

User Guide for Resource Activation

Ericsson Dynamic Activation 1

USER GUIDE

Copyright

© Ericsson AB 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Purpose and Scope	1
1.2	Target Group	1
1.3	Typographic Conventions	1
1.4	Prerequisites	1
2	General	3
2.1	Logging in	3
2.1.1	Logging in Using Internal Authentication	3
2.1.2	Logging in Using External Authentication	4
2.2	Launchpad	4
2.3	Slide-in Navigation Column	6
2.4	User Profile	7
2.5	Resilient Activation Configuration	8
3	Asynchronous Control	11
3.1	Configure Functions	11
4	CAI3G DC	13
4.1	Create CAI3G DC Routing	14
4.2	Edit CAI3G DC Routing	16
4.3	Delete CAI3G DC Routing	17
5	Cluster Strategies	19
5.1	Create Cluster Strategy Instance	20
5.1.1	Parameters	21
5.2	Edit Cluster Strategy Instance	24
5.3	Delete Cluster Strategy Instance	25
6	MO Type and NE Type Mapping	27
6.1	Mapping and Unmapping in Southbound MO Types List	28
6.2	Mapping and Unmapping in Graph	28
7	Notification Rule Configuration	29
7.1	Configure Notifications	29
8	Management	31



8.1	General	31
8.1.1	GUI Overview	31
8.1.2	GUI Icons	33
8.2	Activation Logic Control	34
8.2.1	Activation Logic	34
8.2.2	Options	47
8.3	Network Elements Control	48
8.3.1	Network Elements	48
8.3.2	Network Element Groups	65
8.3.3	Routing	68
8.4	System	73
8.4.1	Licenses	73
8.4.2	Options	74
8.4.3	Notification Email Configuration	76
8.4.4	Synchronize Configuration	77
8.5	Access Control	78
8.5.1	Users	78
8.5.2	Policies	85
8.5.3	Attribute Rules - Restriction Rules	85
8.5.4	Administration Domains	88
8.6	Walkthroughs Control	94
8.6.1	Initial Setup	94
9	Priority Configuration	97
9.1	Add or Edit a Priority Rule	97
9.2	Delete a Priority Rule	99
10	Retry Rule Configuration	101
10.1	Create Retry Rule	102
10.2	Manage Retry Rules	103
10.2.1	View Retry Rule Details	103
10.2.2	Change Retry Rule Priority	104
10.2.3	Edit Retry Rule	104
10.2.4	Copy Retry Rule	104
10.2.5	Delete Retry Rule	104
11	Asynchronous Request Management	105
11.1	Search by Condition	105
11.2	View Details of the Search Result	106
11.3	Delete Pending Items	107
11.3.1	Result of Delete Operation	108
12	Request Management	111
12.1	Search in Request Queues	113
12.2	Monitor and Manage Sub-requests	114



12.2.1	Monitoring Operations	114
12.2.2	View Details of a Sub-Request	116
12.3	Reschedule Expired Sub-requests	117
12.3.1	Add a Scheduled Retry Job	117
12.3.2	Manage Scheduled Retry Jobs	118
13	Processing Queue	119
13.1	Browser Processing Queues	119
13.2	Manage Processing Queues	121
13.2.1	Change Status for Selected Sub-requests	123
13.2.2	Change Status for All Sub-requests	124
14	Dashboard	127
14.1	General Settings	127
14.1.1	Refresh Dashboard	127
14.1.2	Select Monitoring Period	127
14.1.3	Choose Widgets	128
14.1.4	View Statistics Details	129
14.1.5	Change Table Settings	129
14.2	Northbound Performance	130
14.3	Southbound Performance	133
15	User Management	135
15.1	Create a User	136
15.2	Edit a User	138
15.3	Unlock a User	140
16	Log Management	143
16.1	Invoke a Log Search	146
16.2	Filter Search	146
16.3	Sort Search	147
16.4	Cancel Search	147
16.5	View Detailed Northbound and Southbound Information	147
17	Loose Error Handling Management	149
17.1	Rule Parameters	150
17.2	Adding a Rule	151
17.3	Removing rules	151
17.4	Editing a Rule	151
17.5	Duplicating a Rule	152
18	Appendix A - Standard Product Activation Logic	153



Reference List

155



1 Introduction

This document is a guide to the Graphical User Interface (GUI) in Ericsson™ Dynamic Activation (EDA).

1.1 Purpose and Scope

The purpose of this document is to provide help information on how to perform configuration tasks using the GUI.

This document covers all actions available in the GUI. All features are shown in this users guide. But depending on the authorities granted, only the granted GUI items and features are visible for a specific user.

1.2 Target Group

The target group for this document is users of the Dynamic Activation GUI.

For more information about different target groups, see *Library Overview*, Reference [1].

1.3 Typographic Conventions

Typographic conventions are described in *Library Overview*, Reference [1].

1.4 Prerequisites

To perform the configuration tasks, the GUI user must know which attributes need to be configured and their respective values.

For more information, refer to the following documents:

- *Configuration Manual for Subscriber Activation*, Reference [2].
- *Function Specification Resource Activation*, Reference [4].

Note: Screen captures in this document are examples. Some features pictured in them are license or version dependant.





2 General

This section provides basic information about the Dynamic Activation GUI.

Note: The supported web browsers are Chrome 58 and Firefox 52 or later versions.

2.1 Logging in

Use a web browser and direct it to the Dynamic Activation web management address. The address is as follows:

- Using HTTPS:

`https://<VIP-OAM-IP>:8383`

2.1.1 Logging in Using Internal Authentication

For the first time launching after installation, use the default user `admin` and default password `admin` to log in.

Note: The default user is defined during the installation. This user cannot be locked or deleted.

Other users must be created by `System Administrator` before they can log in. For information, see Section 15 on page 135.

- For other users, type the user email and password to log in. The initial password is provided by the `System Administrator`.
- It is mandatory to change the password after the first logon, and make changes regularly later on.
- After logging in, it is possible to change the user profile. For more information, see Section 2.4 on page 6.
- Users are locked if there are too many failed logon attempts. Contact the `System Administrator` to solve the problem.

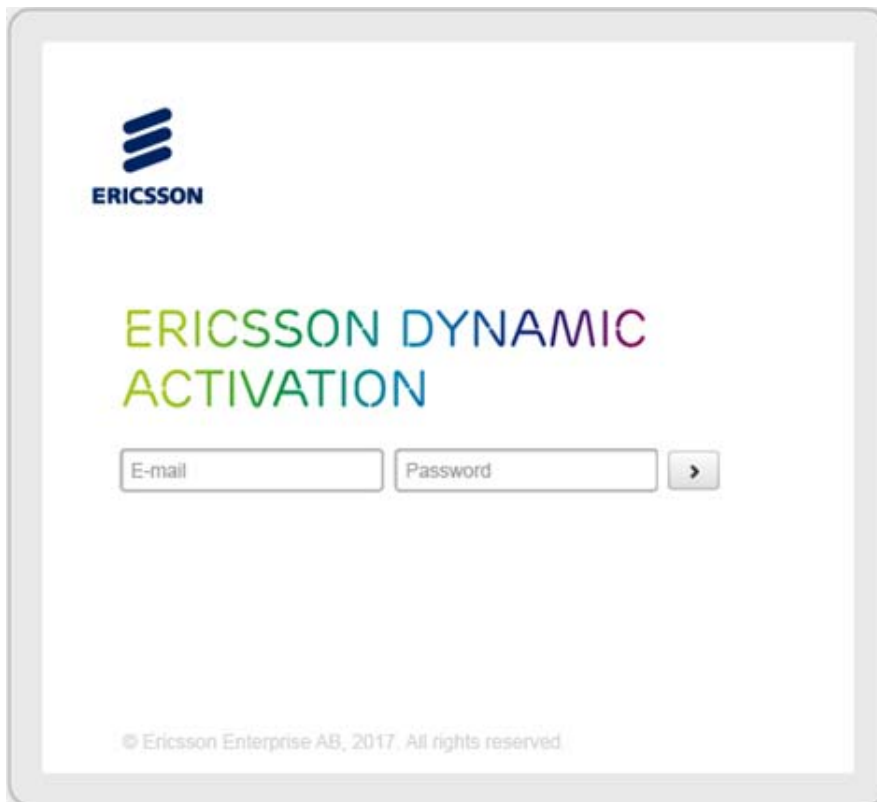


Figure 1 Dynamic Activation Logon Window

2.1.2 Logging in Using External Authentication

When using external authentication, Dynamic Activation users are created in external OpenID connect provider before login. For more information, refer to documents in related OpenID Connect Provider product.

During the OpenID authentication process, browser is redirected to the login page of external OpenID connect server.

- Type the user credential of external Dynamic Activation users to log in.
- After login, browser is redirected to the Dynamic Activation launchpad.
- User profiles of external users are read only.

2.2 Launchpad

Figure 2 shows the launchpad after a successful logon.

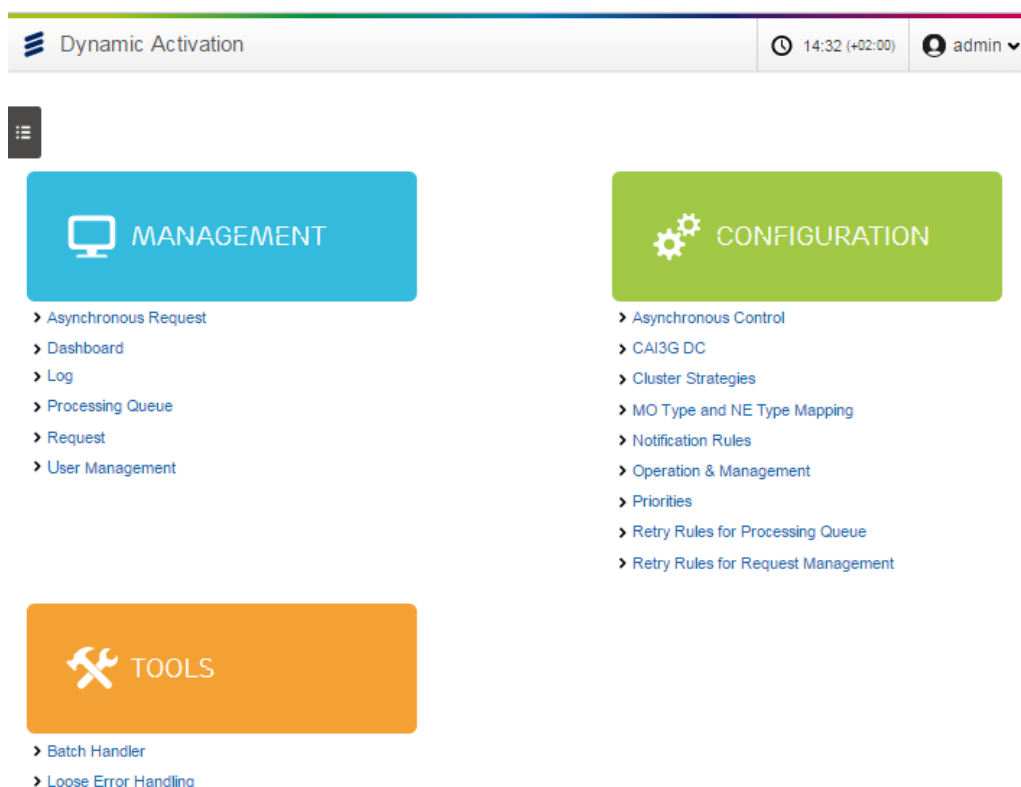


Figure 2 Launchpad


The launchpad provides portals to the following application GUIs:

- **Management**
 - **Asynchronous Request** – Browses the information of asynchronous CAI3G requests that have not been executed successfully. See Section 11 on page 105.
Related configuration: **Priorities**
 - **Dashboard** – Monitors provisioning performance for northbound and southbound. See Section 14 on page 127.
 - **Log** – Manages the processing log. Also can be accessed through the **Operation & Management**. See Section 16 on page 143.
 - **Processing Queue** – Browse and manage provisioning sub-requests on NE/NE groups or clusters level. See Section 13 on page 119.
Related configuration: **Retry Rules for Processing Queue**
 - **Request** – Provides visualized statistics and management of sub-requests for each Network Element (NE) Abstraction Queue. See Section 12 on page 111.
Related configurations: **Notification Rules** and **Retry Rules for Request Management**



- **User Management** – Creates and manages users that can access GUI. Only `System Administrator` has access to this GUI. See Section 15 on page 135.
- Configuration
 - **Asynchronous Control** – Configures the Asynchronous CAI3G request handler function. See Section 3 on page 11.
 - **CAI3G DC** – Configures Routing Rules of CAI3G Distribution. See Section 4 on page 13.
 - **Cluster Strategy Configuration** – Configures instances of Cluster Strategies. See Section 5 on page 19.
 - **MO Type and NE Type Mapping** – Maps MO types to NE types to route sub-requests to corresponding Resource Queues. See Section 6 on page 27.
 - **Notification Rules** – Configures whether to enable intermediate notifications for asynchronous requests on each type of NEs. See Section 7 on page 29.
 - **Operation & Management** – Typical operation and maintenance management, such as managing activation logic, NE configurations, and system configurations. See Section 8 on page 31.
 - **Priorities** – Manages priority rule to be applicable on the Asynchronous CAI3G request. See Section 9 on page 97.
 - **Retry Rules for Processing Queues** and **Retry Rules for Request Management** – Configures rules of provisioning retries in processing queues or Resource Queues. See Section 10 on page 101.
- Note:** For typical workflow of the Resilient Activation configuration, see Section 2.5 on page 8.
- Tools
 - **Batch Handler** – Manage and monitor the batch jobs, refer to *User Guide for Batch Handler*, Reference [10].
 - **Loose Error Handling** – Can also be accessed through the **Operation & Management**. See Section 17 on page 149.

