Manual* for more detailed information on these parameters and their value range.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



RedirectConfig

Attribute	Value
MaxRedirectClients	1000
IsAdditionalInfoEnabled	Off
IsGsmLocationInfoIncluded	Off
MaxPendingHlrRequests	100000
MaxPendingHlrRequestsThreshold	50
IsCamelInfoIncluded	Off
IsDiversionHeaderIncluded	Off
MsrnContactDomain	gateway.blueslice-networks-ims.test
MsrnContactExpires	1
IsVoipDnReverseSearchEnabled	Off

Modify
https://192.168.125.105:8443/webci/jsp/entit...
https://192.168.125.105:8443/webci/jsp/entityEdi
Certificate Error
RedirectConfig Provisioning

MaxPendingHlrRequestsThreshold: 50
MsrnContactDomain: gateway.blueslice-net
MsrnContactExpires: 1
IsAdditionalInfoEnabled: Off
IsGsmLocationInfoIncluded: Off
IsCamelInfoIncluded: Off
IsDiversionHeaderIncluded: Off
IsVoipDnReverseSearchEnabled: Off

Figure 67: Displaying/Editing The SIP Redirect Server Configuration

Viewing/Editing SIP User Agent (RegClient) Configuration

Depending on the Network Operator’s network architecture and needs, the SDM can play the role of a SIP User Agent (RegClient) as part of its SIP application capabilities.

The WebCI’s User Agent window displays the User Agent Configuration, User Agent Register Configuration and User Agent Persistent Contact tables from the User Agent tab and the User Agent RegistrationBinding table from the Registration Binding tab.

The Network Operator can display or modify the SIP User Agent configuration, by displaying or editing these tables. Simply opening the User Agent window will automatically display the User Agent tab.

To view the User Agent Registration Bindings, simply click on the Registration Binding tab. Refer to *Displaying WebCI window content using a search* for step-by-step instructions on how to use the WebCI's search engine.

Note: The SipUa registration bindings are not persistent across a system restart. Therefore, after a restart the SipUa registration bindings are reset and the table is empty. You can also view the RegistrationBindings of a specific Address Of Record, to do so, please refer to the "Viewing/Editing SIP Subscriber profiles (Address Of Records)" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

The other operation that can be executed during running time of the system (without a restart of the HLR services required) is as follows:

Modify. This operation is available for the User Agent Configuration and User Agent Register Configuration tables.

The User Agent Configuration table's following parameters can be modified:

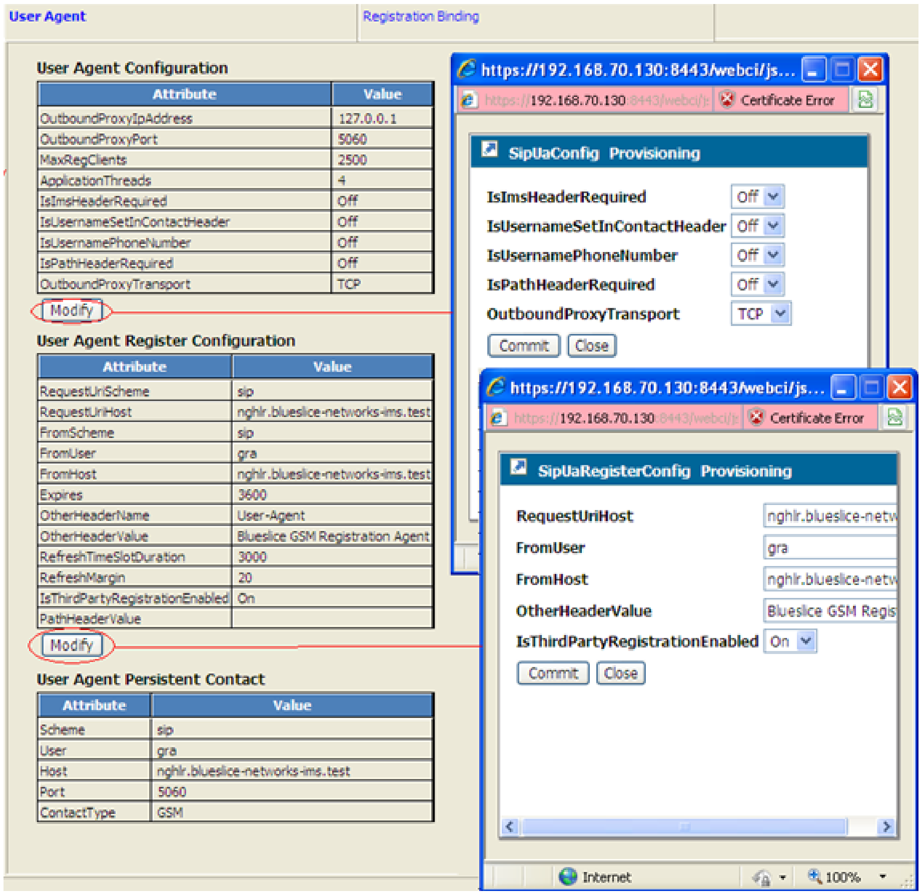
- IsImsHeaderRequired
- IsUsernameSetInContactHeader
- IsUsernamePhoneNumber
- IsPathHeaderRequired
- OutboundProxyTransport

The User Agent Register Configuration table's following parameters can be modified:

- RequestUriHost
- FromUser
- FromHost
- OtherHeaderValue
- IsThirdPartyRegistrationEnabled

Refer to the "User Agent" section of the *SDM System Configuration-Reference Manual* for more detailed information on these parameters and their value range.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



User Agent Configuration

Attribute	Value
OutboundProxyIpAddress	127.0.0.1
OutboundProxyPort	5060
MaxRegClients	2500
ApplicationThreads	4
IsImsHeaderRequired	Off
IsUsernameSetInContactHeader	Off
IsUsernamePhoneNumber	Off
IsPathHeaderRequired	Off
OutboundProxyTransport	TCP

User Agent Register Configuration

Attribute	Value
RequestUriScheme	sip
RequestUriHost	nghlr.blueslice-networks-ims.test
FromScheme	sip
FromUser	gra
FromHost	nghlr.blueslice-networks-ims.test
Expires	3600
OtherHeaderName	User-Agent
OtherHeaderValue	Blueslice GSM Registration Agent
RefreshTimeSlotDuration	3000
RefreshMargin	20
IsThirdPartyRegistrationEnabled	On
PathHeaderValue	

User Agent Persistent Contact

Attribute	Value
Scheme	sip
User	gra
Host	nghlr.blueslice-networks-ims.test
Port	5060
ContactType	GSM

https://192.168.70.130:8443/webci/js...
https://192.168.70.130:8443/webci/j
Certificate Error

SipUaConfig Provisioning

IsImsHeaderRequired	Off
IsUsernameSetInContactHeader	Off
IsUsernamePhoneNumber	Off
IsPathHeaderRequired	Off
OutboundProxyTransport	TCP

Commit
Close
https://192.168.70.130:8443/webci/js...
https://192.168.70.130:8443/webci/j
Certificate Error

SipUaRegisterConfig Provisioning

RequestUriHost	nghlr.blueslice-netw
FromUser	gra
FromHost	nghlr.blueslice-netw
OtherHeaderValue	Blueslice GSM Regis
IsThirdPartyRegistrationEnabled	On

Figure 68: Displaying/Editing The SIP User Agent Configuration

Viewing/Editing SIP TAS Configuration for 3rd Party Registration

With the 'SRI Router' feature, the SDM ngHLR and its SIP Registrar functionality can route mobile terminated calls from the cellular domain to a Telephony Application Server (TAS) when a subscriber is registered in the SIP/IMS domain.

The SIP registration binding is updated with the ID of the TAS the SIP REGISTER comes from. The information of the TasId (configured in the SipTasGt table) will then be used by the SDM ngHLR when receiving a SRI message, in order to relay the SRI message based on the information of the TAS ID found in the SIP registration binding. The SDM ngHLR reroutes the message to the correct TAS (modifying the CdPA Gt and Tt) if the Subscriber is SIP registered or return the message to GSM with a different Translation Type if the Subscriber is not SIP registered.

To achieve this, the SIP Registrar can support part of the 3rd party registrations from a TAS, as follows:

If a 3rd party registration is detected (in SIP, a third party registration is where the "To" and "From" headers are different), the following logic is applied:

1. The FROM URI user part is NOT mandatory.

   If a user part is received, it is ignored.

2. The 3rd party REGISTER is NOT rejected if the host part of the FROM header (i.e.

TAS FQDN) is provisioned in the SipTasGt table.

3. If the 3rd party IMS REGISTER is detected but the TAS FQDN is NOT provisioned, the request is rejected with 404.

If the “To” and the “From” headers are equal, the normal SIP Registration processes are followed (the processes followed without this feature).

This functionality is always activated by default and invoked when a 3rd party registration is detected at runtime.

The WebCI’s SIP Tas window displays the SipTasGt table, which allows to map the SIP registration binding to a TAS GT address. Through this window, the Network Operator can display/add/modify/delete the configuration data for each TAS the SDM ngHLR/SIP will communicate with. This table shall be provisioned with the FQDN of each TAS.

The Network Operator can provision dynamically the SipTasGt table (display/add/modify/delete) during the system’s running-time, by clicking on the WebCI’s ‘Add SipTasGt’, ‘Modify’ or ‘Delete’ buttons. Simply opening the SIP Tas window will automatically display the SipTasGt table.

Note: To remove an entry from this table, there must be no subscribers with the TasId in RegistrationBinding table.

As a particularity, the special entry below is permanent (cannot be deleted). It’s used by the Tekelec ngHLR for the default TasId. If the Subscriber is not found or the Subscriber is not SIP registered or for any other errors, the Tt of the TasId 0 will be used. The Gt of TasId 0 is not used because only the Translation Type is changed in case of a Tekelec ngHLR error. The Network Operator can modify the value of the TasName and of the Translation Type for the default TasId 0.

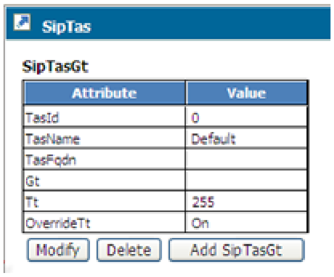
Table 17: SipTasGt permanent entry

TasId	TasName	TasFqdn	Gt	Tt	OverrideTt
0	Default			255	1

Refer to the SipTasGt description in the “SIP Configuration” section of the *SDM System Configuration-Reference Manual* for more details on the SipTasGt table and its parameters and their value range.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document describes the procedures to follow to provision tables in the WebCI).

Hereunder Is The WebCI’s SIP Tas Window:



SipTasGt

Attribute	Value
TasId	0
TasName	Default
TasFqdn	
Gt	
Tt	255
OverrideTt	On

Figure 69: Displaying/Editing The SIP Tas Configuration

Viewing and editing SIP TAS configuration for 3rd party registration

With the ‘SRI Router’ feature, the SDM ngHLR and its SIP Registrar functionality can route mobile terminated calls from the cellular domain to a Telephony Application Server (TAS) when a subscriber is registered in the SIP/IMS domain.

The SIP registration binding is updated with the ID of the TAS the SIP REGISTER comes from. The information of the TasId (configured in the SipTasGt table) will then be used by the SDM ngHLR when receiving a SRI message, in order to relay the SRI message based on the information of the TAS ID found in the SIP registration binding. The SDM ngHLR reroutes the message to the correct TAS (modifying the CdPA Gt and Tt) if the Subscriber is SIP registered or return the message to GSM with a different Translation Type if the Subscriber is not SIP registered.

To achieve this, the SIP Registrar can support part of the 3rd party registrations from a TAS, as follows:

If a 3rd party registration is detected (in SIP, a third party registration is where the “To” and “From” headers are different), the following logic is applied:

1. The FROM URI user part is NOT mandatory. If a user part is received, it is ignored
2. The 3rd party REGISTER is NOT rejected if the host part of the FROM header (i.e. TAS FQDN) is provisioned in the SipTasGt table.
3. If the 3rd party IMS REGISTER is detected but the TAS FQDN is NOT provisioned, the request is rejected with 404.

If the “To” and the “From” headers are equal, the normal SIP Registration processes are followed (the processes followed without this feature).

This functionality is always activated by default and invoked when a 3rd party registration is detected at runtime.

The WebCI’s SIP Tas window displays the SipTasGt table, which allows to map the SIP registration binding to a TAS GT address. Through this window, the Network Operator can display/add/modify/delete the configuration data for each TAS the SDM ngHLR/SIP will communicate with. This table shall be provisioned with the FQDN of each TAS.

The Network Operator can provision dynamically the SipTasGt table (display/add/modify/delete) during the system’s running-time, by clicking on the WebCI’s ‘Add SipTasGt’, ‘Modify’ or ‘Delete’ buttons. Simply opening the SIP Tas window will automatically display the SipTasGt table.

Note: To remove an entry from this table, there must be no subscribers with the TasId in RegistrationBinding table.

As a particularity, the special entry below is permanent (cannot be deleted). It’s used by the Tekelec ngHLR for the default TasId. If the Subscriber is not found or the Subscriber is not SIP registered or for any other errors, the Tt of the TasId 0 will be used. The Gt of TasId 0 is not used because only the Translation Type is changed in case of an Tekelec ngHLR error. The Network Operator can modify the value of the TasName and of the Translation Type for the default TasId 0.

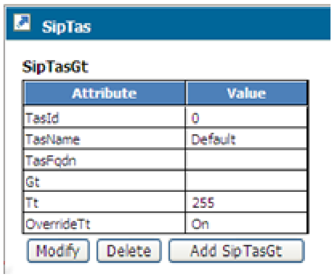
Table 18: SipTasGt permanent entry

TasId	TasName	TasFqdn	Gt	Tt	OverrideTt
0	Default			255	1

Refer to the SipTasGt description in the “SIP Configuration” section of the *SDM System Configuration-Reference Manual* for more details on the SipTasGt table and its parameters and their value range.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document describes the procedures to follow to provision tables in the WebCI).

Hereunder Is The WebCI’s SIP Tas Window:



SipTasGt

Attribute	Value
TasId	0
TasName	Default
TasFqdn	
Gt	
Tt	255
OverrideTt	On

Figure 70: Displaying/Editing The SIP Tas Configuration

Viewing/Editing SIP User Portability configuration

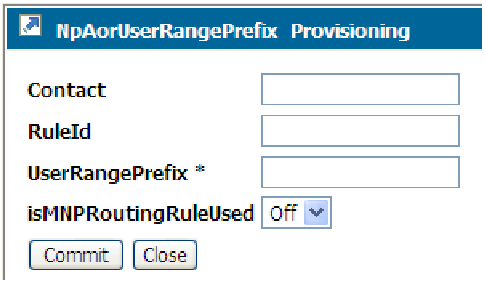
Viewing SIP NP Support for AOR Ranges feature status

1. From the main menu, go to SIP > User Portability
   The UserPortability window displays.
2. In the RedirectConfig table, view the value of the IsSipRangeSupportEnabled attribute.
   When set to On, the SIP NP Support for AOR Ranges feature is enabled.

Configuring SIP NP Support for AOR Ranges feature

The SIP NP Support for AOR Ranges, feature allows the operator to define groups or ranges of users using prefixe sand provision information to redirect SIP INVITE request that are sent to any of these users.

1. From the main menu, go to SIP > User Portability
   The UserPortability window displays.
2. Click the Add button of the NpAorUserRangePrefix table to set up the user range and specify whether the MNP routing rule shall be used.
   The NpAorUserRangePrefix Provisioning window displays.



NpAorUserRangePrefix Provisioning

Contact

RuleId

UserRangePrefix *

isMNPRoutingRuleUsed Off

3. Type the prefix to be used for the range of users
4. Turn On or Off the use of MNP routing rules
    - If MNP routing rules are to be used, also enter the routing rule to use
    - If MNP routing rules are not to be used, add the contact information to be returned in the 302 response.
5. From the main menu, go to SIP > Redirect to enable the SIP NP Support for the AOR Ranges feature. The Redirect window displays.
6. Click the Modify button of the RedirectConfig table.
7. Set the IsSipRangeSupportEnabled attribute to On

    For more information about these attributes, refer to the respective tables in the System Configuration Reference Manual.

Chapter 7

IMS-HSS/SLF Application Configuration

Topics:

This chapter outlines the procedures to configure the IMS-HSS and SLF.

Introduction

The procedures in this chapter show you how to view/modify the IMS-HSS and SLFconfiguration, configure the IMS-HSS AuC, configure the IMS-HSS System Features and the Shared Initial Filtering Criterias. To perform the tasks in the following table, refer to the corresponding section within this chapter.

Requirements: Log in to a WebCI session with a username and password.

Table 19: IMS-HSS/SLF application procedures

Task
Viewing/Editing IMS-HSS and SLF Configuration
Configuring the IMS-HSS AuC
Configuring the IMS-HSS System Features
Configuring Shared Initial Filtering Criterias

For details on the parameters used to configure the IMS-HSS/SLF, the IMS-HSS AuC, IMS-HSS System Features and Shared Initial Filtering Criterias, refer to the "IMS-HSS Entities" section in the *SDM System Configuration - Reference Manual*.

Configuring the IMS-HSS/SLF

The IMS-HSS and SLF are usually configured at installation by the Tekelec *Customer Care Center*. They are both independent from each other, but they are presented together here since they follow similar configuration logic.

The following information needs to be configured at installation in order to run the IMS-HSS and/or SLF applications:

- IMS-HSS and/or SLF configuration information
- On/Off flags to enable/disable independently the IMS-HSS and SLF applications.
- The network information (Local FQDN, LocalSTCPPort, LocalTCPPort, OriginatingRealm, SCTPTransport, TCPTransport, TCP Listen Address, SCTP Listen Address, Destination Realms, Destination Hosts, etc.) needed for the IMS-HSS/SLF to communicate with the peer servers.

Viewing/Editing IMS-HSS/SLF Configuration

The operator can view all of the IMS-HSS and SLF configuration information from the WebCI's IMS-HSS folder and SLF folder respectively, by opening the IMS-HSS Configuration window or the SLF Configuration window. Some of this information can be modified and network information can be deleted/added.

Note: Prior to making any changes (adding, modifying, deleting) to the IMS-HSS/SLF Configuration data during running-time, the IMS-HSS service must first be stopped. Once the changes are made, the

IMS-HSS service can be started once again. This will affect traffic, so make sure to perform this during down time if necessary. Refer to section “Starting and Stopping Services on a blade” of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for more information on how to stop a service.

The Hss Config and Slf Config tables can both be edited, by clicking on the **Modify** button located in the same row as the entry you wish to edit.

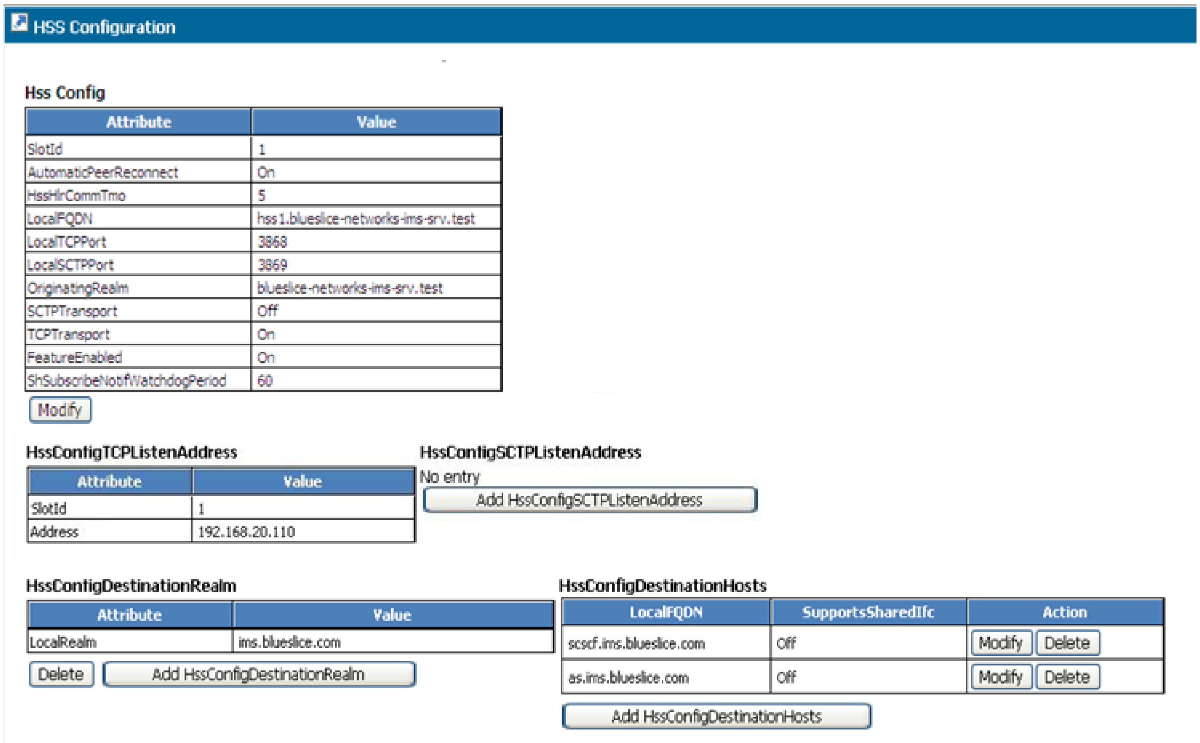
In order to edit the network information, if there is no Modify button available, you must delete the entry by clicking on the Delete button located in the same row as the entry you wish to modify and re-create it by clicking on the Add button.

Further network information can be configured in the other tables displayed in the HSS Configuration/SLF Configuration windows.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

For details on the HSS/SLF configuration parameters, refer to the “IMS-HSS Entities” section in the *SDM System Configuration - Reference Manual* .

Note: Only one TCP or SCTP Listen Address can be configured and it cannot be modified. If it needs to be edited, contact Tekelec Support Team.



Hss Config

Attribute	Value
SlotId	1
AutomaticPeerReconnect	On
HssHlrCommTmo	5
LocalFQDN	hss1.blueslice-networks-ims-srv.test
LocalTCPPort	3868
LocalSCTPPort	3869
OriginatingRealm	blueslice-networks-ims-srv.test
SCTPTransport	Off
TCPTransport	On
FeatureEnabled	On
ShSubscribeNotifWatchdogPeriod	60

HssConfigTCPListenAddress

Attribute	Value
SlotId	1
Address	192.168.20.110

HssConfigSCTPListenAddress

No entry

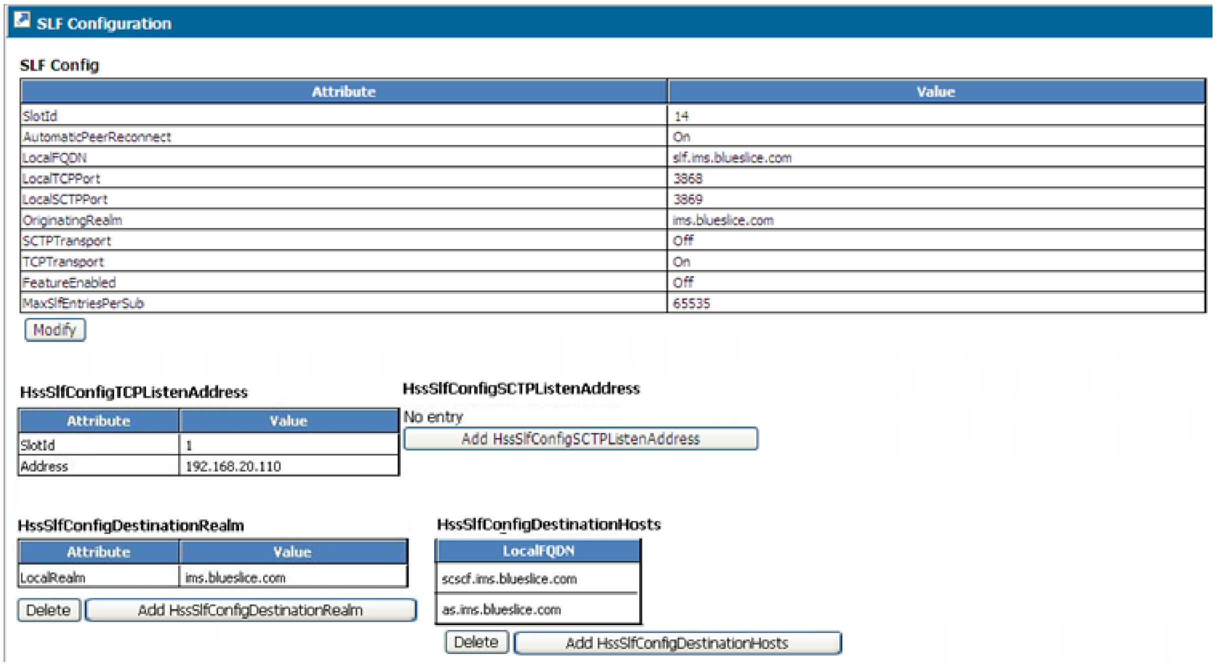
HssConfigDestinationRealm

Attribute	Value
LocalRealm	ims.blueslice.com

HssConfigDestinationHosts

LocalFQDN	SupportsSharedIfc	Action
scscf.ims.blueslice.com	Off	Modify Delete
as.ims.blueslice.com	Off	Modify Delete

Figure 71: IMS-HSS Configuration Window


SLF Configuration
Modify
Add HssSlfConfigSCTPListenAddress
Delete
Add HssSlfConfigDestinationRealm
Delete
Add HssSlfConfigDestinationHosts

SLF Config

Attribute	Value
SlotId	14
AutomaticPeerReconnect	On
LocalFQDN	slf.ims.blueslice.com
LocalTCPPort	3868
LocalSCTPPort	3869
OriginatingRealm	ims.blueslice.com
SCTPTransport	Off
TCPTransport	On
FeatureEnabled	Off
MaxSlfEntriesPerSub	65535

HssSlfConfigTCPListenAddress

Attribute	Value
SlotId	1
Address	192.168.20.110

HssSlfConfigSCTPListenAddress

No entry

HssSlfConfigDestinationRealm

Attribute	Value
LocalRealm	ims.blueslice.com

HssSlfConfigDestinationHosts

LocalFQDN
scscf.ims.blueslice.com
as.ims.blueslice.com

Figure 72: SLF Configuration Window

Once the SLF has been configured, you can provision SLF users (provision Redirect Host Mapping) in order to link Private Identities to their corresponding IMS-HSS host. You can provision SLF users in bulk using XML files, for instructions on this, refer to the *SDM Subscriber Provisioning – User Guide*. If you wish to view/edit/provision SLF users from the WebCI, refer to the “Viewing/Editing IMS-HSS Subscriber Profiles” section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

Configuring the IMS-HSS AuC

The IMS-HSS Authentication Center (AuC) is used to provide authentication to IMS-HSS/SLF users on the IMS networks. The IMS-HSS Authentication Center supports the following authentication schemas and algorithms:

Table 20: Authentication schemas and algorithms

IMS-HSS Authentication Schemas	IMS-HSS Authentication algorithms
Digest	MD5
Digest-AKAv1-MD5	GsmMilenage
Digest-MD5	BasicDigest
Early-IMS-Security	Early-IMS-Security
HTTP_DIGEST_MD5	HttpDigest
NASS-Bundled	TISPAN

IMS-HSS Authentication Schemas	IMS-HSS Authentication algorithms
NoSchema	NoAlgoName

For more details on the IMS-HSS Authentication Center, refer to the "IMS-HSS Authentication Center" section in the *SDM Product Description* .

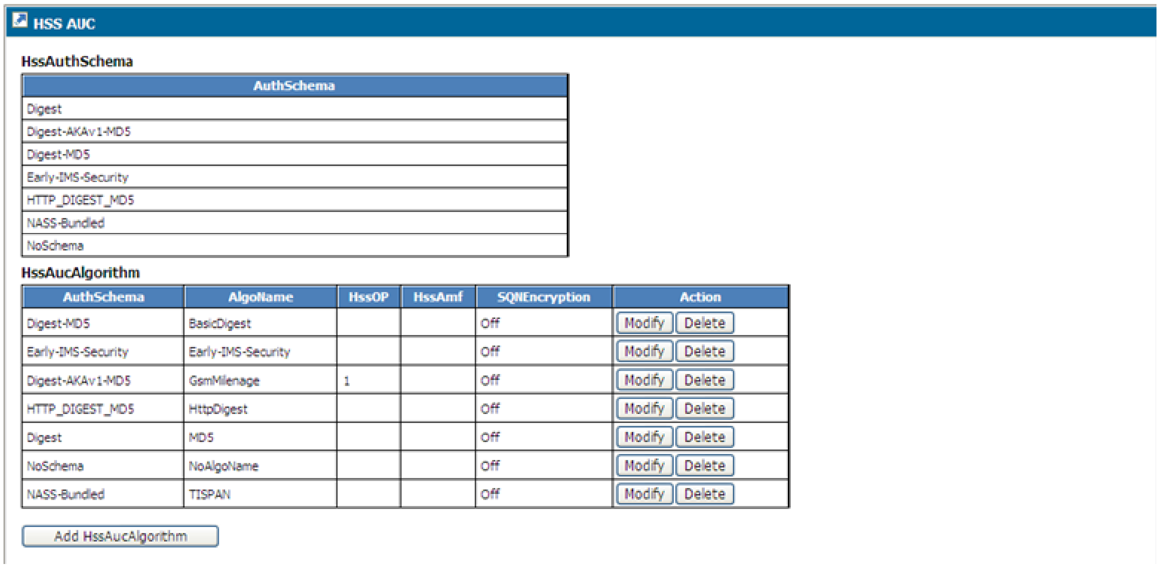
The IMS-HSS Authentication Center's Authentication schemas are usually configured at installation by Tekelec's Customer Care Center. The Network Operator can provision the authentication algorithms that will be used for the supported schemas. To achieve this, the HssAucAlgorithm table must be provisioned from the WebCI's HSS Auc window, which can be opened by extending the HSS folder.

The WebCI also provides a way to define specific Gsm Milenage algorithm by setting the variant part of the algorithm like OP, Amf, C1-C5, R1-R5 values. These values are used in the algorithm to generate the Quintuplet vector. These values are variants in the algorithm and are set to the default values.

The HSS AuC allows you to specialize and define your own algorithm to ensure you a more robust encryption. If you wish to do so, contact the Tekelec Customer Care Center, whom will assist you and store the algorithm file in a library.