2.3 Slide-in Navigation Column

When clicking  on the Dynamic Activation GUI, a slide-in navigation column is displayed to provide easy accesses to all application GUIs.



2.4 User Profile

After successfully logging in, users can view and edit their own user profiles, as shown in Figure 3.

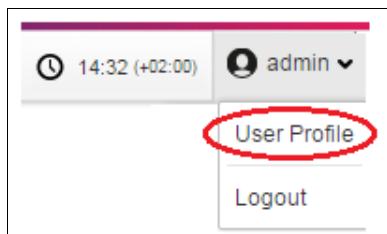
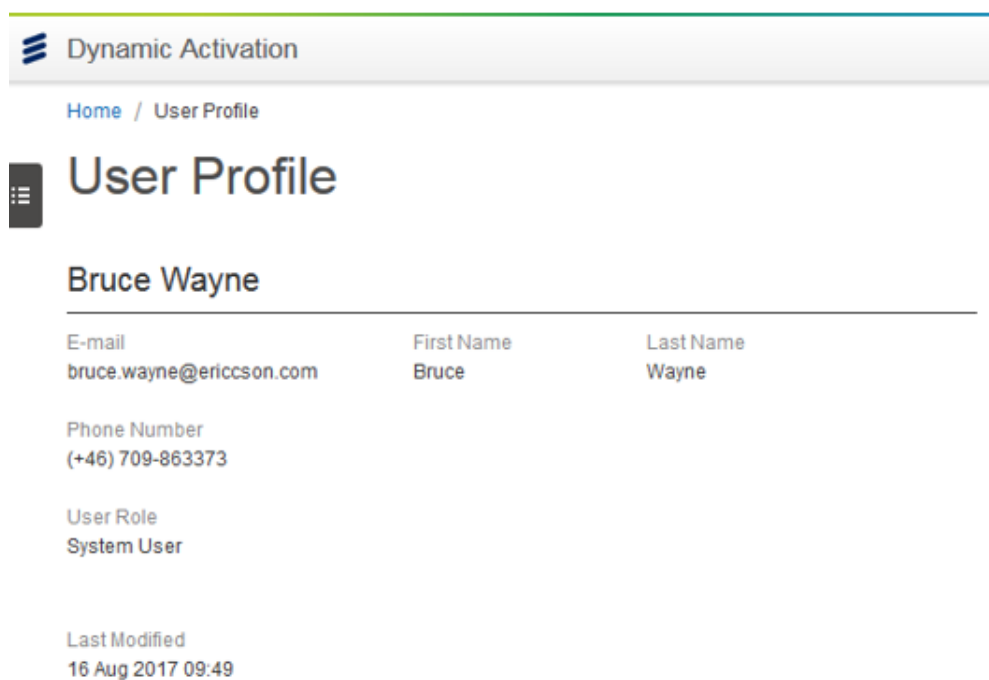


Figure 3 View User Profile

In the **User Profile** GUI, users can:

- View their own user profile.

Note: When using external authentication, user profiles of external users are read only.



- Change the logon password.

The GUI automatically checks whether the new password fulfills the password rules, and shows validation messages accordingly.

- Click **Edit profile** and follow the GUI instruction to change the profile.



Note: **Email** and **User Role** can be only changed in the **User Management** GUI by a **System Administrator**.

E-mail is changed by deleting the old one and then creating a new one.

For instructions, see Section 15.2 on page 138.

The screenshot shows the 'Dynamic Activation' web interface. At the top, there's a header with the logo, 'Dynamic Activation', a clock showing '14:32 (+02:00)', and a user profile icon labeled 'Bruce'. Below the header, the breadcrumb 'Home / User Profile' is visible. The main section is titled 'User Profile' and includes an 'Edit profile' button. The user's name 'Bruce Wayne' is displayed. Below this, there are two columns of information. The left column contains: 'E-mail' (bruce.wayne@ericsson.com), 'First Name' (Bruce), 'Last Name' (Wayne), 'Phone Number' ((+46) 709-863373), and 'User Role' (System Administrator). The right column is titled 'Change Password' and contains: 'Current Password' (input field), 'New Password' (input field), 'Confirm New Password' (input field), and a 'Change Password' button. At the bottom left, it says 'Last Modified 15 May 2017 15:51'.

Figure 4 Change Password and Edit User Profile

2.5 Resilient Activation Configuration

Figure 5 shows the typical workflow of the Resilient Activation configuration.

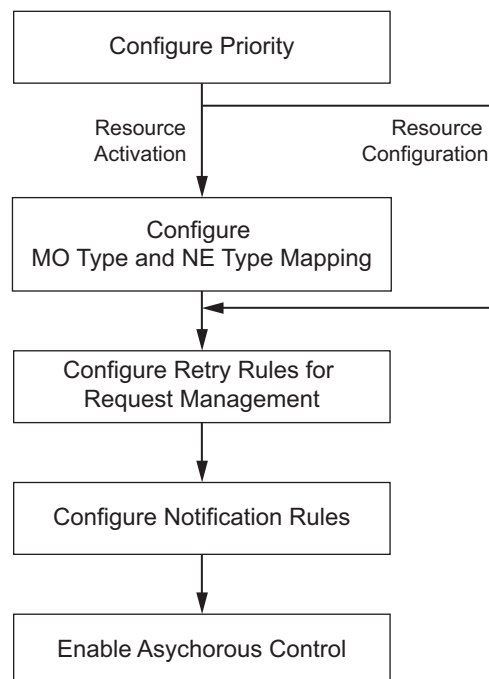


Figure 5 Typical Configuration Workflow

For more information on this function, refer to *Function Specification Dynamic Activation Execution Environment*, Reference [9].





3 Asynchronous Control

The **Asynchronous Control** GUI shown in Page 11 provides the controller of Asynchronous CAI3G request handler functions.

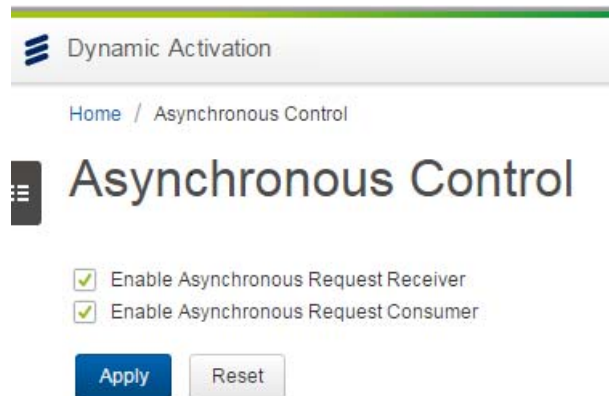


Figure 6 Asynchronous Control GUI

In **Asynchronous Control** GUI:

- **Enable Asynchronous Request Receiver:** A configuration to control whether Dynamic Activation accepts Asynchronous CAI3G request. The initial setting is **Enable** (check box is selected).
- **Enable Asynchronous Request Consumer:** A configuration to control whether Dynamic Activation executes the Asynchronous CAI3G requests and the Asynchronous notifications that have not been executed successfully. The initial setting is **Enable** (check box is selected).




Note: DO NOT DISABLE THE ASYNCHRONOUS REQUEST CONSUMER when the system has ongoing provisioning. Because the notification of the ongoing provisioning would be lost and some data inconsistency errors would be recorded in the log file.

BEFORE DISABLING OR ENABLING THE ASYNCHRONOUS REQUEST CONSUMER, complete all grouped requests when using the Request Grouping requests and notification at same time. Refer to section *Limitations in Function Specification Dynamic Activation Execution Environment*, Reference [9].

3.1 Configure Functions

To configure the Asynchronous CAI3G request handler functions:



- Select or clear the check box  to enable or disable the function. And then click  to apply the configuration.
- Click  to restore to the last configuration.



4 CAI3G DC

Figure 7 shows the GUI used for browsing and managing CAI3G DC Routing.

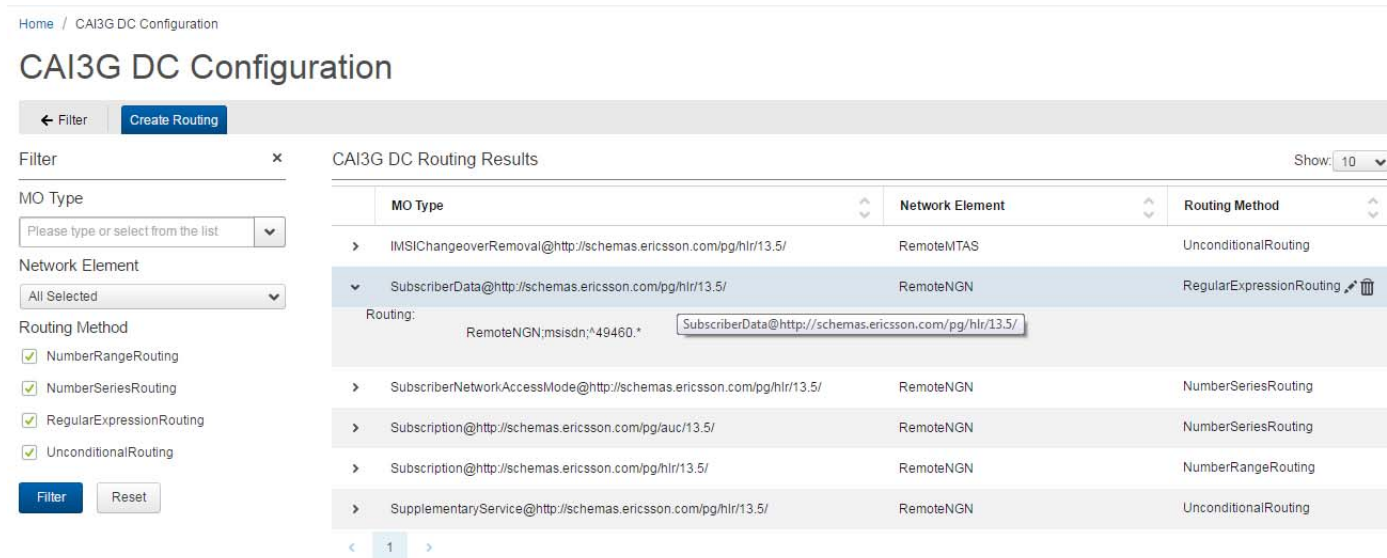


Figure 7 CAI3G DC Configuration

In the **CAI3G DC Configuration** GUI, user can:

- Filter the CAI3G DC configuration (in **Filter** area) that matches the desired condition. The filter panel can be collapsed by or click .

MO Type - Specify the keyword of the desired MO Type in this filed.

Network Element - Select the desired NE in this filed.


Note: The remote CAI3G NE must be created before configuring CAI3G DC routing. For NE creation, see Section 8.3.1 on page 48.

Routing Method - Select the desired routing methods in this filed.

The results are displayed in **CAI3G DC Routing Results** area.

- Click in the action bar to create a CAI3G DC Routing, see Section 4.1 on page 14.
- Click (in **CAI3G DC Routing Results** area) to view the detailed information of a CAI3G DC Routing.




- Hover the mouse over a result (in **CAI3G DC Routing Results** area) to show editor and deletion button  on the right side.

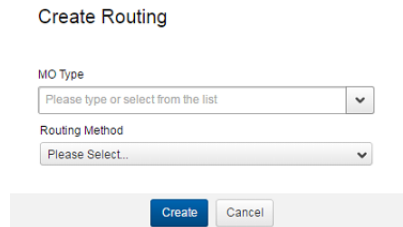
For edit operation, see Section 4.2 on page 16.

For delete operation, see Section 4.3 on page 17.

4.1 Create CAI3G DC Routing

To add a CAI3G DC Routing in the **CAI3G DC Configuration** GUI:

1. Click . This opens the **Create Routing** dialog.



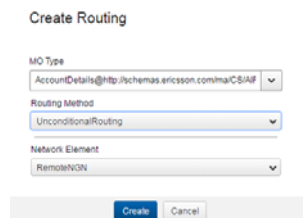
The 'Create Routing' dialog box contains two dropdown menus. The first is labeled 'MO Type' with the placeholder text 'Please type or select from the list'. The second is labeled 'Routing Method' with the placeholder text 'Please Select...'. At the bottom of the dialog are two buttons: 'Create' and 'Cancel'.

2. In **MO Type** field, select a local MO Type from the drop-down list. Or enter the full name of a MO Type that is only available in the remote CAI3G server.

Note: Ensure that the local MOType is available in the remote CAI3G server.

3. In **Routing Method** drop down list, select a routing method from the list. Then the addition parameters of the select Routing Method are displayed.

- UnconditionalRouting



The 'Create Routing' dialog box is shown with 'UnconditionalRouting' selected in the 'Routing Method' dropdown. The 'MO Type' dropdown now shows the text 'AccountDetails@http://schemas.ericsson.com/ma/CSMF'. The 'Network Element' dropdown now shows 'Remote/ON'. The 'Create' and 'Cancel' buttons remain at the bottom.

- a **Network Element** - Select a remote CAI3G NE from the drop-down list.

- NumberRangeRouting



The 'Create Routing' form is shown with the following fields and values:

- MO Type:** AccountDetails@http://schemas.ericsson.com/ma/CS/AF
- Routing Method:** NumberRangeRouting
- Network Element:** RemoteNGN
- MO ID:** MSISDN
- Start Range:** 33000000
- Stop Range:** 44999999
- Buttons:** An 'Add' button with a downward arrow and a trash icon, and a 'Create' button.
- Display Field:** A list containing 'RemoteNGN:MSISDN:121000'.


- a Fill in the addition parameters:


Network Element - Select the remote CAI3G NE from the drop-down list.

MO ID - Specify the MO ID for this MO Type, such as IMSI or MSISDN.

Start Range - Specify the start range of the Number range.

Stop Range - Specify the stop range of the Number range. Stop range must be larger than the start range.

- b Click  to display this routing rule in the display field. More than one routing rules can be added for Number Range Routing.

Click  to remove a selected routing rule from the display field.

- NumberSeriesRouting.

The 'Create Routing' form is shown with the following fields and values:


- MO Type:** AccountDetails@http://schemas.ericsson.com/ma/CS/AF
- Routing Method:** NumberSeriesRouting
- Network Element:** RemoteNGN
- MO ID:** MSISDN
- Series:** 456
- Buttons:** An 'Add' button with a downward arrow and a trash icon, and a 'Create' button.
- Display Field:** A list containing 'RemoteNGN:MSISDN:123'.


- a Fill in the addition parameters:

Network Element - Select the remote CAI3G NE from the drop-down list.

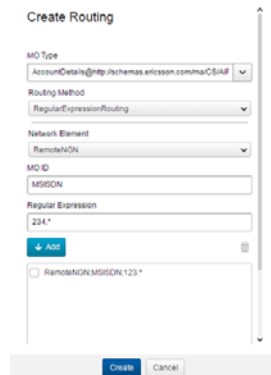
MO ID - Specify the MO ID for this MO Type, such as IMSI or MSISDN.

Series - Specify the number series of MO ID.

- b Click  to display this routing rule in the display field. More than one routing rules can be added for Number series Routing.

Click  to remove a selected routing rule from the display field.

- RegularExpressionRouting





- a Fill in the addition parameters:

Network Element - Select the remote CAI3G NE from the drop-down list.

MO ID - Specify the MO ID for this MO Type, such as IMSI or MSISDN.

Regular expression - Specify the regular expression of MO ID.


- b Click  to display this routing rule in the display field. More than one routing rules can be added for Regular Expression Routing.

Click  to remove a selected routing rule from the display field.

4. Click  to apply the routing rules.

4.2 Edit CAI3G DC Routing

To Edit a CAI3G DC Routing in the **CAI3G DC Configuration** GUI:

1. Hover the mouse over a routing to be edit and then click . This opens the **Edit Routing** slide-in panel.



Edit Routing

MO Type
Subscription@http://schemas.ericsson.com/pghtml/13.5/

Routing Method
NumberRangeRouting

Network Element
Please select...

MO ID

Start Range

Stop Range

[Add](#)

☐ RemoteNGN/msisdn;494600000001;4946000999...

[Save](#) [Cancel](#)


2. Edit the parameters. If routing method has been changed, the additional parameters are to be changed according to the routing methods.

For detailed information of each parameter and operation steps, see Section 4.1 on page 14.

3. Click [Save](#) to save the routing rules.

4.3 Delete CAI3G DC Routing

To delete a CAI3G DC Routing in the **CAI3G DC Configuration** GUI:

1. Hover the mouse over a routing to be deleted and then click the .
2. Click [Yes](#) to confirm the deletion.



5 Cluster Strategies

The **Cluster Strategy Configuration** GUI shown in Figure 8 is used for browsing and managing Cluster Strategy instance.

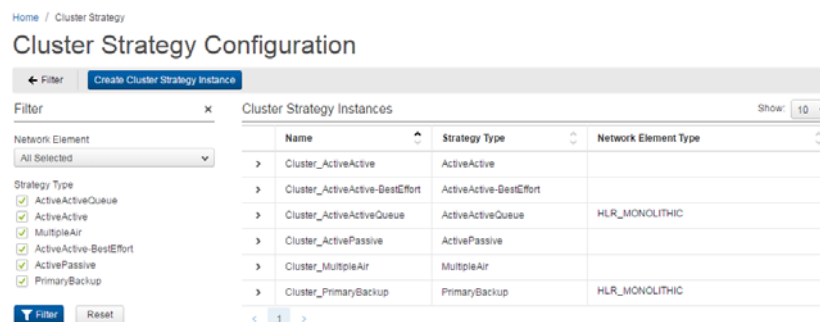





Figure 8 Cluster Strategy Configuration

By default, the **Cluster Strategy Configuration** GUI displays all configured cluster strategy instance, user can:

- Filter the cluster strategy instances (in **Filter** area) that matches the desired condition. The filter panel can be collapsed by  or click .


Network Element - Select the desired NE in this filed.

Strategy Types - Select the desired strategy types in this filed.

- Create a cluster strategy instance by clicking **Create Cluster Strategy Instance**. See Section 5.1 on page 20.
- Edit or delete a configured cluster strategy instance. Hover the mouse over a configured cluster strategy instance to show editor and deletion button  on the right side.

For edit operation, see Section 5.2 on page 24.

For delete operation, see Section 5.3 on page 25.

- View all configured cluster strategy instances in **Cluster Strategy Instance Results** and click  to view the details information.
 - **Name** - The name of the cluster strategy instance.
 - **Strategy Type** - The algorithm that is to be used by the Cluster Strategy to distribute the requests between the NEs in the cluster.

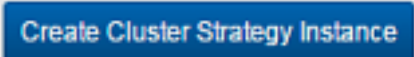
Note: The parameter **Strategy Type** is not editable for a configured cluster strategy instance.

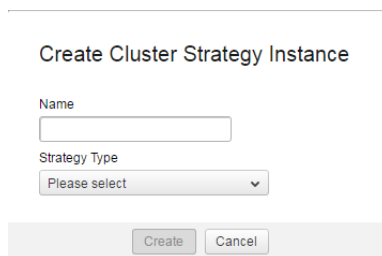


- **Network Element Type** - The NE type that the cluster strategy belongs to. For how to configure NE type, refer to Section 8.3.3 on page 68.

5.1 Create Cluster Strategy Instance

To create a cluster strategy instance in the **Cluster Strategy Configuration** GUI:

1. Click . This opens the **Create Cluster Strategy Instance** dialog.

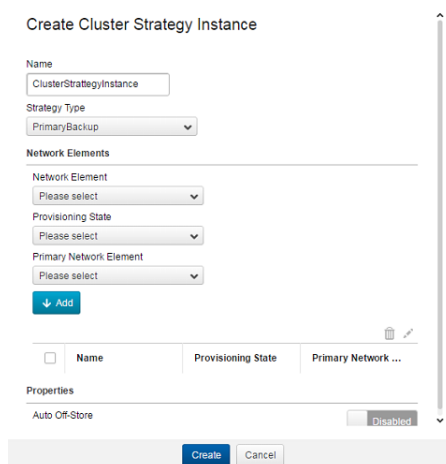


Create Cluster Strategy Instance

Name

Strategy Type

2. Specify a Name and select a Strategy Type. Then the specific parameters of the selected strategy type are displayed in the section **Network Elements** and **Properties** (when applicable).



Create Cluster Strategy Instance

Name

Strategy Type

Network Elements

Network Element

Provisioning State


Primary Network Element


<input type="checkbox"/>	Name	Provisioning State	Primary Network ...
--------------------------	------	--------------------	---------------------

Properties

Auto Off-Store

- Configure the NEs of this cluster strategy instance in **Network Elements** section and then click  to display the configuration of each NE in the display field.


Click  to remove the selected configured NEs from the display field.

Click  to edit the parameters of a selected NE. The configured setting pops up back to the panel.



- (When applicable) Configure the general feature of this cluster strategy type in **Properties** section.

The corresponding parameters of each strategy type and their description are described in Table 1.

3. Click  to create the cluster strategy.

5.1.1

Parameters

The following table describes the corresponding parameters of each strategy type.

Table 1 Parameters of Each Strategy Type

Strategy Type	Section Name	Parameter Name	Description
Active Active	Network Elements	Network Element	Specify the NE to be used for the cluster strategy instance.
		Provisioning State	This field is not applicable for ActiveActive strategy. <ul style="list-style-type: none"> • N/A: Select N/A in the drop-down list for this cluster strategy.
Active Active- BestEffort	Network Elements	Network Element	Specify the NE to be used for the cluster strategy instance.
		Provisioning State	This field is not applicable for ActiveActive-BestEffort strategy. <ul style="list-style-type: none"> • N/A: Select N/A in the drop-down list for this cluster strategy.
MultipleAir	Network Elements	Network Element	Specify the NE to be used for the cluster strategy instance.
		Provisioning State	This field is not applicable for MultipleAir strategy. <ul style="list-style-type: none"> • N/A: Select N/A in the drop-down list for this cluster strategy.
		Order	Order 0 means that this NE works as a primary NE. There must be one and only one NE with order "0" in MultipleAir cluster.



Strategy Type	Section Name	Parameter Name	Description
Active Active Queue	Network Elements	Network Element	Specify the NE to be used for the cluster strategy.
		Provisioning State	<ul style="list-style-type: none">• On: to execute the provisioning commands directly.• Off: to discard the provisioning commands.• Off-Store: to store the provisioning commands into processing queue. The provisioning commands are only enqueued when they are changing the data in NE (such as create, set, and delete operation). <p>There must be at least one NE with provisioning state On in the cluster.</p>
	Properties	Auto Off-Store	<p>Indicates whether the Auto Off-Store function is enabled or not. It is disabled by default.</p> <p>When property Auto Off-Store is enabled, if the provisioning commands fail for some continuous reasons within a period, the provisioning state of this NE is automatically switched to Off-Store. (The reason is configured by Response Code. The period is configured by Minimum Duration (seconds) for continuous Response Code.) At the same time, an event is sent out to inform provisioning state changed for this NE.</p>
		Minimum Duration (seconds) for continuous Response Code	<p>This field only accepts numbers.</p> <p>For example, 600.</p>
		Response Code	<p>This field is a regular expression, which is used for matching valid Respond Code.</p> <p>For example, to match 5 digits respond code starting with 101 or 105, regular expression "(101[0-9][0-9] 105[0-9][0-9])" is used in this field.</p>



Strategy Type	Section Name	Parameter Name	Description
Active Passive	Network Elements	Network Element	Specify the NE to be used for the cluster strategy.
		Provisioning State	<ul style="list-style-type: none"> On-Active: indicates that the NE is ready to receive provisioning requests. On-Passive: indicates that the NE is stand-by. Off: indicates that provisioning is not sent to this NE. <p>There must be one NE with provisioning state On-Active and one or more NEs with provisioning state On-Passive/Off in the cluster.</p>
	Properties	Error Code for detecting passive status of network element	<p>All requests are sent to the On-Active node until it fails owing to link error or matching the error code for detecting passive status of NE (configured by this feature). When this happens, it provisions to other On-Passive nodes in the cluster one by one. The first node, whose response is not link error or the error code configured by this feature, is to be taken as a new On-Active node. If no On-Passive nodes are qualified for On-Active, the original On-Active one keeps its provisioning state.</p>



Strategy Type	Section Name	Parameter Name	Description
Primary Backup	Network Elements	Network Element	Specify the NE to be used for the cluster strategy.
		Provisioning State	<ul style="list-style-type: none">• On: to execute the provisioning commands directly.• Off: to discard the provisioning commands.• Off-Store: to store the provisioning commands into processing queue. The provisioning commands are only enqueued when they are changing the data in NE (such as create, set, and delete operation). <p>There must be at least one NE with provisioning state On in the cluster.</p>
		Primary Network Element	<p>The configuration of primary network must follow the rules:</p> <ul style="list-style-type: none">• There must be one and only one primary NE.• A primary NE can only be in provisioning state ON. <p>Make sure that the processing queue is empty before changing the status of an NE, refer to Section 13 on page 119.</p>
	Properties	Auto Off-Store	<p>Indicates whether the Auto Off-Store function is enabled or not. It is disabled by default.</p> <p>When property Auto Off-Store is enabled, if the provisioning commands fail for some continuous reasons within a period, the provisioning state of this NE is automatically switched to Off-Store. (Where the reason is configured by Response Code. And the period is configured by Minimum Duration (seconds) for continuous Response Code.) At the same time, an event is sent out to inform provisioning state changed for this NE.</p>
		Minimum Duration (seconds) for continuous Response Code	<p>This field only accepts number.</p> <p>For example, 600.</p>
		Response Code	<p>This field is a regular expression, which is used for matching valid Respond Code.</p> <p>For example, to match 5 digits respond code starting with 101 or 105, regular expression "(101[0-9][0-9] 105[0-9][0-9])" is used in this field.</p>

5.2 Edit Cluster Strategy Instance


To edit a cluster strategy in the **Cluster Strategy Configuration GUI**:

1. Hover the mouse on a cluster strategy instance to be edit and then click . This opens the **Edit Cluster Strategy Instance** slide-in panel.






2. Edit the parameters. For detailed information of each parameter and operation steps, see Section 5.1 on page 20.

Note: For cluster strategy `PrimaryBackup`, to change the Network Element to a primary NE, the processing queue must be empty. Otherwise, it is not allowed.

3. Click  to save the cluster strategy instance.

5.3 Delete Cluster Strategy Instance

To delete a Cluster Strategy Instance in the **Cluster Strategy Configuration** GUI:

1. Hover the mouse over a Cluster Strategy Instance to be deleted and then click .
2. Click  to confirm the deletion or click  to cancel the delete action.





6 MO Type and NE Type Mapping

Mapping between MO type and NE type enables routing sub-requests to the corresponding Resource Queues. The **MO Type and NE Type Mapping** GUI is shown in Figure 9 and described afterwards.