For instructions on how to open the HSS Auc window and on how to provision the HssAucAlgorithm table, follow the logic described in *Web Craft Interface (WebCI)* of this document.

Refer to the "HSS AuC" section of the *SDM System Configuration – Reference Manual* for more details on the HssAuthSchema and HssAucAlgorithm entities and their parameters and values.



HssAuthSchema

AuthSchema
Digest
Digest-AKAv1-MD5
Digest-MD5
Early-IMS-Security
HTTP_DIGEST_MD5
NASS-Bundled
NoSchema

HssAucAlgorithm

AuthSchema	AlgoName	HssOP	HssAmf	SQNEncryption	Action
Digest-MD5	BasicDigest			Off	Modify Delete
Early-IMS-Security	Early-IMS-Security			Off	Modify Delete
Digest-AKAv1-MD5	GsmMilenage	1		Off	Modify Delete
HTTP_DIGEST_MD5	HttpDigest			Off	Modify Delete
Digest	MD5			Off	Modify Delete
NoSchema	NoAlgoName			Off	Modify Delete
NASS-Bundled	TISPAN			Off	Modify Delete

Figure 73: IMS-HSS AUC Window

Other Operations

In addition to provisioning the HssAucAlgorithm table with new entries, the following operations are also available:

Delete One entry at a time can be deleted in the HssAucAlgorithm table.

Modify One entry at a time can be modified.

Configuring IMS-HSS System Features

The following information needs to be defined in order to configure IMS-HSS System Features:

1. Charging Information
2. S-CSCF Servers
3. Authorized Visited Networks
4. AS Permission List

   Each of these definitions is identified by a unique ID and can be used by multiple Private Identities. This allows to provision Private Identities (IMPIs) with whichever one of these definitions by simply referring to the desired IDs. Refer to the "Viewing/Editing IMS-HSS Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* , for instructions on how to view/edit/provision Private Identities from the WebCI. For instructions on how to provision Private Identities in bulk using XML files, refer to the *SDM Subscriber Provisioning – User Guide* .

In order to configure these definitions, the HssChargingInfo, HssScscfServer, HssAuthorizedVisitedNetworks, and ASPermList tables must be provisioned from the WebCI's HSS System Features window that can be accessed from the menu's HSS folder.

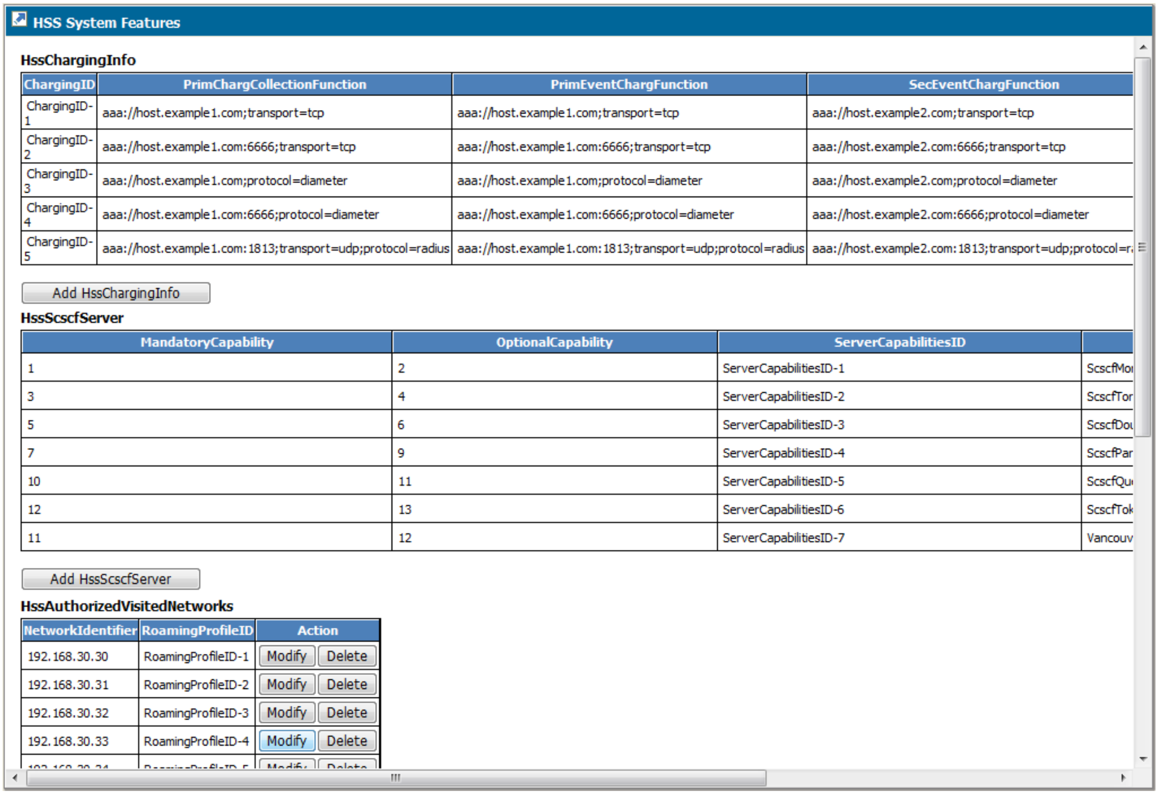
Note: These tables must be provisioned prior to being able to provision IMS-HSS Subscriber profiles.

The following operations are also available:

Delete This button is available for each table and only one entry at a time can be deleted.

Note: It is not possible to delete an entry that is still referred by Private Identities (IMS-HSS Subscriber profiles). Edit those Private Identities and refer to another definition by changing it to the ID of an entry that will remain configured.

Modify This button is available for each table and only one entry at a time can be modified.



HssChargingInfo

ChargingID	PrimChargCollectionFunction	PrimEventChargFunction	SecEventChargFunction
ChargingID-1	aaa://host.example1.com;transport=tcp	aaa://host.example1.com;transport=tcp	aaa://host.example2.com;transport=tcp
ChargingID-2	aaa://host.example1.com:6666;transport=tcp	aaa://host.example1.com:6666;transport=tcp	aaa://host.example2.com:6666;transport=tcp
ChargingID-3	aaa://host.example1.com;protocol=diameter	aaa://host.example1.com;protocol=diameter	aaa://host.example2.com;protocol=diameter
ChargingID-4	aaa://host.example1.com:6666;protocol=diameter	aaa://host.example1.com:6666;protocol=diameter	aaa://host.example2.com:6666;protocol=diameter
ChargingID-5	aaa://host.example1.com:1813;transport=udp;protocol=radius	aaa://host.example1.com:1813;transport=udp;protocol=radius	aaa://host.example2.com:1813;transport=udp;protocol=r

HssScscfServer

MandatoryCapability	OptionalCapability	ServerCapabilitiesID	
1	2	ServerCapabilitiesID-1	ScscfMo
3	4	ServerCapabilitiesID-2	ScscfTor
5	6	ServerCapabilitiesID-3	ScscfDo
7	9	ServerCapabilitiesID-4	ScscfPar
10	11	ServerCapabilitiesID-5	ScscfQu
12	13	ServerCapabilitiesID-6	ScscfTok
11	12	ServerCapabilitiesID-7	Vancouv

HssAuthorizedVisitedNetworks

NetworkIdentifier	RoamingProfileID	Action
192.168.30.30	RoamingProfileID-1	Modify Delete
192.168.30.31	RoamingProfileID-2	Modify Delete
192.168.30.32	RoamingProfileID-3	Modify Delete
192.168.30.33	RoamingProfileID-4	Modify Delete

Figure 74: HSS System Features Window

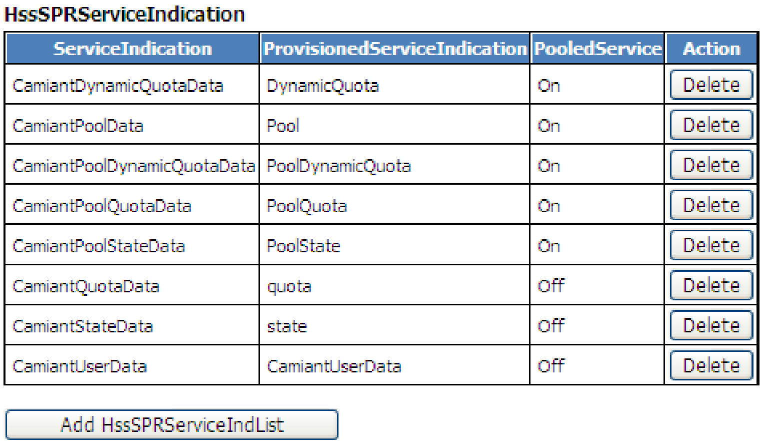
Configuring SPR service indications

This procedure defines the service indications that are provisioned through the OAM and associates them with the service indications sent by the PCRF in the Sh message.

At initial setup of the SPR functionality, the Tekelec *Customer Care Center* will load all Service Indications into the system.

The network operator can configure additional service indications or delete them. Use this procedure to configure service indications using the WebCI.

1. Go to **HSS ➤ HSS System Features**.
2. Locate the *HssSPRServiceIndication* table.

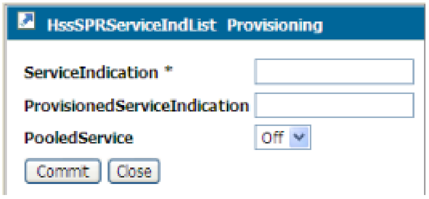


HssSPRServiceIndication

ServiceIndication	ProvisionedServiceIndication	PooledService	Action
CamiantDynamicQuotaData	DynamicQuota	On	Delete
CamiantPoolData	Pool	On	Delete
CamiantPoolDynamicQuotaData	PoolDynamicQuota	On	Delete
CamiantPoolQuotaData	PoolQuota	On	Delete
CamiantPoolStateData	PoolState	On	Delete
CamiantQuotaData	quota	Off	Delete
CamiantStateData	state	Off	Delete
CamiantUserData	CamiantUserData	Off	Delete

3. To add a new service indication, click **Add HssSPRServiceIndList**.

   The HssSPRServiceIndList Provisioning popup window displays.



HssSPRServiceIndList Provisioning

ServiceIndication *	
ProvisionedServiceIndication	
PooledService	Off

   a) Type the service indication from the Sh message into the first field. This field is mandatory.
      For example, type `CamiantPoolData`.
   b) Type the provisioned service indication into the second field.
      For example, type `Pool`.
   c) Set up pooled service.
      For example, select **On** from the drop-down list.
   d) Click **Commit** to save this service indication.

4. To delete a service indication, click its **Delete** button.

Configuring IMS-HSS Shared Initial Filtering Criterias

The IMS-HSS supports Shared Initial Filtering Criterias, which allows the Initial Filtering Criteria of different Service Profiles to be shared. For more details on this functionality, refer to the “Shared Initial Filter Criteria (iFC)” section of the *SDM Product Description* .

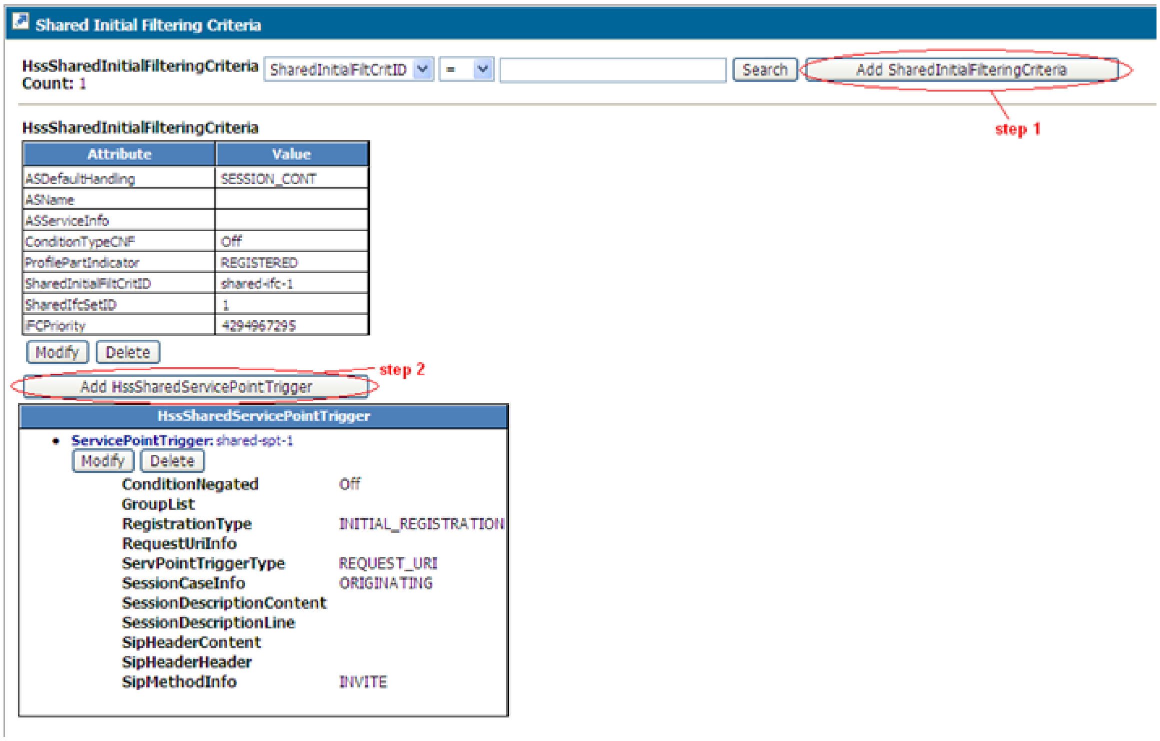
The Network Operator can define, at whatever given time, a list of Shared Initial Filtering Criterias independently of whether the remote S-CSCF supports SharedIFCs or not.

However, in order for this feature to work, the Network Operator must also configure which CSCF is capable of handling Shared IFCs. The configuration is dynamic and stored in the HssConfigDestinationHost table as an added field SupportsSharedIfc that can be turned On or Off. Refer to *Viewing/Editing IMS-HSS/SLF Configuration* of this document.

This section describes how to define Shared Initial Filtering Criterias and Shared Service Point Triggers and then how to assign them to service profiles.

To provision the IMS-HSS with Shared Initial Filtering Criterias, the operator must provision the following tables in the order presented below. These tables can be found in the WebCI's SharedInitialFilteringCriteria window, which can be opened by extending the HSS folder from the WebCI's menu.

1. Provision the HssSharedInitialFilteringCriteria table in order to define a Shared Initial Filtering Criteria, which is identified by a unique SharedInitialFiltCritID.
2. Provision the HssSharedServicePointTrigger table in order to define Shared Service Point Triggers for each Shared Initial Filtering Criteria defined.