The screenshot displays the 'MO Type and NE Type Mapping' GUI. At the top, there's a header with 'Dynamic Activation' and a user profile 'admin'. Below the header, the page title 'MO Type and NE Type Mapping' is shown. The main content area is divided into two tabs: 'Southbound MO Types' (1) and 'Northbound MO Types' (4). The 'Southbound MO Types' tab is active, showing a search bar (2) and a list of MO types. The list includes various Ericsson schema URIs such as 'CAMELTriggeringCriteria@http://schemas.ericsson.com/pg/hlr/13.5/' and 'CallBarringProfile@http://schemas.ericsson.com/ma/bce/'. To the right of the list, a diagram (3) illustrates the mapping between MO types and NE types. The diagram shows a central hub with various MO types connected to different NE types. The NE types are represented by colored dots and labels: MSASpda...om/mahSSI, HSS_FE_IMS, ILF, Subscriber...oning/ILF/, Subscriber...ma/CS/AI/, Subscriber...ma/CS/AIR/, DNSSubscri...Works/5.0/, ENUM, AIR, BCE, NONSIM_HSS..., NONSIM_AAA, AAUUser@ht...airWORKS/, ECSCSCertifi...m/mahECSCSIS/, Subscriber...ning/MTAS/, M2MService.../hr/13.5/, M2M_COMMON..., M2M_HLR_RED, CUDB_HLR, DAE_NOTIFIC..., CUDB_DAE, CUDB_SAPC, CUDB_MASSIV..., and MSASpda...om/mahSSI.

Figure 9 MO Type and NE Type Mapping

In the **MO Type and NE Type Mapping** GUI:

- Panel 1 lists all available southbound MO types that are registered by a legacy JDV or a Service JDV.

For more information about JDV files, refer to *Customer Adaptation Development Guide for Resource Activation*, Reference [3].



- Area **2** provides a search box for narrowing down the southbound MO types list.
- Graph **3** shows all configured mappings between southbound MO types (outer ring) and NE types (inner ring).



The NE types are configured in the **Routing** GUI. For more information, see Section 8.3.3 on page 68.

- Panel **4** lists all northbound MO types that are registered by Service Models.

For more information about Service Models, refer to *User Guide for Designer Studio*, Reference [8].

6.1 Mapping and Unmapping in Southbound MO Types List

To map (or unmap) an MO type and an NE type in panel **1**, do the following:

1. Click  (or ) of a desired southbound MO.

This pops up a list of all available NE types on the Dynamic Activation.

2. Click the desired NE type to create (or remove) the mapping between the chosen MO and NE types.

The newly created (or removed) mapping is displayed (or removed) in graph **3**.

6.2 Mapping and Unmapping in Graph

An alternative operation is available in the **MO Type and NE Type Mapping** GUI that is shown in Figure 9.

- Drag a desired southbound MO type from area **1** to graph **3**. And drop it to a desired NE type (inner ring) to create a mapping between them.
- In area **3**, drag a southbound MO type (outer ring), and drop it to the center of the graph to remove the mapping relationship.



7

Notification Rule Configuration

Figure 10 shows the configuration of intermediate notification for sub-requests in Resource Queues.

Target Resource	Successful	Failed	Rules
PGW	ON	ON	Timelimit Exceeded, Broken Connection, Response Time-out
GFLEX	OFF	ON	Communication Failure, Function Busy
VMS	ON	OFF	Client Error, Server Error
IAM	OFF	OFF	Timelimit Exceeded
OTA	OFF	OFF	Administrative Limit Exceeded
SOS	OFF	ON	Timelimit Exceeded
AFG	OFF	OFF	
CT	OFF	OFF	
MOS	OFF	ON	
NAP	OFF	ON	
SMS	OFF	OFF	
XDMS	ON	ON	

Figure 10 Notification Rule Configuration GUI

Available information is:

- **Target Resource** – All target resources that individual Resource Queues are representing.
- **Successful / Failed** – Whether to send an intermediate notification when a sub-request is performed successfully or failed.
- **Rules** – Retry rules that can trigger an intermediate notification when a sub-request is retried. See Section 10 on page 101.

7.1 Configure Notifications

To configure the intermediate notification settings on a target resource:

1. In the **Notification Rule Configuration** GUI, click a row to open the **Edit notification rule** slide-in panel.



Edit Notification Rule

Target Resource

Successful ☐ OFF

Failed ☒ ON

Rules

- ☒ Unwilling to Perform
- ☒ Communication Failure
- ☐ Function Busy
- ☐ Administrative Limit Exceeded

2. Configure whether to send an intermediate notification based on the **Successful** / **Failed** response of sub-requests.
3. (Optional) Click a retry rule to add (or remove) it as a rule that can trigger a notification when a sub-request is retried.

Note: For more information on how to configure retry rules, see Section 10 on page 101.

4. Click to apply the configuration.

8 Management

8.1 General

Note:

- Do not use the **Back** and **Forward** buttons in the web browser, as this causes an error.
- Do not use multiple browser windows or browser tabs simultaneously on one workstation, as this causes an error.

8.1.1 GUI Overview

The default Dynamic Activation GUI consists of the following parts.

- Main area - contains general items, such as **About** and **Site Map**
- Feature bar - consists of feature tabs.
- The working area - the area where the features are handled.

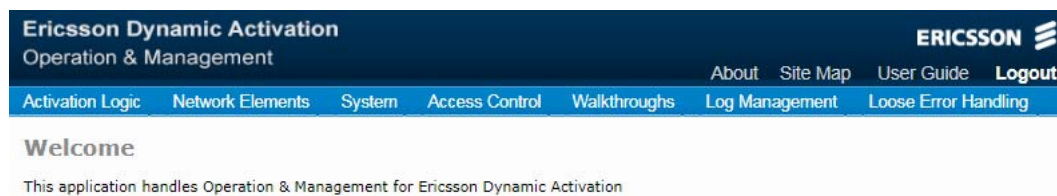


Figure 11 GUI Overview

8.1.1.1 Main Area

The general items of the main area are explained in Table 2.

Table 2 GUI Main Area

Item	Description
About	Shows information about software version.
Site Map	Hyperlinks to Dynamic Activation GUI feature tabs and subtabs.
User Guide	Link to Dynamic Activation GUI User Guide.
Logout	To log out from the Dynamic Activation GUI. After logging out, the logon window shows.

8.1.1.2 Feature Bar

All tabs in the GUI feature bar including their subtabs are shown in Figure 12.



Activation Logic	Activation Logic
	Options
Network Elements	Network Elements
	Network Element Groups
	Routing
	CAI3G DC Routing
System	Licenses
	Options
	Notification E-Mail Configuration
	Synchronize Configuration
Access Control	Users
	Policies
	Attribute Rules
	Administration Domains
Walkthroughs	
Log Management	
Loose Error Handling	

Figure 12 GUI Features

Note: **Log Management** is a link to the **Log Management** GUI which is designed following the latest branding guideline.

Hyperlinks to the feature tabs are reachable from **Site Map**.

8.1.1.3

Working Area

Depending on which tab in the GUI that is selected, the content of this area is changed.

On the GUI front page, a License Capacity Warning table is shown in the working area if there are active license capacity warnings at the moment. The table contains information about License ID, Name of the license and days until the provisioning is stopped.

License capacity warnings

View



License ID	Name	Percent used	Days until blocking provisioning
FAT1023338/9	EMA IMS Core	 106 %	60
FAT1023338/44	EMA 2G 3G	 80 %	











Figure 13 List of License Capacity Warnings

8.1.2







GUI Icons

The common icons used in the Dynamic Activation GUI are shown in Table 3.

Table 3 GUI Icons

Icon	Description
	View Details
	Edit
	Update
	Remove
	Copy
	Undo Change
	Backup
	Restore
 (green)	Activate
 (red)	Deactivate
	Filtering
	Sort Column
	Download
 (green)	Collapse Successful Log



Icon	Description
 (green)	Expand Successful Log
 (red)	Collapse Failed Log
 (red)	Expand Failed Log
	Failed or Suspended
	Successful
	Help text

8.2 Activation Logic Control

This section covers the **Activation Logic** tab in the Dynamic Activation GUI. It consists of the **Activation Logic** and **Options** subtabs.

8.2.1 Activation Logic

The **Activation Logic** subtab contains a list of all Dynamic Activation components, as shown in Figure 14. The following is listed in this tab:

- Standard product activation logics.
- Product customization activation logics.
- Service models.
- Customer adaptation logics that are deployed on the system.

For a list of the components available in the Dynamic Activation standard product, see Section 18 on page 153.

Ericsson Dynamic Activation		ERICSSON	
Operation & Management		About Site Map User Guide Logout	
Activation Logic	Network Elements	System	Access Control
Activation Logic	Options	Walkthroughs	Log Management
Loose Error Handling			
Activation Logic			
View/Edit			
	File	Target Name	Description
	JDV-AAANS-D-Layered-Resource-Provisioning-163.158.jar	AAANS-D Layered Resource Provisioning	Target Component
	JDV-AAANS-D-Monolithic-Resource-Provisioning-163.158.jar	Monolithic AAA Provisioning	Target Component
	JDV-AAANS-D-Service-Provisioning-163.158.jar	AAANS-D Service Provisioning	Target Component
	JDV-AAA-Provisioning-163.158.jar	AAA Provisioning	Target Component
	JDV-AF-Monolithic-Resource-Provisioning-163.158.jar	AF Monolithic Resource Provisioning	Target Component
	JDV-AF-Monolithic-Service-Provisioning-163.158.jar	AF Monolithic Service Provisioning	Target Component
	JDV-AIR-Monolithic-Resource-Provisioning-163.158.jar	AIR Monolithic Resource Provisioning	Target Component
	JDV-AIR-Monolithic-Service-Provisioning-163.158.jar	AIR Monolithic Service Provisioning	Target Component
	JDV-AUC-Massive-Provisioning-163.158.jar	AUC Massive Provisioning	Target Component
	JDV-AUC-Monolithic-Subscriber-Provisioning-163.158.jar	AUC Monolithic Subscriber Provisioning	Target Component
	JDV-AUC-Subscriber-Provisioning-163.158.jar	AUC Subscriber Provisioning	Target Component
	JDV-BCE-Resource-Provisioning-163.158.jar	BCE Resource Provisioning	Target Component
	JDV-BCE-Service-Provisioning-163.158.jar	BCE Service Provisioning	Target Component
	JDV-CA-Provisioning-163.158.jar	ECASCertificate Provisioning	Target Component
	JDV-CG-AUC-CAI-Provisioning-163.158.jar	CG AUC CAI Provisioning	Target Component
	JDV-CG-AUC-Provisioning-163.158.jar	CG AUC Provisioning	Target Component
	JDV-CG-HLR-CAI-Provisioning-163.158.jar	CG HLR CAI Provisioning	Target Component
	JDV-CG-HLR-Provisioning-163.158.jar	CG HLR and M2M Provisioning	Target Component

Figure 14 Activation Logic

The columns can be sorted through the filtering function, which can be useful when the list of **Activation Logic** components is long.

8.2.1.1 Activation Logic Properties

This section contains a table, displaying all the **Configuration Data** properties that exist in the **Activation Logic** subtab.

Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
AllowSipUriWithoutDomain	Indicates whether IMPU without domain is allowed or not. Default value: false <ul style="list-style-type: none">false - IMPU without domain is not allowedtrue - IMPU without domain is allowed	HSS IMS Provisioning
AUTCHOVERMAND	This property enables a check whether AUC subscription data for the new IMSI is mandatory when an initiation of IMSI changeover for an HLR subscription is performed. Value range: 0–1 Default value: 0 0 - AUC subscription data mandatory. 1 - AUC subscription data not mandatory.	CUDB IMSI Changeover Provisioning

**Table 4** *Activation Logic Properties*

Property	Description	Activation Logic ⁽¹⁾
AUTHDMAND	This property enables a check whether the AUC subscription data is mandatory when new HLR subscription data is added to the CUDB. Property value: Value range: 0–1 Default value: 1 0 - AUC subscription data mandatory 1 - AUC subscription data not mandatory	HLR Subscriber Provisioning (applicable for HLR subscription and M2M subscription)
AuthenticationRealm	The authentication realm of HSS. For example, <code>domain.xml</code> . This parameter is empty by default.	Monolithic HSS Provisioning
CAFlag ⁽²⁾	Identifier indicating whether this Activation Logic component is a CA (Customer Adaptation) JDV. Value range: <code>true</code> or <code>false</code>	All activation logics deployed in the system
CentrallmeiDb	This parameter indicates if the “Central IMEI DB” is connected or not. The parameter is checked when equipment objects (<code>imeiData</code>) are created, set, or deleted. Value range: <code>true</code> or <code>false</code> Default value: <code>false</code> <code>true</code> - Central IMEI DB connected <code>false</code> - Central IMEI DB not connected	EIR Provisioning
ChargingTimeZone	The operators timezone deviation in hours and minutes from the UTC. <code>ChargingTimeZone</code> is always preceded by either a “+ ” or “- ” sign. Value Range: <code>[+/-] 0000</code> to <code>[+/-] 2359</code>	AIR Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
CompanySettingName	<p>The name space and name of Company Setting</p> <p>The format of this parameter is <code>x,y;x,y;...</code></p> <p><code>x</code>: Namespace</p> <p><code>y</code>: Parameter name</p> <p>For details on the parameters, refer to BCE-related documents.</p> <p>If <code>companySetting</code> name is configured in the <code>Create</code> request and <code>CompanySettingName</code> is configured on GUI, Dynamic Activation performs the validation:</p> <ul style="list-style-type: none"> If the <code>companySetting</code> name is consistent with the GUI configuration, the provisioning request is sent to BCE. If the <code>companySetting</code> name is not consistent with the GUI configuration, an error is returned. <p>The default value is <code>UP,PNP_ATTACH_CODE_LENGTH;UP,CDG_NO_ANSWER_TIMEOUT;UP,CDG_INTERMITTENT_QUEUE_MESSAGE_INTERVAL;UP,CDG_AGENT_BUSY_TIMEOUT;UP,CDG_AGENT_CANCEL_TIMEOUT;UP,CDG_AGENT_TIMED_OUT_TIMEOUT;UP,CDG_AGENT_UNAVAILABLE_TIMEOUT;UP,AA_TIMEOUT;UP,RESTRICTED_SHORT_NUMBERS_PATTERN;COH,COH_SMS_REMINDER_ENABLED;COH,COH_SMS_REMINDER_TIME_BEFORE_START;COH,COH_MIN_PIN_CODE_LENGTH</code></p>	BCE resource Provisioning
CSPSMAND	<p>This parameter enables a check if the IMSI in HLR subscription must be deleted before deleting AUC subscription data from the CUDB.</p> <p>Value range: <code>true</code> or <code>false</code></p> <p>Default value: <code>false</code></p> <p><code>true</code> - Mandatory</p> <p><code>false</code> - Not mandatory</p>	AUC Subscriber Provisioning (applicable for HLR subscription and M2M subscription)
CertProfile	<p>The certificate profile name that is defined in the ECAS server. It is used when a certificate is signed.</p> <p>For information about the certificate profile, refer to http://ejbca.org/docs/concepts.html#CertificateProfile.</p> <p>Default value: <code>ENDUSER</code></p>	ECAS Provisioning
CertPEMFormat	<p>Indicates if the signed certificate is in the PEM format. Case insensitive <code>YES</code> means true, otherwise it means false.</p> <p>Default value: <code>YES</code></p>	ECAS Provisioning
DisabledPrintoutSuds	<p>This property disables Subscriber Data (SUDs) that are not to be returned in the printout response. The SUD names need to be space separated.</p> <p>Value range: Any simple SUD, for example, <code>CAT</code>, <code>PWD</code>, <code>SCHAR</code>, <code>TSMO</code>, and more.</p> <p>Default value: Empty string, meaning that all SUDs are enabled.</p>	HLR Subscriber Provisioning (applicable for HLR subscription and M2M subscription), HLR Massive Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
DnsDomainCreateCommands ⁽³⁾	<p>The list of CLI command to be sent to IPWorks when adding a domain data.</p> <p>Value range: Any json format string</p> <p>Default value: Empty string</p> <p>Format:</p> <pre>{ "<sequence number 1>": "<dns command>", "<sequence number 2>": "<dns command>", ... }</pre> <p>sequence number - is the order of the dns command send to IPWorks.</p> <p>dns command - is the CLI command send to IPWorks. If the command contains string @DOMAIN@, this string is replaced by the actual Domain Data.</p> <p>For example:</p> <pre>{ "1": "create masterzone iDNS1 @DOMAIN@ -set option=\"notify-source 172.17.4.37\"", "2": "modify masterzone iDNS1 @DOMAIN@ -add AuthoritativeName=\"www.ericsson.com\"" }</pre>	IPWorks/ENUM Provisioning
DnsDomainDeleteCommands ⁽³⁾	<p>The list of CLI command to be sent to IPWorks when removing a domain data.</p> <p>Value range: Any json format string</p> <p>Default value: Empty string</p> <p>Format:</p> <pre>{ "<sequence number 1>": "<dns command>", "<sequence number 2>": "<dns command>", ... }</pre> <p>sequence number - is the order of the dns command send to IPWorks.</p> <p>dns command - is the CLI command send to IPWorks. If the command contains string @DOMAIN@, this string is replaced by the actual Domain Data.</p> <p>For example:</p> <pre>{ "1": "delete masterzone @DOMAIN@ 0.0.4.3.e164.arpa", "2": "delete arecord @DOMAIN@.eric.com;address=10.0.0.2", "3": "delete dnserver dns_U1" }</pre>	IPWorks/ENUM Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
EnumDomain ⁽³⁾	<p>Define the condition to assign the ENUM domain for msisdn or e164.</p> <p>Value range: Any json format string</p> <p>Default value: e164.arpa</p> <p>Empty string means that e164.arpa is used as ENUM domain for all parameters.</p> <p>Format:</p> <pre>{ "msisdn": [{"serie": "<serie value>", "length": <length>, "domain": "<domain value>"} ...], "e164": [{"serie": "<serie value>", "length": <length>, "domain": "<domain value>"} ...] }</pre> <p>serie - the first n digits⁽⁴⁾ of msisdn or e164 ('tel:' and '+' are not counted).</p> <p>length- the length of msisdn or e164.</p> <p>domain- the value of the ENUM domain.</p> <p>domain is assigned when both the serie and length are matched. For regular msisdn or e164(which contains !\.*! in the parameter), it only needs to match the serie and less than or equal to the length.</p> <p>If more than one condition is matched, the first matched domain is to be selected.</p> <p>If no condition is matched, e164.arpa is to be assigned.</p> <p>For example:</p> <pre>{ "msisdn": [{"serie": "123", "length": 11, "domain": "msisdn.arpa.a"}], "e164": [{"serie": "123", "length": 11, "domain": "e164.arpa.a"}] }</pre>	IPWorks/ENUM Provisioning
ErrorCodeMapping	<p>Specifies the error code mapping for MTAS provisioning.</p> <p>Value range: 1 or 2. Default value is 2.</p> <p>If value 1 is set, the following applies (for keeping backward compatibility):</p> <ul style="list-style-type: none"> - When MTAS sends fault code between 1001-2999, Dynamic Activation replies with response code 2002. - When MTAS sends fault code between 3000-3999, Dynamic Activation replies with response code 36501. - When MTAS sends any other fault codes, Dynamic Activation replies with response code 36502. <p>If value 2 is set, the following applies, for elaborating error mapping:</p> <ul style="list-style-type: none"> - When MTAS sends fault code 3002, Dynamic Activation replies with response code 36503. - When MTAS sends fault code 3013, Dynamic Activation replies with response code 36504. - When MTAS sends any other fault codes, Dynamic Activation replies as described above for value 1. <p>For more information about error code description, refer to <i>MTAS Provisioning over CAI3G</i>, Reference [7].</p>	MTAS Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
ExARD	<p>This property indicates which one of the following two parameters is used for the access restriction in the inbound interface:</p> <ul style="list-style-type: none">• <code>AccessRestriction</code> for HSS 11B• <code>ExtendedAccessRestriction</code> for HSS 12A and onwards <p>Value range: <code>true</code> or <code>false</code>.</p> <p>Default value: <code>true</code></p> <p><code>true</code> - Use <code>ExtendedAccessRestriction</code> in the inbound interface to provision HSS 12A and onwards.</p> <p><code>false</code> - Use <code>AccessRestriction</code> in the inbound interface to provision HSS 11B.</p>	HSS EPS Provisioning
ExAssociationId	<p>This property controls the maximum length of <code>associationId</code> attribute:</p> <ul style="list-style-type: none">• <code>false</code> - No extensional ID is used. Maximum length of an association ID is 32 characters. <p>The default value is <code>false</code>.</p> <p>Note: Contact Ericsson support organization if <code>ExAssociationId</code> needs to be changed. <code>ExAssociationId</code> attribute value must be coordinated with service logic implemented in other nodes. This value must not be modified if there is maiden installations or new migrations from Monolithic systems.</p>	HSS IMS Provisioning
ExMaxNumberOfContacts	<p>This property indicates which one of the following two ranges is used for the maximum number of contacts in the inbound interface:</p> <p>1–5 and default value 1 for HSS 12B</p> <p>1–200 for HSS 14A and onwards</p> <p>Value range: <code>true</code> or <code>false</code></p> <p>Default value: <code>true</code></p> <p><code>true</code> - Use maximum number of contacts with range [1-200] in the inbound interface to provision HSS 14A and onwards.</p> <p><code>false</code> - Use maximum number of contacts with range [1-5] and default value 1 in the inbound interface to provision HSS 12B.</p>	HSS IMS Provisioning
ExValidation	<p>Enables or disables support for password encryption.</p> <p>Value range: <code>true</code> or <code>false</code></p> <p>Default value: <code>true</code></p> <p><code>true</code> - support for password encryption is enabled.</p> <p><code>false</code> - support for password encryption is disabled.</p> <p>Must be set to <code>true</code> when HSS validator is corresponding to the following HSS-FE releases:</p> <ul style="list-style-type: none">• 12A R5F or higher• 12B R6D/1 or higher• 14A R1A or higher	HSS Provisioning IMS



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
EntityProfile	<p>The End Entity Profile name that is defined in the ECAS server. It is used when a certificate is signed.</p> <p>For information about the End Entity Profile, refer to http://ejbca.org/docs/concepts.html#EndEntityProfile</p> <p>Default value: EMPTY</p>	ECAS Provisioning
FamilyProvisionTowardsCUDB	<p>Indicates whether SAPC family data provisions to CUDB or not when routing CUDB_SAPC and SAPC are both configured.</p> <ul style="list-style-type: none"> • NO - SAPC family data provisions to SAPC-FE • YES - SAPC family data provisions to CUDB <p>Default value: NO</p>	SAPC Service Provisioning
GetCompanySetting	<p>The parameter value is Yes or No, which is case insensitive:</p> <ul style="list-style-type: none"> • Yes: In getCompanyResponse, Dynamic Activation returns the companySetting information according to the CompanySettingName configuration; • No: In getCompanyResponse, Dynamic Activation does not return the companySetting information. <p>Default value: No.</p>	BCE resource Provisioning
GenericEricssonNonSIMSolution	<p>Generic Ericsson HSS data model without the xB2BUA deployment.</p> <p>Value: YES or NO</p> <p>Default value: YES</p> <p>If the value is set to YES, the VoWifiService interface (Create/Set/Delete) is used for provisioning of AAA, HSS, and Ericsson Certificate Authority Server (ECAS).</p> <p>If the value is set to NO, the NonSIMHSSUser interface (Set) is used for provisioning of HSS. And the VoWifiService interface (Create/Set/Delete) is used for provisioning of AAA and ECAS.</p>	Wi-Fi Calling for Multiple Device Voice over Wi-Fi Subscription



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
HLRNotificationPendBlock	Enable or disable the Data Consistency Assurance in Core Network and CUDB feature. If enabled, Dynamic Activation blocks an HLR provisioning command if there is already a pending notification in progress. Dynamic Activation retries the blocked provisioning command several times, until the previous one is finished. Value range: disabled and enabled Default value: disabled	HLR Subscriber Provisioning, HLR Massive Provisioning
HLRNotificationNumberOfRetries	The maximum number of retries for Dynamic Activation to send the blocked provisioning command towards the HLR. Value range: 0–10 Default value: 5	
HLRNotificationRetryFactor	Specifies the factor for extending the waiting time before each retry, so these retries can have increasing intervals. Value range: 1–10 Default value: 2	
HLRNotificationWaitTime	Specifies the timer (in ms) for calculating intervals of the retries towards the HLR. Value range: 0–120000ms (2 mins) Default value: 2000ms	
HLRNotificationTimeout	Specifies for how long a pending HLR Notification blocks new provisioning commands. When the time-out is exceeded, Dynamic Activation continues the corresponding provisioning command. Value range: 0–120000ms (2 mins) Default value: 62000ms (62s)	
HSSSubscriberFormat	The subscriber ID format of HSS. Value: The correct format used for the monolithic HSS subscriber ID, which is used for Ericsson Non-SIM in the HSS IMPI operation. Default value: <imsi>@<domain>	Wi-Fi Calling for Multiple Device Voice over Wi-Fi Subscription
IssuerDN	The CA's Distinguish Name (DN) created in ECAS, which is used to sign the certificate. Ensure that the CA name must be as same as the Common Name (CN) of DN when creating a CA in ECAS. This configuration is used for ECAS provisioning if the CA3G request does not contain the IssuerDN.	ECAS Provisioning
MaxParallelRequests ⁽⁵⁾	Specifies how many subscribers are updated in parallel when a massive update command is executed. Value range: 1–1024 Default value: 10 MaxParallelRequests has to have a value lower than the total pool size.	AUC Massive Provisioning, HLR Massive Provisioning, HSS EPS Massive Provisioning, MNP Provisioning, M2M Profile Provisioning, M2M Service Profile Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
MaxRetries	<p>The maximum number of retries for an LDAP operation to CUDB when an LDAP Collision (CDC) occurs.</p> <p>Value range: 0–65535</p> <p>Default value: 10</p>	<p>AUC Massive Provisioning, AUC Subscriber Provisioning (applicable for HLR subscription and M2M subscription), CUDB Subscriber Provisioning, HLR Massive Provisioning, HLR Profile Provisioning, HLR Service Associated Data Provisioning, HLR Subscriber Provisioning (applicable for HLR subscription and M2M subscription), HSS EPS Massive Provisioning, MNP Provisioning, Dynamic Activation Scheduled Procedures, M2M Profile Provisioning, M2M Service Profile Provisioning, SAPC Provisioning, ENUM Layered Resource Provisioning</p>
MaxRetry	<p>The maximum number of times that a JDV request is retried.</p> <p>Value range: 0–10</p> <p>Value 0 or empty indicates that no retries are to be made.</p> <p>If the value is invalid or out of range, it is set to 0.</p> <p>The default value is 3.</p>	Monolithic IPWorks AAANS User Provisioning
MaintenanceMode	<p>Indicates whether AAA is in maintenance mode. In this mode, all AAA commands are rejected by AAA JDV logics with the specific error code 35257.</p> <p>Values: YES or NO, which is case insensitive.</p> <p>If it is set to YES, JDV AAA rejects all the requests.</p> <p>If the value in this field is not YES or NO, it is set to NO.</p> <p>Default value: YES</p>	Monolithic IPWorks AAANS User Provisioning
MNCLength	<p>Specifies the Mobile Network Code length</p> <p>Value range: 2 or 3</p> <p>Default value: 2</p>	CUDB IMSI Changeover Provisioning
NominationList	<p>Specifies which list is the nomination list (0-9) in equipment data.</p> <p>This parameter is checked when equipment objects (imeiData) are created, set, or deleted.</p> <p>Value range: String 0–9</p> <p>Default value: 1</p>	EIR Provisioning
NPOwnNetworkPrefix	<p>The network prefix of the home operator who uses Dynamic Activation</p> <p>Example: 19021902</p> <p>Value pattern: (#1(0 1 2 3 4) [0-9]){1,10}</p> <p>Default value: Empty string, which means that MNP provisioning in HLR provisioning is bypassed.</p>	HLR Subscriber Provisioning (applicable for CAI and CAI3G)
OriginOperatorID	<p>The origin ID of the operator.</p> <p>Default value: operator</p>	AIR Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
ProvisioningUri	The URI used for AIR provisioning. Default value: Air	AIR Provisioning
	The URI used to send provisioning requests Default value: ejbca/ejbcaws/ejbcaws?wsdl	ECAS Provisioning
RetryErrorMessage	The key words list used in error messages. The key words are separated by a #. When an error message contains any words in the list, resend the command to AAA. For example, already exists#No matching object(s) Default value: empty For Failover NE group, the RetryErrorMessage value must contain "Failed to connect to ssh server#Network closed".	Monolithic IPWorks AAANS User Provisioning
RetryInterval	The time (in seconds) to wait before another retry. Only integer value is valid. Value range: 0–10 Value 0 or empty indicates that there is no interval between the retries. If the value is invalid or out of range, it is set to 2.	Monolithic IPWorks AAANS User Provisioning
RevokeCertificateByUserName	Indication for revoking user certificate by username or certificate serial number Values: YES or NO Default value: NO If it is set to YES, the VoWifiService uses username as identity towards ECAS and it revokes all users certificates. If it is set to NO, the VoWifiService uses certificate serial number as identity towards ECAS and it just revokes the user-specific certificate.	Wi-Fi Calling for Multiple Device Voice over Wi-Fi Subscription