Shared Initial Filtering Criteria
SharedInitialFiltCritID
=
Search
Add SharedInitialFilteringCriteria
step 1
Modify
Delete
step 2
Add HssSharedServicePointTrigger
Modify
Delete

HssSharedInitialFilteringCriteria
Count: 1

HssSharedInitialFilteringCriteria

Attribute	Value
ASDefaultHandling	SESSION_CONT
ASName	
ASServiceInfo	
ConditionTypeCNF	Off
ProfilePartIndicator	REGISTERED
SharedInitialFiltCritID	shared-ifc-1
SharedIfcSetID	1
IFCPriority	4294967295

HssSharedServicePointTrigger

- ServicePointTrigger: shared-spt-1

ConditionNegated	Off
GroupList	
RegistrationType	INITIAL_REGISTRATION
RequestUriInfo	
ServPointTriggerType	REQUEST_URI
SessionCaseInfo	ORIGINATING
SessionDescriptionContent	
SessionDescriptionLine	
SipHeaderContent	
SipHeaderHeader	
SipMethodInfo	INVITE

Figure 75: IMS-HSS Shared Initial Filtering Criteria Window

Once Shared IFCs have been defined, they can be assigned to IMS-HSS Service Profiles by linking the identifier of a Shared IFC to a IMS-HSS Service Profile. The Network Operator can achieve this by entering a SharedInitialFiltCritID as the value of the HssServiceProfile's InitialFilterCriteria attribute when provisioning a IMS-HSS service profile. For instructions on how to provision/edit IMS-HSS service profiles from the WebCI, refer to the "Viewing/Editing IMS-HSS Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* . For instructions on how to provision IMS-HSS Subscriber Profiles in bulk using XML files, refer to the *SDM Subscriber Provisioning – User Guide* .

Chapter 8

AAA Application Configuration

Topics:

This chapter outlines the procedures to configure the AAA.

Introduction

This chapter outlines the procedures to configure the AAA. The procedures in this chapter show you how to view/modify the AAA configuration, provision the Dynamic Address Allocation Policies and IP Address pools. To perform the tasks in the following table, refer to the corresponding section within this chapter.

Table 21: AAA Configuration Tasks

Task
View/Editing AAA Configuration
Configuring System and NAS Accounting Servers, Network Access Servers, System and NAS Authentication Servers
Provision Address Allocation Policies (AAA Provisioning Configuration)

Requirements**: Log in to a WebCI session with a username and password.**

For details on AAA Configuration and Dynamic Address Allocation Policies refer to the “AAA” chapter in the *SDM System Configuration - Reference Manual*.

Configuring the AAA

The AAA is usually configured at installation by Tekelec’s *Customer Care Center*. The following information needs to be configured at installation in order to run the AAA application:

- AAA configuration information
- On/Off flags to enable/disable the AAA application and the Accounting and Authentication Proxy Modes.
- The network information (Server port, AAA Listen Port, Server IP Address, AAA Listen IP Address, etc.) needed for the AAA to communicate with the peer servers: Network Access Servers, System Accounting Servers, NAS Accounting Servers, System Authentication Servers, NAS Authentication Servers.
- AAA Address Allocation Policies and IP Address pools.

Viewing/Editing AAA Configuration

The operator can view all of the AAA configuration information from the WebCI’s AAA folder, by opening the AAA Configuration window. Some of this information can be modified and network information can be deleted/added.

IMPORTANT: Take note that prior to making any changes (adding, modifying, deleting) to the AAA Configuration data during running-time, the IMS-HSS service must first be stopped. Once the changes are made, the IMS-HSS service can be started once again. This will affect traffic, so make sure to perform this during down time if necessary. Refer to section “Starting and Stopping Services on a blade" of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for more information on how to stop a service.

The AAA Config table can be edited, by clicking on the **Modify** button located underneath it.

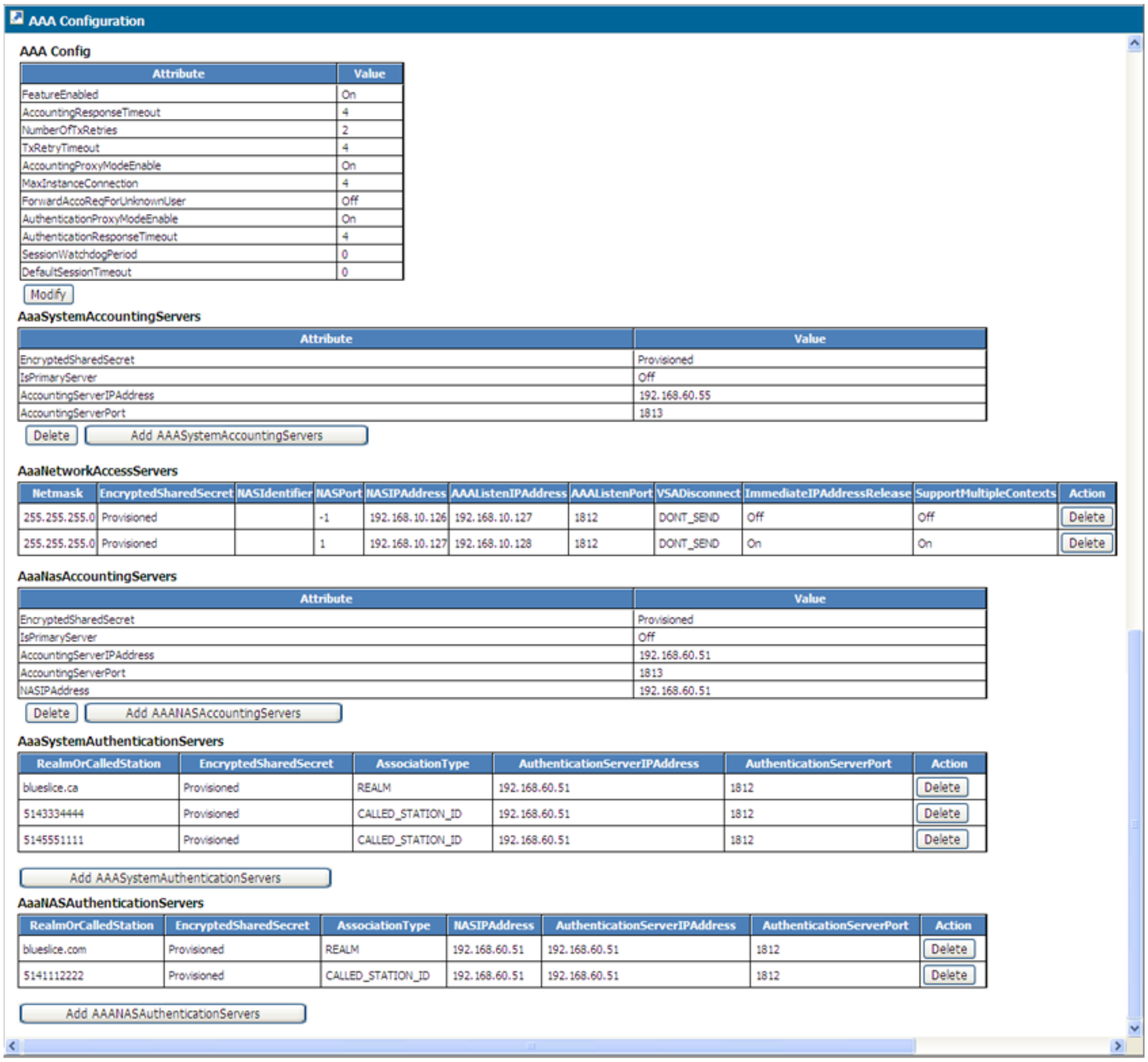
In order to edit the network information, you must delete the entry by clicking on the Delete button located in the same row as the entry you wish to modify and re-create it by clicking on the Add button.

Add AAA Network Access Servers

The following rules need to be followed when configuring the AAA Network Access Servers table:

1. To use two different ports, two entries must be provisioned in the AAA Network Access Servers table for one single NAS.

   Both of these entries can have the same NASIPAddress and the same AAAListenIPAddress.
2. To use one single port, only one entry needs to be configured in the AAA Network Access Servers table for one single NAS, but the NAS must be able to send both Access-Request and Accounting-Request messages to the same port.



AAA Config

Attribute	Value
FeatureEnabled	On
AccountingResponseTimeout	4
NumberOfTxRetries	2
TxRetryTimeout	4
AccountingProxyModeEnable	On
MaxInstanceConnection	4
ForwardAccoReqForUnknownUser	Off
AuthenticationProxyModeEnable	On
AuthenticationResponseTimeout	4
SessionWatchdogPeriod	0
DefaultSessionTimeout	0

AaaSystemAccountingServers

Attribute	Value
EncryptedSharedSecret	Provisioned
IsPrimaryServer	Off
AccountingServerIPAddress	192.168.60.55
AccountingServerPort	1813

AaaNetworkAccessServers

Netmask	EncryptedSharedSecret	NASIdentifier	NASPort	NASIPAddress	AAAListenIPAddress	AAAListenPort	VSADisconnect	ImmediateIPAddressRelease	SupportMultipleContexts	Action
255.255.255.0	Provisioned		-1	192.168.10.126	192.168.10.127	1812	DONT_SEND	Off	Off	Delete
255.255.255.0	Provisioned		1	192.168.10.127	192.168.10.128	1812	DONT_SEND	On	On	Delete

AaaNasAccountingServers

Attribute	Value
EncryptedSharedSecret	Provisioned
IsPrimaryServer	Off
AccountingServerIPAddress	192.168.60.51
AccountingServerPort	1813
NASIPAddress	192.168.60.51

AaaSystemAuthenticationServers

RealmOrCalledStation	EncryptedSharedSecret	AssociationType	AuthenticationServerIPAddress	AuthenticationServerPort	Action
blueslice.ca	Provisioned	REALM	192.168.60.51	1812	Delete
5143334444	Provisioned	CALLED_STATION_ID	192.168.60.51	1812	Delete
5145551111	Provisioned	CALLED_STATION_ID	192.168.60.51	1812	Delete

AaaNASAuthenticationServers

RealmOrCalledStation	EncryptedSharedSecret	AssociationType	NASIPAddress	AuthenticationServerIPAddress	AuthenticationServerPort	Action
blueslice.com	Provisioned	REALM	192.168.60.51	192.168.60.51	1812	Delete
5141112222	Provisioned	CALLED_STATION_ID	192.168.60.51	192.168.60.51	1812	Delete

Figure 76: AAA Configuration Window

AAA Provisioning Configuration – Provisioning AAA Address Allocation Policies and IP Address Pools

The AAA server allocates IP addresses or DHCP addresses to users at Authentication, depending on the allocation policy type configured for the address allocation policy that is selected by the AAA after comparison of the data retrieved from the Access-Request RADIUS messages with the following data configured in the AAA and associated to address allocation policies:

- A SGSN address
- A combination of a SGSN address and Called Station ID
- A realm
- A Called StationID
- A NAS Identifier

For more details on the allocation of IP addresses/DHCP addresses, refer to the "AAA Address Allocation" section in the *SDM Product Description* document.

By default, the AAA server provides dynamic address allocations to users upon reception of Access-Request messages. However, the AAA's address allocation functionality can also be done statically, by allowing the Network Operator to provision a AAA user with static IP addresses for a specific Called Station (APN) or Realm. Moreover, if desired, a static IP address can also be assigned to a Calling Station (MSISDN). This allows the operator to assign an IP address per Calling Station (MSISDN) for a specific Called Station (APN). This can be achieved by executing the AssignIPAddress() operation. The ReleaseIPAddress() operation is also available to allow the Network Operator to release a static IP Address. For more details on these two operations, refer to the "AAA Operations" section of the *SDM System Configuration – Reference Manual* . For instructions on how to execute these operations from the WebCI, refer to the "Viewing/Editing AAA Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

To configure the AAA's dynamic address allocation functionality, the operator must provision the following tables in the order presented below. These tables can be found in the WebCI's AAA Provisioning Configuration window, which can be opened by extending the AAA folder from the WebCI's menu.

1. Provision the AAAAddressAllocationPolicy table in order to define Address Allocation Policies:
   a) Allocation Policy Name
   b) Allocation Policy Type:

      - ADDRESS_POOL: The AAA allocates an IP address by sending it back in the Access-Accept message. An allocation policy of this type is an IP address pool, for which IP address ranges must be provisioned. In this case, step 2 must be followed.
      - DHCP_IDENT: The AAA sends back a DHCP address instead of an IP address in the Access-Accept message.
      - NO_IP_ALLOC: The AAA doesn't allocate an IP address.

   c) Use Full Address Pool (On/Off): this indicates whether or not the AAA must continuously re-use evenly the whole IP address range or not for this address allocation policy, in order to achieve even allocation of IP Addresses.

      For more details on this, refer to the "Even allocation of IP Addresses" section in the *SDM Product Description* document.

   d) Audit Logging Enabled (On/Off): The AAA can generate logs each time it allocates and de-allocates IP addresses for selected address pools.

      The AuditLoggingEnabled parameter allows the Network Operator to enable/disable the generation of audit loggings. These logs are stored in audit files, which can be managed and configured by the Network Operator through the CLI or WebCI. For instructions on how to manage audit files, refer to the "Configuring and Enabling/Disabling Audit logging" in the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

2. Provision the AAAAddressAllocationRanges table in order to define IP Address ranges for each IP address pool defined (address allocation policy defined with Allocation Policy Type: 'ADDRESS_POOL').

   Note that it is possible to have many range entries for an IP address pool. IP Address ranges only need to be defined for address allocation policies of type 'ADDRESS_POOL' and the WebCI rejects the provisioning of IP Address ranges for address allocation policies of any other type (NO_IP_ALLOC and DHCP_IDENT).

3. Provision the AAAAddressAllocationAssociation table in order to associate each address allocation policy to one of the following association value and type:

Table 22: Association types

Association value	Auxiliary value	Association Type
<SGSN address>	--------------------------	SGSN Address
<SGSN address>	<Called Station Id>	SGSN and Called Station
<Realm>	--------------------------	REALM
<Called-Station_id>	--------------------------	CALLED_STATION-ID
<NAS Identifier>	--------------------------	NAS Identifier
-------------------------------------	--------------------------	SYSTEM

One entry must absolutely be provisioned to associate an address allocation policy with the default AssociationType 'SYSTEM'. The address allocation policy associated to this association type is the default allocation policy.

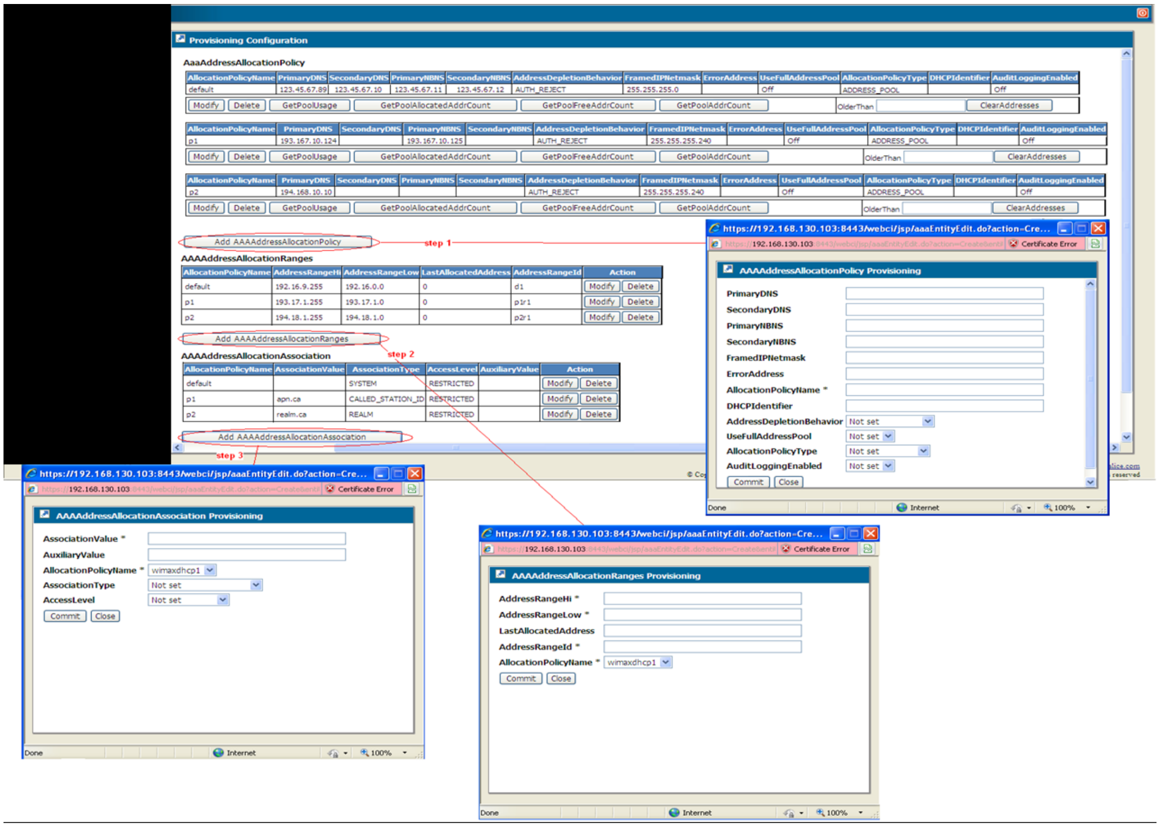
In order to make an address allocation policy selection, the AAA compares the data received in the Access-Request with the association values defined in this table. When a match is found, the AAA uses the address allocation policy associated to the matching association value.