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
Rootdn ⁽⁶⁾	<p>The Rootdn is used for creating objects in CUDB from the Dynamic Activation system.</p> <p>Value range: 0–255 characters.</p> <p>Default value: dc=operator, dc=com</p>	<p>AUC Massive Provisioning, AUC Subscriber Provisioning (applicable for HLR subscription and M2M subscription), CUDB IMSI Changeover Provisioning, CUDB Subscriber Provisioning, EIR Provisioning, HLR Massive Provisioning, HLR Profile Provisioning, HLR Service Associated Data Provisioning, HLR Subscriber Provisioning (applicable for HLR subscription and M2M subscription), HSS Provisioning AVG, HSS EPS Massive Provisioning, HSS Provisioning EPS, HSS Provisioning IMS, MNP Provisioning, Dynamic Activation Scheduled Procedures, DAE Provisioning, SAPC Provisioning, AAA Provisioning, M2M Profile Provisioning, M2M Service Profile Provisioning, CUDB SUBDEL Provisioning, ENUM Layered Resource Provisioning, AAANSO Layered provisioning</p>
	<p>The root DN of HSS.</p> <p>The default value is applicationName=HSS,nodeName=jambala.</p>	Monolithic HSS Provisioning of IMS
Routeuserphone	<p>This property indicates whether routing naptrTxt with user=phone. user=phone is added after the naptrTxt and separated by a semicolon ";".</p> <p>Example: !^.*\$!SIP:+12225550189@example.com;user=phone!</p> <p>Value range: 0–1</p> <p>Default value: 0</p> <p>0 - Route NaptrTxt without user=phone.</p> <p>1 - Route NaptrTxt with user=phone. Except if the value of SIP URI contains non-numerical character, it routes NaptrTxt without user=phone.</p>	IPWorks/ENUM Provisioning
ServiceCheckMsisdnCho	<p>This property indicates whether blocking the provisioning for MSISDN Changeover when the subscriber has services other than AUC, HLR, and EPS.</p> <p>Value range: true or false</p> <p>Default value: true</p> <p>true - Block the provisioning.</p> <p>false - Do not block the provisioning.</p>	CUDB IMSI Changeover Provisioning
SubjectDN	<p>The subject DN postfix.</p> <p>CN=username + SubjectDN is used as the default value of subjectDN if the CAI3G request does not contain the SubjectDN.</p>	ECAS Provisioning



Table 4 Activation Logic Properties

Property	Description	Activation Logic ⁽¹⁾
TTL	The default value of Time To Live in seconds of the DNS record. Value range: Integer 0–2147483647	AF Provisioning
UserPasswordEncryption	This parameter shows whether UserPassword is encrypted. Values: YES or NO, which is case insensitive. Default value: YES	Monolithic HSS Provisioning
X3GPPAssertedIdentity	The authentication realm of PGM Document. This is a Tel URL or SIP URL. Default value: sip:4687500061@tcv.ics.se	PGM Document resource Provisioning
Xcaproot	The XCAP root of PGM Document. Default value: services.	PGM Document resource Provisioning

(1) This column shows in which Activation Logic Target a specific property exists.

(2) This is not a configurable property. It is set during deploy time of a component.

(3) If the string or commands contains quote(""), it needs to be escaped by backslash(\).

(4) n is less than or equal to 15 and greater than 0

(5) Increasing the value can affect normal provisioning throughput when a massive update command is executed. This affects only the Payload node that executes the massive update operation.

(6) Make sure that `Rootdn` is the same as for LDAP data source, and matches the configured `Rootdn` value in CUDB. The parameter is case-sensitive.

8.2.1.2 View Activation Logic Properties

To view an activation Logic, follow these steps:

1. Click the **View Details** icon  for the Activation Logic to view.

A new page is displayed, holding information about properties, and values set for the current activation logic. Depending on the Activation Logic, both **Configuration Data** and **Target Data** is shown.

2. Click **Done** if the information stated for this activation logic is accurate.
3. Click **Change This...** to edit the property values. For information on how to edit an activation logic, see Section 8.2.1.3 on page 46.

8.2.1.3 Edit Activation Logic Properties

To change the properties of an Activation Logic, follow these steps:

1. Click the **Change...** icon  for the Activation Logic to modify.

A new page is shown, displaying the **Configuration Data** properties that are possible to modify for the current Activation Logic. For information about the different properties that are possible to modify, see Table 4.

2. Modify the value of the properties as needed.




3. Click **Apply**.

A verification page is displayed. The page shows all the parameters defined for the Activation Logic property. Users can continue to edit the parameters as needed by clicking appropriate icons. If the parameters are correctly set, click **Done**.

8.2.1.4 Back Up Activation Logic Properties

To back up configuration data in Activation Logic, follow these steps:

1. Click the **Backup** icon  for the Activation Logic to back up.

A new page is shown, containing a **Configuration Data Name** text area and a list of the **Configuration Data** properties included in this specific Activation Logic.

2. Label the backup by entering a name in the **Configuration Data Name** text area.
3. Click **Apply**.

A verification page is displayed. The page shows all the parameters defined for the Activation Logic property. Users can continue to edit the parameters as needed by clicking appropriate icons. If the parameters are correctly set, click **Done**.

8.2.1.5 Restore Activation Logic Properties

To restore an Activation Logic, follow these steps:

1. Click the **Restore** icon  for the Activation Logic to restore.

A new page is shown, displaying a scroll-bar containing the Activation Logic backups. And a list of the current **Configuration Data** properties for this specific Activation Logic.

2. Select the desired backup in the scroll-bar.
3. Click **Apply**.

A verification page is displayed. The page shows all the parameters defined for the Activation Logic property. Users can continue to edit the parameters as needed by clicking appropriate icons. If the parameters are correctly set, click **Done**.

8.2.2 Options

Users can change the default setting of the `RootDN` attribute for all applicable components in the **Activation Logic**, and for the `CUDB Lookup`. See Figure 15.



It is possible to override the default setting by updating the components individually. For **Activation Logic** components, see Section 8.2.1.1 on page 35. For the CUDB Lookup, see *Configuration Manual for Subscriber Activation*, Reference [2].

Options

! New value may interrupt provisioning traffic.

Change All RootDN's To:

Apply

Figure 15 Options Window

The following table describes the properties in the **Options** window.

Table 5 Options Configuration

Property	Description
Change All RootDN's To:	The default <code>RootDN</code> value that is to apply for all JDVs in Activation Logic and for CUDB Lookup. ⁽¹⁾

(1) Make sure that `Rootdn` is the same as for LDAP data source, and matches the configured `Rootdn` value in CUDB. The parameter is case-sensitive.

8.3 Network Elements Control

From the **Network Elements** tab, it is possible to administer Network Elements (NE), NE groups, and routing.

8.3.1 Network Elements

From the **Network Elements** subtab it is possible to administer NE configurations, see Figure 16.

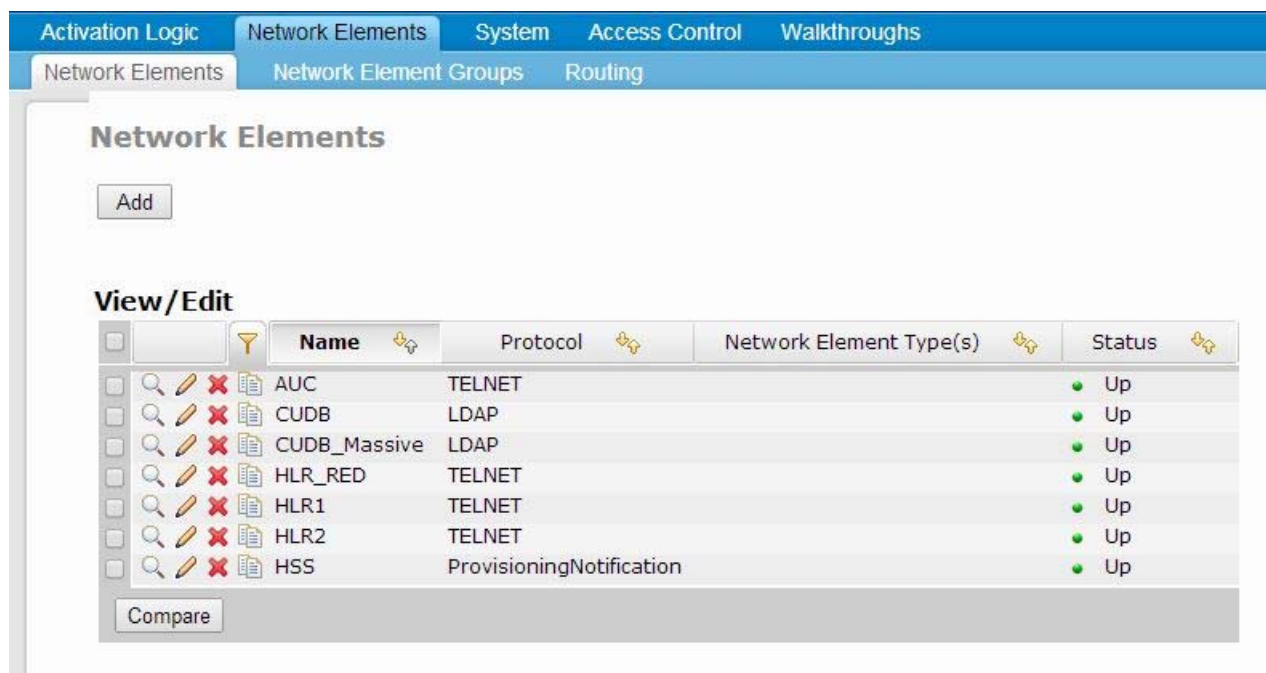


Figure 16 Network Elements Window

In the **Network Elements** page, a table displays all configured NEs. It shows the NE **Name**, **Function(s)**, **Protocol**, and **Status**. Operators can **Add**, **View**, **Copy**, **Edit**, **Remove**, and **Compare** NEs by clicking appropriate icons.

8.3.1.1 Adding Network Elements

To add an NE, follow these steps:

1. Click **Add**.
2. In **Network Elements - Add - Step 1 / 2**, enter the name of the NE in the **Name** field, and select the protocol for the NE from the drop-down list.

By default, the **Active Resource ID** for the NE is assigned.

To change the default **Active Resource ID**, press **Advanced**.

Information about the fields in this page is available in Section 8.3.1.6 on page 51.

Click **Next**.


3. In **Network Elements - Add - Step 2 / 2**, specify the protocol parameters, see Section 8.3.1.6 on page 51. The fields that are available depend on the protocol selected for the NE and on installed features. Information about most common fields is available in Section 8.3.1.7 on page 52.
4. Click **Apply**.



A verification page is displayed. The page shows all the parameters defined for the NE. Users can continue to edit the parameters as needed by clicking appropriate icons. If the parameters are correctly set, click **Done**.

8.3.1.2 Copying Network Elements

To copy an existing NE, follow these steps:

1. Click the copy icon  for the NE to copy.
2. In **Network Elements - Add - Step 1 / 2**, change the name of the NE in the **Name** field. And select the protocol for the NE from the drop-down list.

By default, the **Active Resource ID** for the NE is assigned.

To change the default **Active Resource ID**, press **Advanced**.

Information about the fields in this page is available in Section 8.3.1.6 on page 51.

Click **Next**.

3. In **Network Elements - Add - Step 2 / 2**, change the protocol parameters, see Section 8.3.1.6 on page 51. The fields that are available depend on the protocol selected for the NE and on installed features. Information about most common fields is available in Section 8.3.1.7 on page 52.
4. Click **Apply**.

A verification page is displayed. The page shows all the parameters defined for the NE. Users can continue to edit the parameters as needed by clicking appropriate icons. If the parameters are correctly set, click **Done**.

8.3.1.3 Editing Network Elements

To change the parameters of an NE, follow these steps:

Note: Editing an NE during traffic terminates existing connections and can cause provisioning failures.

1. Click the change icon  for the NE to modify.

A new page is shown, containing the **General**, and the **Protocol parameters** tabs.

2. Click each tab to change parameters as needed.

Information about most common fields is available in Section 8.3.1.6 on page 51.

3. Click **Apply**.




A dialog is displayed stating that the change terminates existing connections and ongoing provisioning traffic for this NE. If the parameters are correctly set, click **OK** to proceed.