When a match is not found, the AAA uses the address allocation policy that is associated to the AssociationType: 'SYSTEM'.

Note: An allocation policy may be associated with one or more Called Station Ids or one or more Realms but may not be associated with a combination of Realms and Called Station Ids.

Provisioning this table also allows you to associate each address allocation policy with an Access Level, which indicates whether the address allocation policy can only be used for users who pass authentication or whether it can be used for users who don't pass authentication. For more details on this, refer to the "Extension to handle Restricted Access for Unauthorized Users" section of the *SDM Product Description* .

For more information on the tables to be provisioned and their parameter values, refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual* .



Provisioning Configuration

AaaAddressAllocationPolicy

AllocationPolicyName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPIdentifier	AuditLoggingEnabled
default	123.45.67.89	123.45.67.10	123.45.67.11	123.45.67.12	AUTH_REJECT	255.255.255.0		Off	ADDRESS_POOL		Off

AllocationPolicyName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPIdentifier	AuditLoggingEnabled
p1	193.167.10.124		193.167.10.125		AUTH_REJECT	255.255.255.240		Off	ADDRESS_POOL		Off

AllocationPolicyName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPIdentifier	AuditLoggingEnabled
p2	194.168.10.10				AUTH_REJECT	255.255.255.240		Off	ADDRESS_POOL		Off

AAAAddressAllocationRanges

AllocationPolicyName	AddressRangeHi	AddressRangeLow	LastAllocatedAddress	AddressRangeId	Action
default	192.16.9.255	192.16.0.0	0	d1	Modify Delete
p1	193.17.1.255	193.17.1.0	0	p1r1	Modify Delete
p2	194.18.1.255	194.18.1.0	0	p2r1	Modify Delete

AAAAddressAllocationAssociation

AllocationPolicyName	AssociationValue	AssociationType	AccessLevel	AuxiliaryValue	Action
default		SYSTEM	RESTRICTED		Modify Delete
p1	apn.ca	CALLED_STATION_ID	RESTRICTED		Modify Delete
p2	realm.ca	REALM	RESTRICTED		Modify Delete

https://192.168.130.103:8443/webci/jsp/aaaEntityEdit.do?action=Cre...

AAAAddressAllocationPolicy Provisioning

PrimaryDNS	
SecondaryDNS	
PrimaryNBNS	
SecondaryNBNS	
FramedIPNetmask	
ErrorAddress	
AllocationPolicyName *	
DHCPIdentifier	
AddressDepletionBehavior	Not set
UseFullAddressPool	Not set
AllocationPolicyType	Not set
AuditLoggingEnabled	Not set

https://192.168.130.103:8443/webci/jsp/aaaEntityEdit.do?action=Cre...

AAAAddressAllocationAssociation Provisioning

AssociationValue *	
AuxiliaryValue	
AllocationPolicyName *	wimaxdhcp1
AssociationType	Not set
AccessLevel	Not set

https://192.168.130.103:8443/webci/jsp/aaaEntityEdit.do?action=Cre...

AAAAddressAllocationRanges Provisioning

AddressRangeHi *	
AddressRangeLow *	
LastAllocatedAddress	
AddressRangeId *	
AllocationPolicyName *	wimaxdhcp1

Figure 77: Provisioning Address Allocation Policies

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

In addition to provisioning the Address Allocation Policies, the following operations are also available:

Delete/Modify. The following table's entries can be deleted or modified one entry at a time:

a) AaaAddressAllocationPolicy

b) AaaAddressAllocationRanges

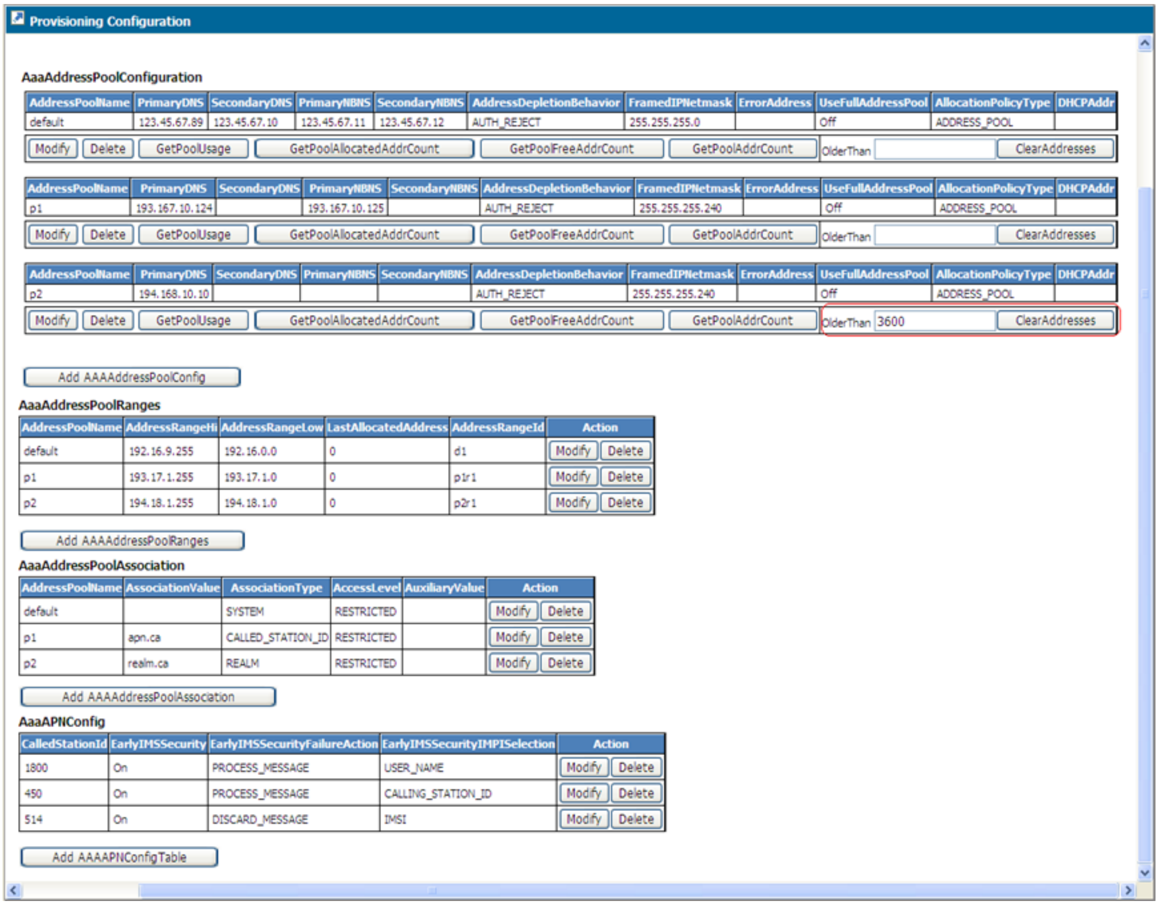
c) AaaAddressAllocationAssociation

ClearAddresses. The ClearAddresses operation allows to manually reset (de-allocate) some or all the IP addresses, within a specific address allocation policy, that have been allocated to subscribers.

This operation can be executed for each AAA Address Allocation Policy entry with 'AllocationPolicyType=ADDRESS_POOL' in the AaaAddressAllocationPolicy table.

When executing this operation, the following field must be populated:

OlderThan: age in seconds. The allocations that have been made before <age> seconds ago will be reset. Setting <age> to 0 will clear all IP addresses.



Provisioning Configuration

AaaAddressPoolConfiguration

AddressPoolName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPAddr
default	123.45.67.89	123.45.67.10	123.45.67.11	123.45.67.12	AUTH_REJECT	255.255.255.0		Off	ADDRESS_POOL	

OlderThan

AddressPoolName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPAddr
p1	193.167.10.124		193.167.10.125		AUTH_REJECT	255.255.255.240		Off	ADDRESS_POOL	

OlderThan

AddressPoolName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPAddr
p2	194.168.10.10				AUTH_REJECT	255.255.255.240		Off	ADDRESS_POOL	

OlderThan 3600

AaaAddressPoolRanges

AddressPoolName	AddressRangeHi	AddressRangeLow	LastAllocatedAddress	AddressRangeId	Action
default	192.16.9.255	192.16.0.0	0	d1	Modify Delete
p1	193.17.1.255	193.17.1.0	0	p1r1	Modify Delete
p2	194.18.1.255	194.18.1.0	0	p2r1	Modify Delete

AaaAddressPoolAssociation

AddressPoolName	AssociationValue	AssociationType	AccessLevel	AuxiliaryValue	Action
default		SYSTEM	RESTRICTED		Modify Delete
p1	apn.ca	CALLED_STATION_ID	RESTRICTED		Modify Delete
p2	realm.ca	REALM	RESTRICTED		Modify Delete

AaaAPNConfig

CalledStationId	EarlyIMSSecurity	EarlyIMSSecurityFailureAction	EarlyIMSSecurityIMPISelection	Action
1800	On	PROCESS_MESSAGE	USER_NAME	Modify Delete
450	On	PROCESS_MESSAGE	CALLING_STATION_ID	Modify Delete
514	On	DISCARD_MESSAGE	IMSI	Modify Delete

Figure 78: Clear IP Addresses

Example:

In the figure above, when performing the following for the AAA Allocation Policy Name: p2:

d) entering the value '3600' for the OlderThan parameter

e) clicking on the ClearAddresses button

the AAA will reset (de-allocate) all of this AAA Allocation Policy's (p2) IP addresses that have been allocated before 3600 seconds ago.

Disabling the AAA Address Allocation:

If you wish to disable the AAA Address Allocation, simply provision the AAAAddressAllocationPolicy table's AllocationPolicyType parameter with the 'NoIP' value. In this case, the AAA will not allocate any addresses whether the allocation is done dynamically or statically by the Network Operator.

Chapter 9

DNS Enum server configuration

Topics:

This chapter describes the configuration of the DNS Enum server.

DNS ENUM Server Configuration

The DNS ENUM Server is usually configured at installation by Tekelec's *Customer Care Center* when the functionality has already been purchased. The following information needs to be configured to run the DNS ENUM Server:

- The maximum number of users that can be provisioned per Subscription (SubscriptionID).
- On/Off flags to enable/disable the feature that supports the ENUM Server.
- The DNS ENUM Listen Address and Port.
- The Domain Name List configuration.

  The operator can view all of this configuration information from the WebCI's ENUM Server folder, by opening the ENUM Server Configuration window and the Provisioning Configuration window. Some of this information can be modified and even added and deleted.

Important: Take note that prior to changing the activation status of the ENUM Server functionality (enable/disable) during running-time, the HSS service must first be stopped. Once the changes are made, the HSS service can be started once again. This will affect traffic, so make sure to perform this during low traffic periods.

To view, edit, add or delete some DNS ENUM Server configuration parameters, you must access the following windows:

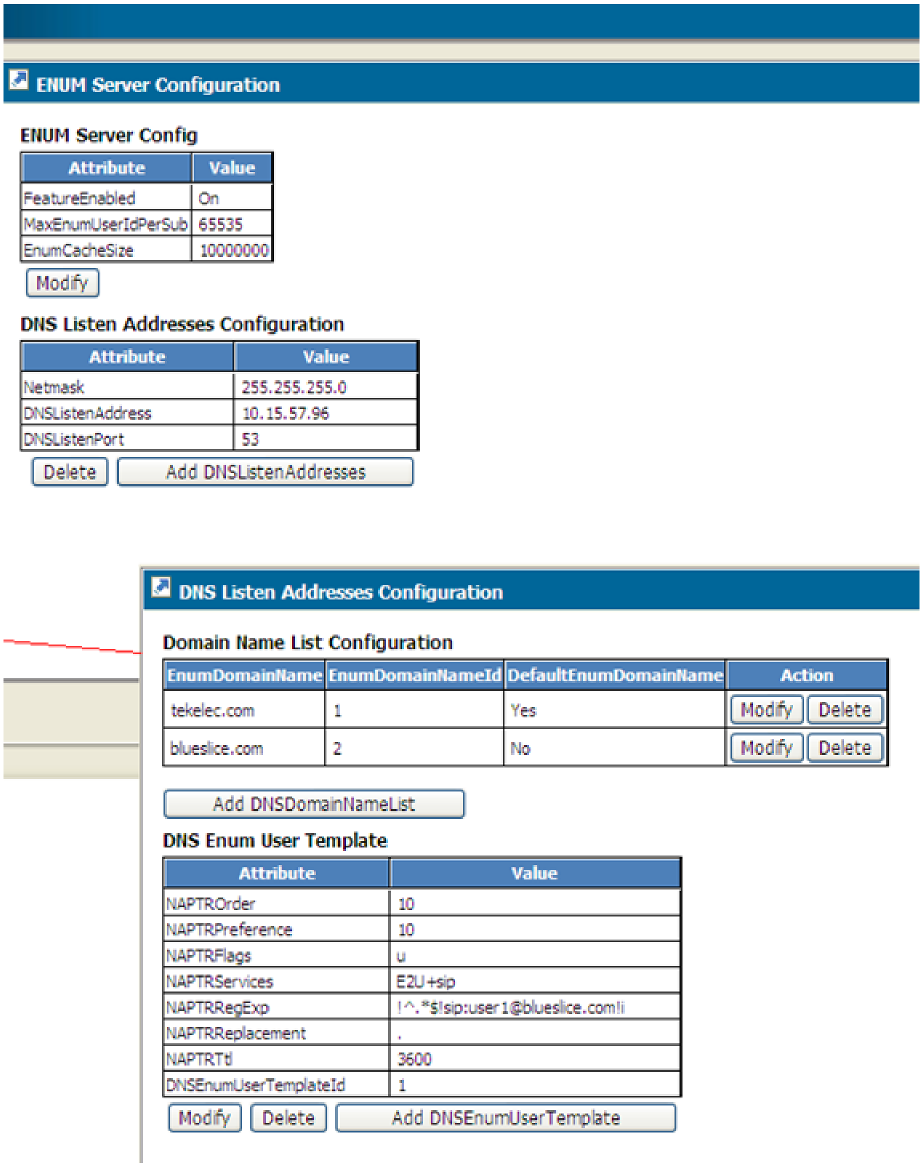
- ENUM Server Configuration window, which displays the ENUM Server configuration table and the DNS Listen Addresses Configuration table.
- The Provisioning Configuration window, which displays the Domain Name List Configuration table and the DNS ENUM User Template table. The DNSEnumUserTemplate table allows to define templates that can be used by multiple ENUM profiles. Each ENUM profile can be provisioned to refer to a template defined in this table.

  These windows can be accessed by extending the ENUM Server folder in the WebCI's menu.

  For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in this document.

  For more details on the parameters of each one of these windows, refer to the “ENUM” chapter of the *SDM System Configuration – Reference Manual*.

  Once the DNS ENUM Server has been configured properly, ENUM Users can be provisioned in the system. To achieve this from the WebCI, refer to the “Viewing/Editing DNS ENUM Users” section of the *SDM Monitoring, Maintenance, Troubleshooting – User Guide* document. To provision DNS ENUM Users in bulk, refer to the IMS-HSS Subscriber provisioning XML scripts in the *SDM Subscriber Provisioning – User Guide.*



ENUM Server Config

Attribute	Value
FeatureEnabled	On
MaxEnumUserIdPerSub	65535
EnumCacheSize	10000000

DNS Listen Addresses Configuration

Attribute	Value
Netmask	255.255.255.0
DNSListenAddress	10.15.57.96
DNSListenPort	53

Domain Name List Configuration

EnumDomainName	EnumDomainNameId	DefaultEnumDomainName	Action
tekelec.com	1	Yes	Modify Delete
blueslice.com	2	No	Modify Delete

DNS Enum User Template

Attribute	Value
NAPTROrder	10
NAPTRPreference	10
NAPTRFlags	u
NAPTRServices	E2U+sip
NAPTRRegExp	!^.*$!sip:user1@blueslice.com!i
NAPTRReplacement	.
NAPTRTtl	3600
DNSEnumUserTemplateId	1

Figure 79: Configuring The DNS ENUM Server

Chapter 10

HSS/AAA Support for Early IMS Security Configuration

Topics:

This chapter describes the configuration of the HSS/AAA Support for Early IMS Security.

Introduction

The Tekelec HSS/AAA support the security mechanisms for early IMS implementations, as per the TR33.978 standard.

This means that upon receiving, from an Early-IMS Configured APN, a RADIUS Accounting Request START message, the HSS/AAA can send back to the GGSN an Accounting-Response. For more details on the SDM's behavior when receiving messages from the Early IMS APN, refer to the "HSS/AAA Support for IMS Security" section in the *SDM Product Description* .

In order to configure the HSS/AAA's Early IMS Security capability, the Network Operator must provision the AaaAPNConfig table, by opening the AAA Provisioning Configuration window from the WebCI's AAA folder.

The AaaAPNConfig table allows the operator to configure the following for a Called Station ID:

- Set the Early IMS Security feature ON/OFF. By default, it is set to 'Off'.
- Select the action the AAA must take in case of Early IMS Security failure.
- Set the attribute (CallingStationId, IMSI, User Name) for which the HSS must find an IMPI that matches.

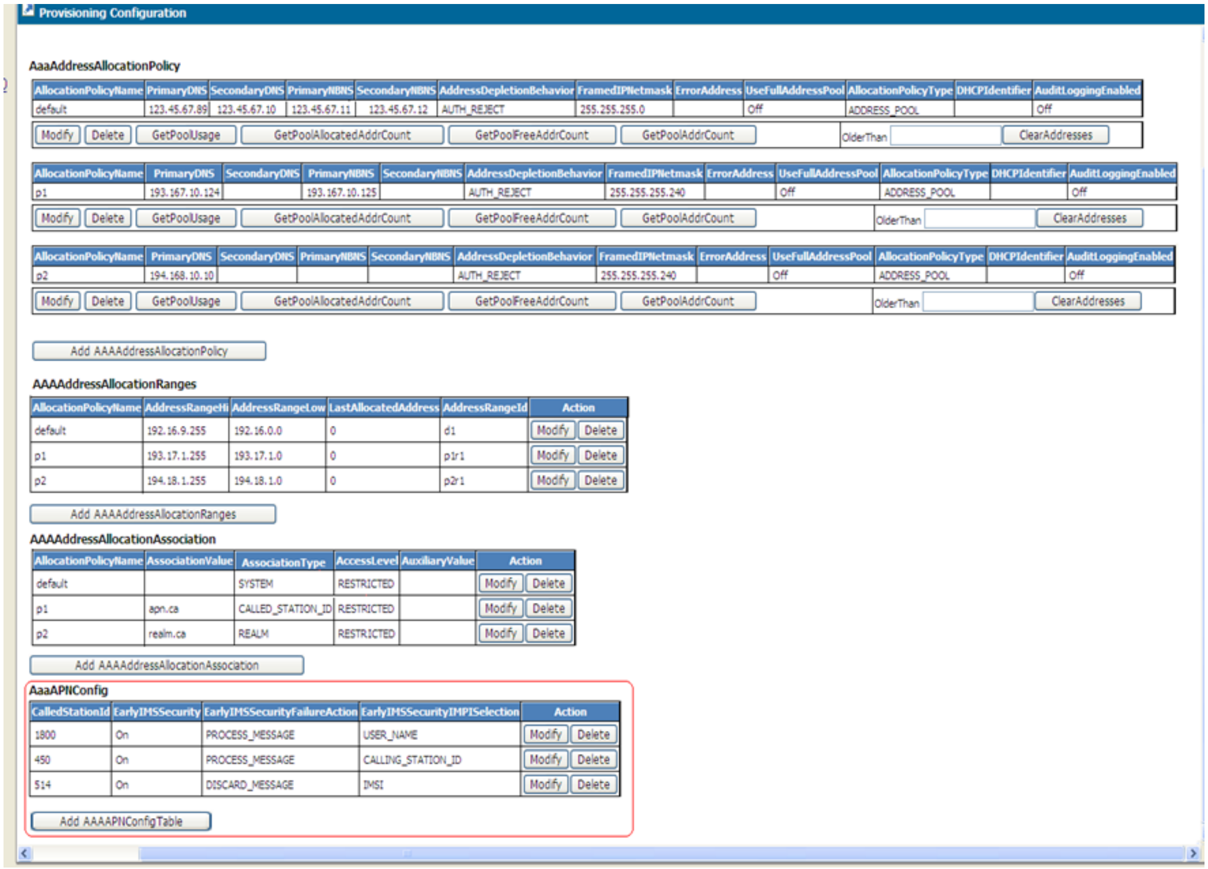
  For more details on the AaaAPNConfig table's attributes and their values, refer to the "AAA Provisioning Configuration" section in the *SDM System Configuration - Reference Manual* .

  In addition, the Network Operator must provision the Private Identities (IMPIs), for which the AAA may receive messages from the Early IMS Network, with the following values:

- 'Early-IMS-Security' value for the AlgoName parameter
- 'On' value for the Early-IMS-Security flag

  For instructions on how to provision a HSS Private Identity (IMPI), refer to the "Viewing/Editing HSS Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

  The figure hereunder shows the AaaAPNConfig table from the WebCI.


Provisioning Configuration
Modify
Delete
GetPoolUsage
GetPoolAllocatedAddrCount
GetPoolFreeAddrCount
GetPoolAddrCount
OlderThan
ClearAddresses
Add AAAAddressAllocationPolicy
Add AAAAddressAllocationRanges
Add AAAAddressAllocationAssociation
Add AAAAPNConfigTable

AaaAddressAllocationPolicy

AllocationPolicyName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPIdentifier	AuditLoggingEnabled
default	123.45.67.89	123.45.67.10	123.45.67.11	123.45.67.12	AUTH_REJECT	255.255.255.0		Off	ADDRESS_POOL		Off

AllocationPolicyName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPIdentifier	AuditLoggingEnabled
p1	193.167.10.124		193.167.10.125		AUTH_REJECT	255.255.255.240		Off	ADDRESS_POOL		Off

AllocationPolicyName	PrimaryDNS	SecondaryDNS	PrimaryNBNS	SecondaryNBNS	AddressDepletionBehavior	FramedIPNetmask	ErrorAddress	UseFullAddressPool	AllocationPolicyType	DHCPIdentifier	AuditLoggingEnabled
p2	194.168.10.10				AUTH_REJECT	255.255.255.240		Off	ADDRESS_POOL		Off

AAAAddressAllocationRanges

AllocationPolicyName	AddressRangeHi	AddressRangeLow	LastAllocatedAddress	AddressRangeId	Action
default	192.16.9.255	192.16.0.0	0	d1	Modify Delete
p1	193.17.1.255	193.17.1.0	0	p1r1	Modify Delete
p2	194.18.1.255	194.18.1.0	0	p2r1	Modify Delete

AAAAddressAllocationAssociation

AllocationPolicyName	AssociationValue	AssociationType	AccessLevel	AuxiliaryValue	Action
default		SYSTEM	RESTRICTED		Modify Delete
p1	apn.ca	CALLED_STATION_ID	RESTRICTED		Modify Delete
p2	realm.ca	REALM	RESTRICTED		Modify Delete

AaaAPNConfig

CalledStationId	EarlyIMSSecurity	EarlyIMSSecurityFailureAction	EarlyIMSSecurityIMPISelection	Action
1800	On	PROCESS_MESSAGE	USER_NAME	Modify Delete
450	On	PROCESS_MESSAGE	CALLING_STATION_ID	Modify Delete
514	On	DISCARD_MESSAGE	IMSI	Modify Delete

Figure 80: Configuring The Early IMS Security

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

Other Operations

In addition to provisioning the AaaAPNConfig table with new entries, the following operations are also available:

Modify. This button allows to modify the AaaAPNConfig entry located in the same row as the Modify button clicked on.

Delete. This button allows to delete a AaaAPNConfig entry located in the same row as the Modify button clicked on.

Chapter 11

LTE-HSS Application Configuration

Topics:

This chapter outlines the procedures to configure the LTE-HSS.

Introduction

The procedures in this chapter show you how to view/add/modify the LTE-HSS configuration, and configure the HSS PLMN for roaming purposes. To perform the tasks in the following table, refer to the corresponding section within this chapter.

Table 23: LTE-HSS Configuration Tasks

Task
Viewing/Editing LTE HSS Configuration
Configuring the LTE HSS PLMN
Configuring the LTE HSS GMLC Node List
Configuring the LTE HSS Realms

Requirements: Log in to a WebCI session with a username and password.

For details on the parameters used to configure the LTE-HSS, HSS PLMN, GMLC Node List and LTE-HSS Realms refer to the “LTE-HSS” section in the *SDM System Configuration - Reference Manual* .

Configuring the LTE-HSS

The LTE-HSS is usually configured at installation by Tekelec’s *Customer Care Center*.

The following information needs to be configured at installation in order to run the LTE-HSS application:

1. LTE-HSS configuration information.

   The LTE-HSS configuration data can be displayed/edited from the WebCI, as described below.

2. The network information (Local FQDN, LocalSTCPPort, LocalTCPPort, OriginatingRealm, SCTPTransport, TCPTransport, TCP Listen Address, SCTP Listen Address, Destination Realms, Destination Hosts, etc.) needed for the LTE-HSS to communicate with the peer servers.

   The LTE-HSS network configuration data can be displayed/edited/added from the WebCI, as described below.

Viewing/Editing LTE-HSS Configuration

The operator can view all of the HSS configuration information from the WebCI’s LTEHSS folder, by opening the LTEHSS Configuration window. Some of this information can be modified and network information can be deleted/added.

Important: Prior to making any changes (modifying) to the LTE-HSS Options data during running-time, the LTE-HSS service must first be stopped. Once the changes are made, the LTE-HSS service can be started once again. This will affect traffic, so make sure to perform this during down time if necessary. Refer to section "Starting and Stopping Services on a blade" of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for more information on how to stop a service.

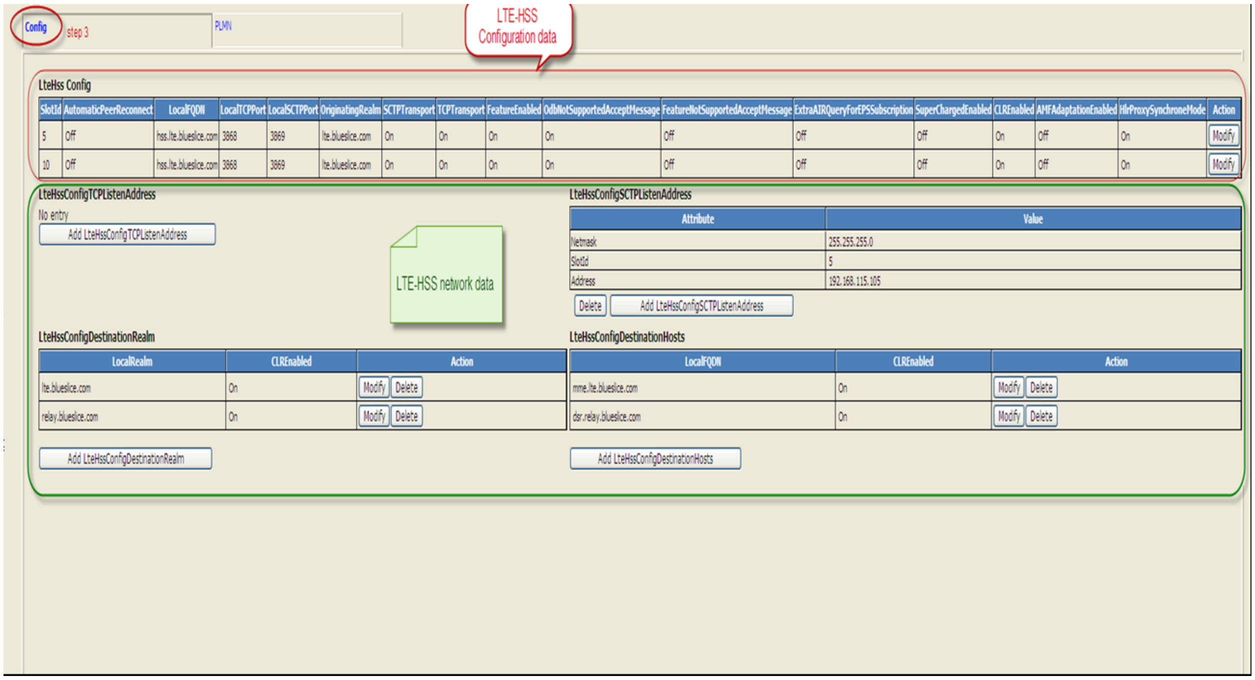
The LteHss Config table can be edited, by clicking on the **Modify** button located in the same row as the entry you wish to edit.

In order to edit the network information, if there is no Modify button available, you must delete the entry by clicking on the Delete button located in the same row as the entry you wish to modify and re-create it by clicking on the Add button.

Further network information can be configured in the other tables (LteHssConfigTCPListenAddress, LteHssConfigSCTPListenAddress, LteHssConfigDestinationRealm, LteHssConfigDestinationHosts) displayed in the LTEHSS Configuration window.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

For details on the LTE-HSS configuration parameters, refer to the "LTE-HSS Entities" section in the *SDM System Configuration - Reference Manual* .