8.3.1.4 Removing Network Elements

Note: Before removing an NE, consider the following:

- All requests associated to the NE must be deleted from the Processing Queue. Otherwise the requests remain in the database. For more information, see Section 13.1 on page 119.
- A **Network Element** used in a **Network Element Type** cannot be removed.

To remove an NE, follow these steps:

1. Click the remove icon  for the NE.

A window opens to confirm the remove operation.

2. Click **OK**.

Tips!

If an NE is removed without removing its associated requests first, recreate a new NE with the same name. So you can remove all the requests in the **Processing Queue** GUI.

8.3.1.5 Comparing Network Elements

It is possible to compare two NEs to see the difference between their parameters.

To compare NEs, follow these steps:

1. In the NEs table, select two NEs to compare.
2. Click **Compare**.

A page that shows the parameters of the two NEs side by side is displayed. Information about most common fields is available in Section 8.3.1.6 on page 51.

8.3.1.6 Network Elements Parameters

A Network Element is defined by the following parameters.



Table 6 Network Element Parameters

Parameters	Property	Description
General	Name	The name for the NE. Allowed characters are a-z, A-Z, 0-9, - and _ . White spaces are not considered, they are automatically removed.
	Protocol ⁽¹⁾	The connection protocol for the NE. The following protocols and protocol parameters are included: <ul style="list-style-type: none">• LDAP - For parameters see Section 8.3.1.7.1 on page 53.• Telnet - For parameters see Section 8.3.1.7.2 on page 55.• SSH - For parameters see Section 8.3.1.7.3 on page 56.• Provisioning Notification - For parameters see Section 8.3.1.7.4 on page 58.• CAI3G - For parameters see Section 8.3.1.7.5 on page 59.• HTTP - For parameters see Section 8.3.1.7.6 on page 61.• CF-SSH - For parameters see Section 8.3.1.7.7 on page 62.• DNS - For parameters see Section 8.3.1.7.8 on page 63.
	Version ⁽²⁾	The version of the NE.
	Active Resource ID	Unique identity for the NE used in alarm handling. This parameter is only available in Advanced mode.
	State	The state of an NE. The value can be either Active or Inactive . This parameter is only applicable when NE Group Type Active-Active is used.
	Status	Status of the NE (Up or Down). The value is generated automatically by the system.
	Network Element Type	The NE type to which the NE belongs.

(1) Depending on customer adaptations or installed features, the connection protocols can differ. Only the protocols listed in the column to the right are supported.

(2) Currently only supported for MTAS. For more information, refer to *Configuration Manual for Subscriber Activation, Reference [2]*.

8.3.1.7 Connection Protocol Parameters

The following table describes the connection protocol parameters for all the NEs, including the internal NEs:



Table 7 Connection Protocol Parameters

Parameter	Description
Pool Size	<p>The maximum number of open connections in the pool towards the NE for each PL node.</p> <p>The number of open connections in the pool will vary over time on needed basis.</p> <p>It is suggested to set this parameter to a number not exceeding the expected number of concurrent requests for each PL node.</p> <p>The Pool Size is set for 1x per PL node. For example, if total sessions for an HLR-FE are 20 and two PL blades handles traffic, the Pool Size to configure is $20/2 = 10$.</p> <p>Value range: 1–1024</p> <p>Default value: 10</p> <p>This is a mandatory parameter.</p>
Idle Timeout (minutes)	<p>The maximum time, in minutes, a connection is allowed to be idle (unused) in the pool.</p> <p>A periodic check is performed to find and close timed out connections.</p> <p>Value range: 1–2147483647</p> <p>Default value: 1</p>
Blocking Timeout (ms)	<p>The time, in milliseconds, to wait for a free connection in the pool.</p> <p>Value range: 0–300000</p> <p>Default value: 10000</p> <p>If the time is exceeded, an <code>Out of Resources</code> exception is raised.</p>

8.3.1.7.1

LDAP Connection Protocol Parameters

The following table shows more LDAP connection protocol parameters.

Table 8 LDAP Connection Protocol Parameters

Parameter	Description
Host	<p>IPv4/IPv6⁽¹⁾ address or hostname.</p> <p>The host containing the database.</p>
Port	<p>Defines to which port LDAP listens.</p> <p>Value range: 1–65535</p>
User DN	<p>The username to log on to the database. For example, <code>cn=manager,dc=operator,dc=com</code>.</p>
Heartbeat DN	<p>The distinguished name (DN) that is fetched during heartbeat checks. For example, <code>ou=mscCommonData,dc=operator,dc=com</code></p>
Number of Retries	<p>Number of times that connection is retried, if detected LDAP busy failure.</p> <p>Value range: 0–10</p> <p>Default value: 3</p>



Parameter	Description
Retry Time Interval (ms)	<p>After receiving an LDAP error, this parameter determines how long to wait before trying again. For description of the LDAP error code, refer to <i>Function Specification Resource Activation</i>, Reference [4].</p> <p>Value range: 0–60000</p> <p>Default value: 1000</p> <p>Retry Time Interval (ms) has to have a value lower than Long Retry Time Interval (ms).</p>
Long Retry Time Interval (ms)	<p>After receiving an LDAP error, this parameter determines how long to wait before trying again. For description of the LDAP error code, refer to <i>Function Specification Resource Activation</i>, Reference [4].</p> <p>Value range: 0–180000</p> <p>Default value: 15000</p>
Response Timeout (ms)	<p>Response time-out in milliseconds represents the read time-out for LDAP operations. If the LDAP connector does not get an LDAP response within the specified time, it ends the read attempt. A value less than or equal to zero means no read time-out is specified. This is equivalent to waiting for the response infinitely until it is received.</p> <p>This time-out is not used for detecting long running requests, but rather to ensure that the LDAP server is continuously responding to the LDAP client. This means that a request can be ongoing for several minutes, even if the response time-out is set to just a few seconds, without being ended.</p> <p>Value range: 0–86400000</p> <p>Default value: 11000 ⁽²⁾</p> <p>Value 0 means that the time-out is disabled and can be used for Massive Searches. When Timeout is disabled, there is no guarantee that the connection is closed if there is network disturbance.</p> <p>Response Timeout is recommended:</p> <ul style="list-style-type: none">• To be activated for Individual Provisioning and Massive Updates, that is <code>ResponseTimeout>0</code>.• To be set to a high value for Massive Searches, max value to use is 86400000, which is equivalent to 24 hours.• To be set to a higher value on the tertiary CUDB node in a CUDB Group. This is to avoid all CUDB nodes to be blacklisted if there is slow connections. <p>Note: Too low Response Timeout value for secondary or tertiary CUDB nodes can cause all CUDB nodes to be blacklisted. Response Timeout for secondary and tertiary CUDB nodes must have a sufficient high value, so it can handle single CUDB transactions with longer response time.</p>
Connection Timeout (ms)	<p>Time in milliseconds to wait for a connection attempt to get contact, before ending the attempt.</p> <p>Value range: 0–300000</p> <p>Default value: 11000</p>
Retry Factor	<p>After receiving some communication faults from the LDAP server, Retry Factor together with Number of Retries and Retry Time Interval determines how long to wait before a retry.</p> <p>Value range: ≥ 1</p> <p>Default value: 2</p>



Parameter	Description
Password	The password to log on the database.
Binary Attributes	<p>A list of what LDAP attributes are binary.</p> <p>Default value: Configured for CUDB.</p> <p>For the Binary Attributes parameter, choose the default Configured for CUDB radio button.</p>

(1) IPv6 is not valid for Native and CEE deployments.

(2) The default value is based on the Open Shortest Path First (OSPF) dead time-out to avoid premature failover or blacklisting.

8.3.1.7.2

Telnet Connection Protocol Parameters

The following table shows more telnet connection protocol parameters.

Table 9 Telnet Connection Protocol Parameters

Parameter	Description				
Host	<p>IPv4/IPv6⁽¹⁾ address or hostname.</p> <p>The host containing the telnet server.</p>				
Port	<p>Defines to which port telnet listens.</p> <p>Value range: 1–65535</p>				
username	The username to log on to the telnet server.				
Password	The password for the telnet server.				
Login Process	<p>Write the logon output followed by #. This must then be followed by the password output, followed by #. If there is any new output between the password output and the prompt, add that output followed by #.</p> <p>For example:</p> <table> <tr> <td>Telnet Login</td><td>Login Process⁽²⁾</td></tr> <tr> <td> <pre>login: admin1 loginack passw: ***** pswack <</pre> </td><td> <pre>log in:#passw:#pswack#. ⁽³⁾</pre> </td></tr> </table>	Telnet Login	Login Process ⁽²⁾	<pre>login: admin1 loginack passw: ***** pswack <</pre>	<pre>log in:#passw:#pswack#. ⁽³⁾</pre>
Telnet Login	Login Process ⁽²⁾				
<pre>login: admin1 loginack passw: ***** pswack <</pre>	<pre>log in:#passw:#pswack#. ⁽³⁾</pre>				
Prompt	The prompt output on the telnet server, for example, <.				
Response Timeout (ms)	<p>Time in milliseconds to wait for a response after sending a request.</p> <p>Value range: 0–300000</p> <p>Default value: 11000⁽⁴⁾</p>				
Connection Timeout (ms)	<p>Time in milliseconds to wait for a connection attempt to get contact before the attempt is aborted.</p> <p>Value range: 0–300000</p> <p>Default value: 11000</p>				
Number of Retries	<p>Number of times that connection is retried, if detected telnet busy failure.</p> <p>Value range: 0–10</p> <p>Default value: 3</p>				



Parameter	Description
Function Busy Timer (ms)	After receiving a <code>Function Busy</code> response from the <code>telnet</code> server, this parameter determines how long to wait before trying again. The unit is milliseconds. Value range: 0–60000 Default value: 1000
Retry Factor	After receiving a <code>Function Busy</code> response from the <code>telnet</code> server, <code>Retry Factor</code> together with <code>Number of Retries</code> and <code>Function Busy Timer</code> determines how long to wait before a next try. Value range: ≥ 1 Default value: 2
Long Retry Time Interval (ms)	After receiving a broken connection from the HLR, this parameter determines how long to wait before trying again. Value range: 0–180000 Default value: 15000

(1) IPv6 is not valid for Native and CEE deployments.

(2) If using an APG43L, the Login Process is either `login:##Password:##`, or `login:#Password:`

(3) The “.” at the end of the line is mandatory. The Dynamic Activation cannot log in to the HLR-FE node/s if the “.” is missing.

(4) The default value is based on the Open Shortest Path First (OSPF) dead time-out to avoid premature failover or blacklisting.

8.3.1.7.3

SSH Connection Protocol Parameters

The following table shows more SSH connection protocol parameters.

Table 10 SSH Connection Protocol Parameters

Parameter	Description
Host	IPv4/IPv6 ⁽¹⁾ address or hostname. The host containing the SSH server.
Port	Defines to which port SSH listens. Value range: 1–65535
username	The username to log on to the SSH server.
Password	The password for the SSH server.
Private Key	The Private Key for SSH communication with SSH server. Public key is used to authenticate with external SSH server, and Public Key is created based on the Private Key. Private Keys must not be shared with the external SSH server.



Parameter	Description		
Login Process	Write the logon output followed by #. This must then be followed by the password output, followed by #. If there is any new output between the password output and the prompt, add that output followed by #.		
	For example:		
	SSH logon	Login Process	
	login: admin1 loginack passw: ***** pswack <	login:#passw:#pswack#. ⁽²⁾	
App username	The application username for logon procedure.	These attributes are used for IPWorks only.	
App Password	The application user password for logon procedure.		
App Command	The application initiating or starting up command.		
App Login Procedure Prompt	The displayed prompt the application print during the logon procedure.		
	For example:		
	SSH logon	Login Process	
	\$ ssh -l actadm <IP address of IPWorks> Password: Last login: Thu Jul 2 10:00:00 2015 from <IP address of the login user> \$ ipwcli IPWorks>Login : admin IPWorks>P assword: ***** Login to server succ essful.	Last login #IPWorks> Login:#IPWorks> Password:#Login to server successful	
Line Termination Character	The Line Termination Character of application commands output during the command interaction.		
	Default value: \n		
Prompt	The prompt output on the SSH server, for example, <.		
Response Timeout (ms)	Time in milliseconds to wait for a response after sending a request.		
	Value range: 0–300000		
	Default value: 11000 ⁽³⁾		



Parameter	Description
Connection Timeout (ms)	Time in milliseconds to wait for a connection attempt to get contact before the attempt is aborted. Value range: 0–300000 Default value: 11000
Number of Retries	Number of times that connection is retried, in case of detected SSH busy failure. Value range: 0–10 Default value: 3
Function Busy Timer (ms)	After receiving a <code>Function Busy</code> response from the SSH server, this parameter determines how long to wait before trying again. The unit is milliseconds. Value range: 0–60000 Default value: 1000
Retry Factor	After receiving a <code>Function Busy</code> response from the SSH server, Retry Factor, Number of Retries, and Function Busy Timer determine how long to wait before a retry. Value range: ≥ 1 Default value: 2
Long Retry Time Interval (ms)	After receiving a broken connection from the NE, this parameter determines how long to wait before trying again. The optimal value can be different for different NEs. Value range: 0–180000 Default value: 15000

(1) IPv6 is not valid for Native and CEE deployments.

(2) The “.” at the end of the line is mandatory. The Dynamic Activation cannot log on to the HLR-FE node/s if the “.” is missing.

(3) The default value is based on the Open Shortest Path First (OSPF) dead time-out to avoid premature failover or blacklisting.

8.3.1.7.4 Provisioning Notification Protocol Parameters

Provisioning Notification is a module used for notifying front ends after successful provisioning to CUDB.

The Provisioning Notification module uses SOAP over HTTP as protocol and the following table show more connection protocol parameters.