LteHss Config

SlotId	AutomaticPeerReconnect	LocalFQDN	LocalTCPPort	LocalSCTPPort	OriginatingRealm	SCTPTransport	TCPTransport	FeatureEnabled	OdbNotSupportedAcceptMessage	FeatureNotSupportedAcceptMessage	ExtraAIRQueryForEPSSubscription	SuperChargedEnabled	CLREnabled	AMFAdaptationEnabled	HlrProxySynchroneMode	Action
5	Off	hss.lte.blueslice.com	3868	3869	lte.blueslice.com	On	On	On	On	Off	Off	Off	On	Off	On	Modify
10	Off	hss.lte.blueslice.com	3868	3869	lte.blueslice.com	On	On	On	On	Off	Off	Off	On	Off	On	Modify

LteHssConfigTCPListenAddress

No entry

Add LteHssConfigTCPListenAddress

LteHssConfigSCTPListenAddress

Attribute	Value
Netmask	255.255.255.0
SlotId	5
Address	192.168.115.105

Delete Add LteHssConfigSCTPListenAddress

LteHssConfigDestinationRealm

LocalRealm	CLREnabled	Action
lte.blueslice.com	On	Modify Delete
relay.blueslice.com	On	Modify Delete

Add LteHssConfigDestinationRealm

LteHssConfigDestinationHosts

LocalFQDN	CLREnabled	Action
mme.lte.blueslice.com	On	Modify Delete
dsr.relay.blueslice.com	On	Modify Delete

Add LteHssConfigDestinationHosts

Figure 81: LTE-HSS Configuration Window

Once the LTE-HSS has been configured, you can provision LTE-HSS users (by first provisioning PDN context templates and then the PDN context data from the SDM's HLR Subscriber Profile). For information on how to configure PDN Context Templates, refer to *Provisioning PDN Context Templates* in this document. You can provision LTE-HSS users in bulk using XML files, for instructions on this, refer to the *SDM Subscriber Provisioning –User Guide* . If you wish to view/edit/provision LTE-HSS users from the WebCI, refer to the "Viewing/Editing LTE-HSS Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* .

Configuring the LTE HSS PLMN

PLMNs must be defined for the LTE-HSS, by defining in the HSSPLMN[ ] entity the Mobile Country Codes and Mobile Network Codes for a range of IMSIs. This is used by the LTE-HSS in case of roaming, in order to determine whether the subscriber is allowed to roam or not based on its location (PLMN).

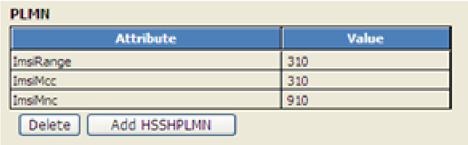
From the WebCI, the PLMNs can be defined for the LTE-HSS, by provisioning the PLMN table located in the LTEHSS Configuration window's PLMN tab.

Simply click on the **Add HSSPLMN** button (located below the PLMN table) in order to create a new entry with a MCC and MNC for a specific IMSI range.

In order to edit a PLMN entry, you must delete the entry by clicking on the Delete button located in the same row as the entry you wish to modify and re-create it by clicking on the Add HSSPLMN button.

For details on the LTE-HSS PLMN parameters, refer to the "LTE-HSS Entities" section in the *SDM System Configuration - Reference Manual* .

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



PLMN

Attribute	Value
ImsiRange	310
ImsiMcc	310
ImsiMnc	910

Figure 82: LTE-HSS PLMN Definitions

Configuring the LTE-HSS GMLC Node List

GMLC nodes must be defined for the LTE-HSS, by defining the GmlcNodeList[ ] entity. When the LTE-HSS receives an LCS Routing Information Request (RIR) from the GMLC it contains either an IMSI or a MSISDN as well as a GMLC number.

The GMLC number is validated against the GMLC Node List to ensure it belongs to a network that is authorized to request User Equipment (UE) information.

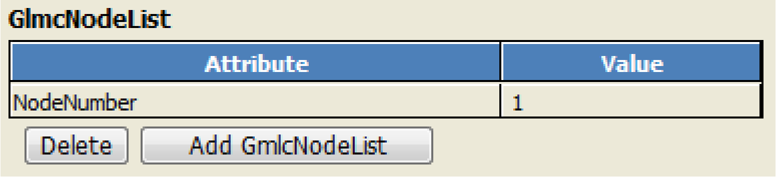
From the WebCI, the GMLC nodes can be defined for the LTE-HSS, by provisioning the GMLCNodeList table located in the LTE-HSS Configuration window's GMLCNodeList tab.

Click on the **Add GmlcNodeList** button in order to create a new Node Number entry.

In order to edit a GmlcNodeList entry, you must delete the entry by clicking on the Delete button located in the same row as the entry you wish to modify and re-create it by clicking on the Add GmlcNodeList button.

For details on the LTE-HSS GmlcNodeList parameters, refer to the “LTE-HSS" section in the *SDM System Configuration - Reference Manual* .

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



GlmcNodeList

Attribute	Value
NodeNumber	1

Figure 83: Gmlc Node List Definitions

Configuring the LTE-HSS Realms

Realms must be defined for the LTE-HSS, by defining the LteHssRealms[ ] entity, host and realm for a range of IMSIs. Each IMSI range is associated with a specific host and realm value. It is used when the LTE-HSS receives a diameter request message from a node in another network and needs to determine the host and realm values to send in the response. It is also used when the LTE-HSS initiates a request message.

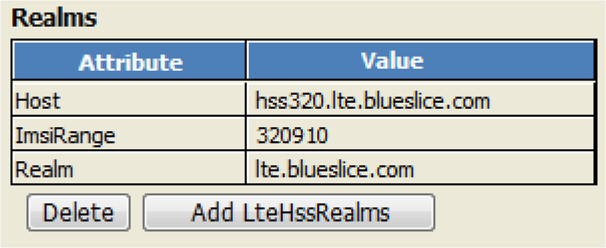
From the WebCI, Realms can be defined for the LTE-HSS, by provisioning the Realms table located in the LTE-HSS Configuration window’s Realms tab.

Click on the **Add LteHssRealms** button (located below the Realms table) in order to create a new entry with a host and a realm for a specific IMSI range.

In order to edit a Realms entry, you must delete the entry by clicking on the Delete button located in the same row as the entry you wish to modify and re-create it by clicking on the Add LteHssRealms button.

For details on the LTE-HSS Realms parameters, refer to the “LTE-HSS” section in the *SDM System Configuration - Reference Manual* .

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).



Realms

Attribute	Value
Host	hss320.lte.blueslice.com
ImsiRange	320910
Realm	lte.blueslice.com

Figure 84: LTE-HSS Realms Definitions

Introduction to LTE-HSS System Features

The procedures in this chapter describes how to view and modify the LTE-HSS System Features, and configure the LTE-HSS options for LTE-HSS logging.

It also describes how to view and modify the support for multiple realms feature.

Requirements: Log in to a WebCI session with a username and password.

For details on the parameters used to configure the LTE-HSS options, refer to the “LTE-HSS Options” section in the *SDM System Configuration - Reference Manual* .

Viewing/Editing LTE-HSS Options

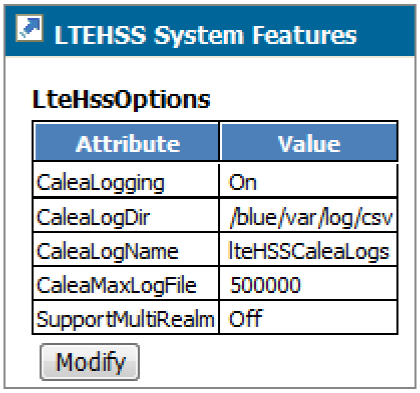
The operator can view all of the LTE-HSS Options information from the WebCI’s LTE-HSS System Features folder, by opening the LteHssOptions window. All of this information can be viewed and modified.

Important: Prior to making any changes (modifying) to the LTE-HSS Options data during running-time, the LTE-HSS service must first be stopped. Once the changes are made, the LTE-HSS service can be started once again. This will affect traffic, so make sure to perform this during down time if necessary. Refer to section “Starting and Stopping Services on a blade” of the *SDM Monitoring, Maintaining, Troubleshooting – User Guide* for more information on how to stop a service.

The LteHssOptions table can be edited, by clicking on the **Modify** button located under the table.

For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)* in both this document and the *SDM System Configuration – Reference Manual* document (this document gives more details on these tables and each of their parameters and values supported).

For details on the LTE-HSS Options parameters, refer to the “LTE-HSS System Features” section in the *SDM System Configuration - Reference Manual* .



LTEHSS System Features

LteHssOptions

Attribute	Value
CaleaLogging	On
CaleaLogDir	/blue/var/log/csv
CaleaLogName	lteHSSCaleaLogs
CaleaMaxLogFile	500000
SupportMultiRealm	Off

Figure 85: LTE-HSS System Features, LTE-HSS Options

LTE-HSS Logging is activated and deactivated dynamically in the LteHssOptions table using the CaleaLogging attribute. When modifying the LTE-HSS log directory name, log file name and the maximum number of lines in the log file, the LTE-HSS service must be stopped and restarted.

The multiple realms feature is activated and deactivated dynamically in the LteHssOptions table using the SupportMultiRealm attribute.

For details on the LTE-HSS Realms parameters, refer to the "LTE-HSS Realms" section in the *System Configuration - Reference Manual*.

Configure Diameter Relay Agent

Use this procedure to configure the LTE-HSS for Diameter Relay Agent support. This procedure established a static route to allow the LTE-HSS to send and receive Diameter far-end messages coming through the Diameter Relay Agent.

1. Go to **Diameter>DRA Configuration>DRAConfig**.
2. Click **Add DRAconfig**.
3. Enter the Diameter host name of the Diameter Relay Agent that will connect to the HSS.
4. Enter the Diameter host realm of the Diameter Relay Agent that will connect to the HSS.
5. Click **Commit**.
6. Go to **HSS>HSS Configuration**.

   Note: If the following two tables are left empty, the SDM allows any connection from a Diameter peer.

7. Click **Add** or **Modify HSSConfigDestinationHost.**
8. Enter the name of the HSS node (LocalFQDN) and click Commit
9. Click **Add** or **Modify HSSConfigDestinationRealm**.
10. Enter the name of the domain to which the HSS belongs (LocalFQDN) and click Commit.

Chapter 12

EIR Application Configuration

Topics:

This chapter provides the procedures to configure the Equipment Identity Register (EIR) through the WebCI.

Introduction

Note: Some configurations require the stop of all processes on the blade and a restart of the blade to implement the changes. Read the procedure carefully prior to starting the configuration.

- For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)*
- To stop and restart a process, refer to section "Starting and Stopping Services on a blade" in the *SDM Monitoring, Maintaining, Troubleshooting User Guide*.
- For table descriptions, configuration values, rules, and all other operations, refer to the indicated entity table in the *SDM System Configuration Reference Manual*.

Configure EIR for ECR Message Processing

Use this procedure for set up EIR for ECR Message Processing.

1. Stop the LTE-HSS service that is running on the same blade as the EIR service before configuring the EirGlobalConfig table. Refer to the "Stop/Start one single service on a blade" procedure in the *SDM Monitoring, Maintaining, Troubleshooting User Guide*.
2. Configure global EIR settings to define the common EIR configuration that will be used by all EIR applications belonging to the same platform.
3. Restart the LTE-HSS service. Refer to the "Stop/Start one single service on a blade" procedure in the *SDM Monitoring, Maintaining, Troubleshooting User Guide*.
4. Configure EIR response types to define which equipment status will be returned in the MECheck-Identity answer if an IMEI has been configured in more than one list (White/Grey/Black).
5. Configure EIR IMEI equipment status to define new unbound IMEIs and to associate them with their equipment status. Use this procedure also to modify an IMEI‘s equipment status or software version, or to delete an IMEI from the EirImeiEquipStatus table.
6. Create unbound IMEI/IMSI association to associate an unbound mobile equipment IMEI (from the EirImeiEquipStatus table) with a subscriber‘s IMSI. This procedure can also associate several IMEIs to the same IMSI, and several IMSIs to the same IMEI.
7. Bind IMEI and IMEI/IMSI associations to a subscription to link other front-end profiles to the subscription.
8. Configure EIR IMEI equipment status to define new bound IMEIs and to associate them with their equipment status. Use this procedure also to modify a bound IMEI‘s equipment status or software version, or to delete a bound IMEI from the EirBoundImeiEquipStatus table.
9. Create bound IMEI/IMSI association to associate a bound mobile equipment IMEI (from the EirBoundImeiEquipStatus table) with a subscriber‘s IMSI. This procedure can also associate several bound IMEIs to the same IMSI, and several IMSIs to the same bound IMEI.
10. Create EIR IMEI range to define an IMEI range for an associated equipment status. The range can overlap with another range, which can have a different equipment status configuration.

Configure Global EIR Settings

Use this procedure to define the common EIR settings in The EirGlobalConfig table. These settings will be used by all EIR applications belonging to the same platform.

Requirements:

- The LTE-HSS service that is running on the same blade as the EIR service must be stopped prior to configuring the EirGlobalConfig table.
- The LTE-HSS service must be restarted before the EIR changes can take effect.
- For both procedures, refer to procedure Stop/Start one single service on a blade in the *Monitoring, Maintaining, Troubleshooting User Guide*
- The EirGlobalConfig table must have exactly one entry at service startup.

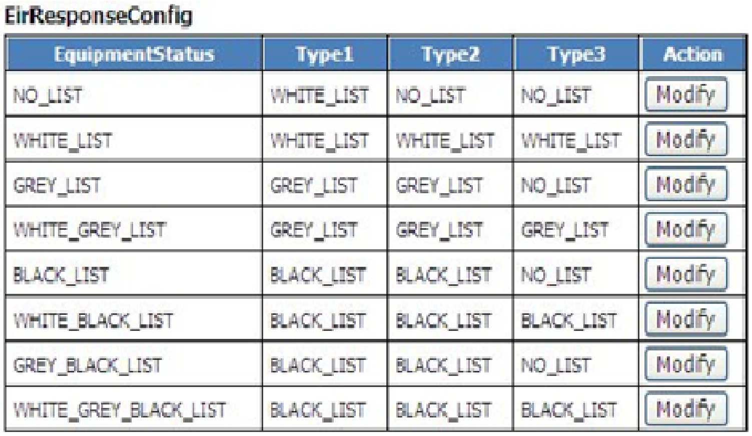
1. Go to **EIR>EIR Configuration>EirGlobalConfig**.
2. Click **Modify** in the EIRGlobalConfig table.
   The EirGlobalConfig Provisioning pop-up window opens.
3. Enter or select the information for each field:
   - Enter the system-wide default mobile network code (MNC)
   - Enter the system-wide default mobile country code (MCC)
   - Select the system-wide EIR response type to be returned for IMEIs that are on more than one list.
   - Select the global response option for searching IMEIs in the database as a response to an ME-Identity-Check-Request.
   - Turn on or off whether the IMSI shall be checked and the result to be included in an MECheck-Identity Answer.
   - Turn on or off whether an IMSI shall be dynamically created when an unknown IMEI associated with a non-blacklisted result is found.
4. Click **Commit**.

Configure EIR response types

Use this procedure to modify the response types, which will return a global ME-Check-Identity answer for unbound IMEIs that have been configured in more than one list, for example, in the white, grey, and black lists This table can be modified dynamically while the LTE-HSS service is running.

Note: The EquipmentStatus attribute of this table is predefined to exactly eight values, which are read at startup. If the EIR feature is turned on and this table does not contain exactly these eight values, the EIR process will not start.

1. Go to **EIR>EIR Configuration>EirResponseConfig**.
2. Click **Modify** button for the equipment status attribute to be modified.
   The EirResponseConfig Provisioning pop-up window opens.



EirResponseConfig

EquipmentStatus	Type1	Type2	Type3	Action
NO_LIST	WHITE_LIST	NO_LIST	NO_LIST	Modify
WHITE_LIST	WHITE_LIST	WHITE_LIST	WHITE_LIST	Modify
GREY_LIST	GREY_LIST	GREY_LIST	NO_LIST	Modify
WHITE_GREY_LIST	GREY_LIST	GREY_LIST	GREY_LIST	Modify
BLACK_LIST	BLACK_LIST	BLACK_LIST	NO_LIST	Modify
WHITE_BLACK_LIST	BLACK_LIST	BLACK_LIST	BLACK_LIST	Modify
GREY_BLACK_LIST	BLACK_LIST	BLACK_LIST	NO_LIST	Modify
WHITE_GREY_BLACK_LIST	BLACK_LIST	BLACK_LIST	BLACK_LIST	Modify

Figure 86: EirResponseConfig Provisioning Window

3. Select a different response type.
4. Click **Commit**.

Configure EIR IMEI Equipment Status

Use this feature to modify an IMEI's equipment status or software version, or to delete an IMEI from the EirImeiEquipStatus table

1. Go to **EIR>EIR Configuration>EirImeiEquipStatus**.
2. Update the EirImeiEquipStatus table:
   - Click **Modify** to select a different equipment status or change the software version.
   - Click **Add EirImeiEquipStatus** to add a new IMEI
   - Click **Delete** to remove an IMEI from the EirImeiEquipStatus table.

Create Unbound IMEI/IMSI Association

Use this procedure to associate an unbound IMEIs (from the EirImeiEquipStatus table) with a subscriber's IMSI. The table also allows to link several IMEIs to the same IMSI, and several IMSIs to the same IMEI.

1. Go to **EIR>EIR Configuration>EirImeiEquipStatus**.
2. Associate an IMEI to an IMSI:
   - Click the **Add EirImeiImsiAssociation** button of the IMEI to be associated with an IMSI.
   - Enter the new IMSI.
   - Click **Submit**
   - Repeat this step for each new association

3. Modify or delete an IMEI/IMSI association at EIR>EIR Configuration>EirImeiImsiAssociation
    - Click the **IMEI Modify** button to change the association; or
    - Click the **IMEI Delete** button to delete the association

Bind IMEI and IMEI/IMSI Associations to a Subscription

Use this procedure to bind an unbound IMEI or IMEI/IMSI associations to a subscription ID. The operator can then link another front-end profile to the subscription ID.

1. Go to **EIR>EIR Configuration>EirImeiEquipStatus**.
2. Enter the subscription ID to be associated with the IMEI.

    Note: The mandatory IMEI must have a subscription ID already assigned before other IMEIs can be bound.
3. Click **BindIMEI**

    This step creates a new entry in the EirBoundImeiEquipStatus table. The new entry includes the specified SubscriptionID and the data from the corresponding EirImeiEquipStatus entry (which is subsequently removed).

    In addition, all EirImeiImsiAssociation entries that have the given IMEI are moved to the EirBoundImeiImsiAssociation table.

    Note: If a SubscriptionID is removed from the SDM Subscription table, a cascade operation will result in the deletion of all EirBoundImeiEquipStatus entries that specify that SubscriptionID.

Configure EIR Bound IMEI Equipment Status

Use this feature to modify a bound IMEI's equipment status or software version, or to delete an IMEI from the EirBoundImeiEquipStatus table

1. Go to **SubscriptionID>EIR>display/modify>Add EirBoundImeiEquipStatus**.
2. Update the EirBoundImeiEquipStatus table:
    - Click **Modify** to select a different equipment status or change the software version.
    - Click **Add EirBoundImeiEquipStatus** to add a new bound IMEI.
    - Click **Delete** to remove a bound IMEI from the EirBoundImeiEquipStatus table.

Create Bound IMEI/IMSI Association

Use this procedure to associate a bound IMEI (from the EirBoundImeiEquipStatus table) with a subscriber's IMSI. The table also allows to link several IMEIs to the same IMSI, and several IMSIs to the same IMEI.

1. Go to **SubscriptionID>EIR>display/modify>Add EirBoundImeiEquipStatus**.
2. Associate a bound IMEI to an IMSI:
    1. Click the **Add EirBoundImeiImsiAssociation** button of the bound IMEI to be associated with an IMSI.
    2. Enter the new IMSI.
    3. Click **Commit**.
    4. Repeat this step for each new association
3. Modify or delete a bound IMEI/IMSI association at **SubscriptionID>EIR>display/modify>AddEirBoundImeiEquipStatus**.
    - Click the **IMEI Modify** button to change the association; or
    - Click the **IMEI Delete** button to delete the association

Create EIR IMEI Range

Use this procedure to associate a bound IMEI (from the EirBoundImeiEquipStatus table) with a subscriber's IMSI. The table also allows to link several IMEIs to the same IMSI, and several IMSIs to the same IMEI.

1. Go to **EIR>EIR Configuration>EirImeiRange**.
2. Click the EirIMEIRange button to define the Start IMEI, End IMEI, and equipment status for the range.
3. Click **Commit**.

Chapter 13

LTE-EIR Application Configuration

Topics:

This chapter provides the initial procedures on how to configure the LTE-EIR through the WebCI.

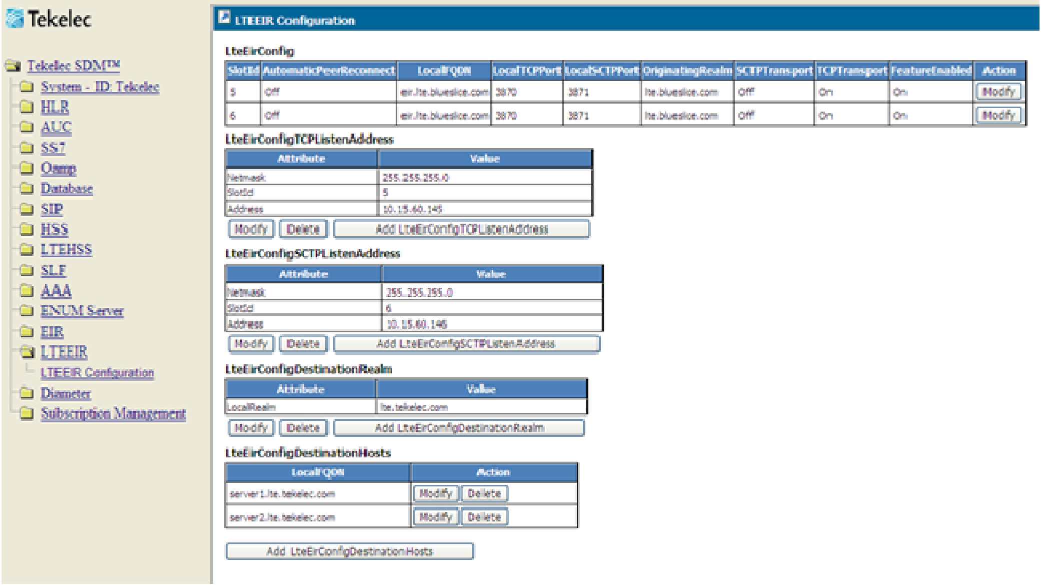
Introduction

Note: Some configurations require the stop of all processes on the blade and a restart of the blade to implement the changes. Read the procedure carefully prior to starting the configuration.

- For help using the WebCI and for instructions on how to provision tables in the WebCI, refer to *Web Craft Interface (WebCI)*
- To stop and restart a process, refer to section "Starting and Stopping Services on a blade" in the *SDM Monitoring, Maintaining, Troubleshooting User Guide*.
- For table descriptions, configuration values, rules, and all other operations, refer to the indicated entity table in the *SDM System Configuration Reference Manual*.

Configuring LTE-EIR Diameter tables

This procedure lists the high-level steps for the initial configuration of the LTE-EIR Diameter tables through the WebCI.



LteEirConfig

SlotId	AutomaticPeerReconnect	LocalFQDN	LocalTCPPort	LocalSCTPPort	OriginatingRealm	SCTPTransport	TCPTransport	FeatureEnabled	Action
5	Off	eir.lte.blueslice.com	3870	3871	lte.blueslice.com	Off	On	On	Modify
6	Off	eir.lte.blueslice.com	3870	3871	lte.blueslice.com	Off	On	On	Modify

LteEirConfigTCPListenAddress

Attribute	Value
Netmask	255.255.255.0
SlotId	5
Address	10.15.60.145

LteEirConfigSCTPListenAddress

Attribute	Value
Netmask	255.255.255.0
SlotId	6
Address	10.15.60.146

LteEirConfigDestinationRealm

Attribute	Value
LocalRealm	lte.tekelec.com

LteEirConfigDestinationHosts

LocalFQDN	Action
server1.lte.tekelec.com	Modify Delete
server2.lte.tekelec.com	Modify Delete

Figure 87: LTE-EIR Diameter Table Configuration

1. Stop the LTE-HSS service that is running on the same blade as the LTE-EIR service before configuring the LTEEirConfig table. Refer to procedure "Stop/Start one single service on a blade" in the *SDM Monitoring, Maintaining, Troubleshooting User Guide*.
2. Go to **LTEEIR>LTEEIR Configuration**.
3. Click the **Add LteEirConfig** button to configure the LTE-EIR, including the *Diameter Host Name* and the *Diameter Realm*.
4. Click the **Add LteEirConfigTcpListenAddress** button to configure the IP address for a TCP connection.

5. Click the **Add LteEirConfigSctpListenAddress** button to configure the IP address for an SCTP connection.
6. Restart the LTE-HSS service. Refer to procedure "Stop/Start one single service on a blade" in the *SDM Monitoring, Maintaining, Troubleshooting User Guide*.
7. Go to **LTEEIR>LTEEIR Configuration**.
8. Click the **Add LteEirConfigDestinationHosts** button to define the Diameter host authorized to establish a new Diameter connection with the EIR application.
   Add, modify, and delete operations can be performed while the LTE process is running.
9. Click the **Add LteEirConfigDestinationRealm** button to restrict the Diameter Realm that will be authorized to connect with it.
   Add, modify, and delete operations can be performed while the LTE process is running.

Glossary

A

AAA	Authentication, Authorization, and Accounting (Rx Diameter command)
AC	Application Context
ASP	Application Server Process A process instance of an Application Server. An Application Server Process serves as an active or standby process of an Application Server (e.g., part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances of) MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP end-point, and may be configured to process signaling traffic within more than one Application Server.
AuC	Authentication Center

C

CC	Country Code
CLI	Command-line interface
CSCF	Call Session Control Function

D

Diameter	Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in

D

both local and roaming AAA situations.

Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

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 5 ISS, but does not have to be.

E

EIR

Equipment Identity Register

A network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). Use of the EIR can prevent the use of stolen handsets because the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being registered on the network, thus making them useless.

E

ENUM

T**E**lephone **NU**mber **M**apping

ESD

Electro-Static Discharge

F

FMC

Fixed-Mobile Convergence

G

GGSN

Gateway GPRS Support Node

An edge router that acts as a gateway between a GPRS wireless data network and other networks. The MPE supports GGSN nodes as network elements. See also GPRS, PGW, and SGW.

GT

Global Title Routing Indicator

GTT

Global Title Translation

A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE 5 ISS uses to determine which service database to send the query message when an MSU enters the EAGLE 5 ISS and more information is needed to route the MSU. These service databases also verify calling card numbers and credit card numbers. The service databases are identified in the SS7 network by a point code and a subsystem number.

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

HLR

Home Location Register

HPLMN

Home Public Land Mobile Network

HSS

Home Subscriber Server

A central database for subscriber information.

I

IMEI

International Mobile Equipment Identifier

IMSI

International Mobile Subscriber Identity

IPSP

IP Server Process

A process instance of an IP-based application. An IPSP is essentially the same as an ASP, except that it uses MU3A in a peer-to-peer fashion. Conceptually, an IPSP does not use the services of a signaling gateway.

ITU

International Telecommunications Union

M

M3UA

SS7 MTP3-User Adaptation Layer

M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.

MAP

Mobile Application Part

MCC

Mobile Country Code

M

A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.

MNC

Mobile Network Code

A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.

N

NA

Nature of Address

NDC

Network destination code

NI

Network Indicator

NP

Number Plan

O

OAMP

Operations, Administration and Maintenance Part

OPC

Originating Point Code

P

PDN

Packet Data Network

A digital network technology that divides a message into packets for transmission.

PEM

Power Entry Module

P

There are two pluggable redundant Power Entry Modules (PEMs) that are located at the rear bottom side of each shelf. Each PEM provides power terminals for four 30 amp power feeds.

PLMN

Public Land Mobile Network

S

SAP

Service Access Point

SC

System Controller

SCCP

Signaling Connection Control Part

S-CSCF

Serving - Call Session Control Function

Provides user and service authentication and authorization, client registration, SIP-routing capabilities, service integration, data management, FW/NAT traversal, multi-network integration and an interface to third-party applications.

SCTP

Stream Control Transmission Protocol

An IETF transport layer protocol, similar to TCP that sends a message in one operation.

The transport layer for all standard IETF-SIGTRAN protocols.

SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an

S

	association; in TCP, these are sockets) for transmission of user messages.
SDM	Subscriber Data Management
SEP	Signaling End Point A node in an SS7 network that originates or terminates signaling messages. One example is a central office switch.
SGSN	Serving GPRS Support Node
Signaling Point	See SP.
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
SLC	Signaling Link Code
SLF	Subscription Locator Function
SOAP	Simple Object Access Protocol
SP	Signaling Point A set of signaling equipment represented by a unique point code within an SS7 domain.

S

SS7

Signaling System #7

SSA

Subsystem Allowed

SSH

Secure Shell

A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

SSN

Subsystem Number

A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry.

SSP

Subsystem Prohibited network management message.

SSR

SIP Signaling Router

Function responsible for querying a redirection server and proxying requests to other SSR servers, redirect servers, SSR Service Points, and Gateways. It helps in evolving a Flat NGN network into a hierarchical network.

STP

Signal Transfer Point

The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the

S

	Service Control Point (SCP) over the network.
Subscriber Data Management	See SDM.
Subsystem Number	See SSN.

T

TCAP	Transaction Capabilities Application Part
Translation Type	See TT.
TT	Translation Type Resides in the Called Party Address (CdPA) field of the MSU and determines which service database is to receive query messages. The translation type indicates which Global Title Translation table determines the routing to a particular service database.

U

UMTS	Universal Mobile Telecommunications System The standard for 3G used by GSM service providers. UMTS includes voice and audio services, for fast data, graphic and text transmissions, along with transmission of moving images and video.
USM	User Security Management
USSD	Unstructured Supplementary Service Data

V

V

VLR

Visitor Location Register

A component of the switching subsystem, within a GSM network. The switching subsystem includes various databases which store individual subscriber data. One of these databases is the HLR database or Home Location Register; and the VLR is another.

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.