Table 11 Provisioning Notification Protocol Parameters

Parameter	Description
The end point URL for the notification service	<p>The URL endpoint syntax is as follows:</p> <pre>http://<IPv4 address, IPv6 address, or hostname>:<port number>/<service>⁽¹⁾⁽²⁾</pre> <p>The following are URL examples for IMS and EPS:</p> <pre>http://<HSS_OAM_VIP>:<Configured_Port_x>/HssIsmSdaUdcWS/services/NotificationService http://<HSS_OAM_VIP>:<Configured_Port_y>/HssEsmUdcWS/services/NotificationService</pre> <p>Where:</p> <p><HSS_OAM_VIP> – Can be a hostname or an IPv4/IPv6 address.⁽¹⁾</p> <p><Configured_Port_n> – Can be obtained from the configurable attributes of the HSS node:</p> <ul style="list-style-type: none"> • In case of HSS-FE, the attributes are hss-SoapNotificationsPort for IMS provisioning, and hss-EsmSoapNotificationsPort for EPS provisioning. • In case of HSS/SLF, the attributes are HSS-SoapNotificationsPort for IMS provisioning, and HSS-EsmSoapNotificationsPort for EPS provisioning.
The end point URL for the heartbeat procedure	<p>The URL endpoint syntax is as follows:</p> <pre>http://<IPv4 address, IPv6 address, or hostname>:<port number>/<service>?wsdl⁽¹⁾⁽²⁾</pre> <p>Note: wsdl file is downloaded for each heartbeat attempt.</p> <p>The following are URL examples for IMS and EPS:</p> <pre>http://<HSS_OAM_VIP>:<Configured_Port_x>/HssIsmSdaUdcWS/services/NotificationService?wsdl http://<HSS_OAM_VIP>:<Configured_Port_y>/HssEsmUdcWS/services/NotificationService?wsdl</pre> <p>Where:</p> <p><HSS_OAM_VIP> – Can be a hostname or an IPv4/IPv6 address.⁽¹⁾</p> <p><Configured_Port_n> – Can be obtained from the configurable attributes of the HSS node:</p> <ul style="list-style-type: none"> • In case of HSS-FE, the attributes are hss-SoapNotificationsPort for IMS provisioning, and hss-EsmSoapNotificationsPort for EPS provisioning. • In case of HSS/SLF, the attributes are HSS-SoapNotificationsPort for IMS provisioning, and HSS-EsmSoapNotificationsPort for EPS provisioning.
The number of attempts to resend in case of a connection level error	<p>Number of times that the connection is retried when connection error occurs.</p> <p>Value range: 0–10</p> <p>Default value: 3</p>
The interval (ms) between the retry attempts	<p>The waiting time between retries for connection,</p> <p>Value range: 0–60000</p> <p>Default value: 1000</p>

(1) IPv6 is not valid for Native and CEE deployments. The IPv6 address needs to be specified within brackets [IPv6 address].

(2) IP address and port number must be the same for the end-point URL for the notification service and the end-point URL for the heartbeat procedure.



8.3.1.7.5 CAI3G Connection Protocol Parameters

The following table shows more CAI3G connection protocol parameters.

Table 12 CAI3G Connection Protocol Parameters

Parameter	Description
SSL/TLS	If checked, SSL/TLS is used as the lower-level protocol. By default using HTTP as low-level protocol.
Request Traffic URL	A full URL used for sending requests. The URL syntax is as follows: <code>http://<IPv4 address⁽¹⁾, IPv6 address, or hostname>:<port number>/<service></code>
Heartbeat URL	A full URL used for sending heartbeat requests. The URL syntax is follows: <code><Request Traffic URL>/CAI3G?wsdl</code> If the Heartbeat URL is not configured, the status of the NE is Up.
The User ID to use for CAI3G Login	Username for the Login request.
The Password to use for CAI3G Login	Password for the Login request.
Number of Retries	Number of times that connection is retried, in case of detected function busy failure. Value range: 0-10. Default value: 3
Retry Time Interval (ms)	After receiving the function busy response from server, this parameter determines how long to wait before trying again. The unit is milliseconds. Value range: 0-60000 Default value: 1000
Session Control URL ⁽²⁾	A full URL used for sending session control requests (login or logout). The URL syntax is the same as the one for Request Traffic URL. This URL can be the same as Request Traffic URL, or a different URL can be used.
WS-Security Mode ⁽²⁾	WS-Security authentication for the subscription request. It provides a UsernameToken as a means of identifying the request by username, and optionally using a password (or public key, or password equivalent) to authenticate that identity to the web service producer.
authentication username / password text ⁽³⁾	UsernameToken and password are in plain text



Parameter	Description
authentication username / password digest ⁽³⁾	UsernameToken and password are in the format of digest. A digest password is produced by hash method by a given username, realm, and password.
Carry LogId	Request carries the Log ID of the local Dynamic Activation in the SOAP header to the remote CAI3G server.

(1) IPv6 is not valid for Native and CEE deployments. The IPv6 address needs to be specified within brackets [IPv6 address].

(2) The Session Control URL and WS-Security Mode are alternative parameters. When the WS-Security Mode is selected, Session Control URL cannot be specified.

(3) The authentication format of WS-Security, which can be set only when the WS-Security mode is selected.

8.3.1.7.6

HTTP Connection Protocol Parameters

The following table shows more HTTP connection protocol parameters.

Table 13 HTTP Connection Protocol Parameters

Parameter	Description
Host	The IPV4/IPV6 ⁽¹⁾ address or hostname
Port	The port to which HTTP listens Value range: 1–65,535
Agent	The HTTP agent name
The URI used to test the connectivity	The URI to test the connectivity between Dynamic Activation and NE nodes. For example, up/UnifiedProvisioningService
Content Encoding	The content encoding Value range: enumeration value="deflate", "gzip", "none" For example: none
Secure	Support for security consideration
CA ⁽²⁾ used to validate server	Trust store for the validation of the server certificate.
CA ⁽²⁾ file password	The password of the trust store.
Mutual authentication (Two-way handshake)	Indicates whether the connection needs two-way SSL.
Client certificate used in mutual authentication	The key store contains client certificate.
Client certificate file password	The password of the Key Store P12 file is supported.
Authentication Method	The method of Authentication Value range: enumeration value="basic", "none" For example: none
HTTP Username	The username to log onto the http server
HTTP Password	The password to log onto the http server



Parameter	Description
Customized Heartbeat	Support for HTTP post heartbeat
HTTP Post Body	HTTP post request body

(1) IPv6 is not valid for Native and CEE deployments.

(2) Certificate Authority

8.3.1.7.7

CF-SSH Connection Protocol Parameters

The following table shows more CF-SSH connection protocol parameters.

Table 14 CF-SSH Connection Protocol Parameters

Parameter	Description
Host	IPv4/IPv6 ⁽¹⁾ address or hostname. The host containing the SSH server.
Port	Defines to which port SSH listens. Value range: 1–65535. Default value: 22
username	The username to log on to the SSH server.
Password	The password for the SSH server.
Key	The Private Key for SSH communication with SSH server. Public key is used to authenticate with external SSH server, and Public Key is created based on the Private Key. Private Keys must not be shared with the external SSH server.
Subsystem	Key for the term environment variable. If not set, vt100 is used.
Version of NE	The version of the data source, configured in the JDV. The CF-SSH connector is only applicable for ENUM/IPWorks functionality, and the version to use can be found in <i>Configuration Manual for Subscriber Activation</i> , Reference [2].
Prompt	The prompt output on the SSH server, for example, >. Default value: >
Line Termination Character	The Line Termination Character of application commands output during the command interaction. Default value: \n
Response Timeout (ms)	Time in milliseconds to wait for a response after sending a request. Value range: 1–300000. Default value: 11000 ⁽²⁾ .
Connection Timeout (ms)	Time in milliseconds to wait for a connection attempt to get contact before the attempt is aborted. Value range: 1–300000. Default value: 11000
Number of Retries	Number of times that connection is retried, in case of detected SSH busy failure. Value range: 0–10. Default value: 3



Parameter	Description
Retry Factor	After receiving a Function Busy response from the SSH server, Retry Factor together with Number of Retries, and Function Busy Timer determines how long to wait before a retry. Value range: ≥ 1 . Default value: 2
Long Retry Time Interval (ms)	After receiving a broken connection from the remote node, this parameter determines how long to wait before trying again. Value range: 0–180000 Default value: 15000
App username	The application username for logon procedure.
App Password	The application user password for logon procedure.
App Command	The application initiating or starting up command.
App Login Procedure Prompt	The displayed prompt that the application is printing during the logon procedure. For example:
	SSH logon
	Login Process
	<pre> \$ ssh -l actadm <IP address> Password: Last login: Thu Jul 2 10:00:00 2015 from <IP address of the login user> \$ ipwcli Prompt>Login: admin Prompt>Password: ***** Login to server successful. </pre>

(1) IPv6 is not valid for Native and CEE deployments.

(2) The default value is based on the Open Shortest Path First (OSPF) dead time-out, to avoid premature failover or blacklisting.

8.3.1.7.8

DNS Connection Protocol Parameters

The following table shows more DNS connection protocol parameters.

Table 15 DNS Connection Protocol Parameters

Parameter	Description
Domain	The domain used to resolve user account information.
Name Servers	IPv4/IPv6 ⁽¹⁾ address or hostname of name server. .
Response Timeout (ms)	Defines how long (in milliseconds) Dynamic Activation waits for a response from the NE before it times out. Value range: 0 to 99999999. Default value: 60000

(1) IPv6 is not valid for Native and CEE deployments.



8.3.1.7.9 CF-HTTP Connection Protocol Parameters

The following table shows more CF-HTTP connection protocol parameters.

Table 16 CF-HTTP Connection Protocol Parameters

Parameter	Description
Host	The IPV4/IPV6 ⁽¹⁾ address or hostname
Port	The port to which HTTP listens Value range: 1–65,535
Auth username	The username of basic access authentication
Auth password	The password of basic access authentication
Base Uri	The base URI of REST For example, /provisioning/v1
HeartBeat Uri	The URI to perform heart beat (HTTP GET). For example, /provisioning/v1/dataplans/global
HeartBeat accepted response code	The accepted HTTP status code from heartbeat Default value: 201,404,414,500
Secure	Indicates whether to use secure communication (HTTPS) Default value: false
Key store file	The key store that contains client certificate.
Key store file password	The password of the Key Store P12 file that is supported
Mutual authentication	Indicates whether the mutual authentication (two-way hand shake) is allowed Default value: false
Trust store file	The trust store for the validation of the server certificate
Trust store file password	The password of the trust store
Version of NE	The version of the data source, configured in the JDV. The CF-HTTP connector can be used for: <ul style="list-style-type: none">• Monolithic SAPC 17A. The value is 17.• SAPC 1 and later versions for both Monolithic and Layered SAPC. For example, the value is 1.

(1) IPv6 is not valid for Native and CEE deployments.

8.3.1.7.10 AIR-Connector Connection Protocol Parameters

The following table shows more AIR-Connector connection protocol parameters.

Table 17 AIR-Connector Connection Protocol Parameters

Parameter	Description
Host	The IPV4/IPV6 ⁽¹⁾ address or hostname



Parameter	Description
Port	The port to which HTTP listens Value range: 1–65,535
Agent	The HTTP agent name
Auth user name	The username of basic access authentication
Auth password	The password of basic access authentication
Base Uri	The base URI of REST The final URI format for AIR provisioning is <code><Base URI><Provisioning URI></code> The <code><Provisioning URI></code> is an activation logic property. For detailed information, refer to Section 8.2.1.1 on page 35. For example, if Base URI is <code>/CS</code> and Provisioning URI is <code>/Air</code> , the endpoint of AIR provisioning is <code><Host>:<Port>/CS/Air</code>
HeartBeat Uri	The URI to perform heart beat (HTTP POST). The final URI format for heart beat is <code><Heartbeat URI></code> For example, if Heartbeat URI is <code>/CS</code> , the endpoint of heart beat is <code><Host>:<Port>/CS</code>
HeartBeat Post Body	The HTTP body to perform heart beat (HTTP POST). For example, <code><methodCall><methodName>GetCapabilities</methodName><params><param><value><struct></struct></value></param></params></methodCall></code>
HeartBeat accepted response code	The accepted HTTP status code from heartbeat Default value: 201,404,414,500
Secure	Indicates whether to use secure communication (HTTPS) Default value: <code>false</code>
Key store file	The key store that contains client certificate.
Key store file password	The password of the Key Store file that is supported
Mutual authentication	Indicates whether the mutual authentication (two-way hand shake) is allowed Default value: <code>false</code>
Trust store file	The trust store for the validation of the server certificate
Trust store file password	The password of the trust store
Version of NE	The version of the data source, configured in the JDV. The AIR connector can be used for AIR version CS6, CS16 and CS17.

(1) IPv6 is not valid for Native and CEE deployments.

8.3.2 Network Element Groups

From the **Network Element Groups** it is possible to administer routing to NE type, see Figure 17. To upload the default NE groups, refer to *System Administrators Guide for Native Deployment*, Reference [5]



Ericsson Dynamic Activation
Operation & Management

ERICSSON

About Site Map User Guide Logout

Activation Logic Network Elements System Access Control Walkthroughs Log Management Loose Error Handling

Network Elements Network Element Groups Routing CAI3G DC Routing

Network Element Groups

Add

View/Edit

	Name	Group Type	Network Element Type	Status
	AAANSND-NOTIFICATION-GROUP	Active-Active	AAA_FE_NSD	Ok
	AUCFE-MASSIVE-UPDATE-GROUP	Round-Robin	AUC_MASSIVE_UPDATE	Empty
	AUCFE-VALIDATION-GROUP	Round-Robin	AUC_VALIDATION	Empty
	CUDB-AUTO-REPLAY-GROUP	Failover		Empty
	CUDB-GROUP	Failover	CUDB, CUDB_AAA, CUDB_EIR, CUDB_HLR, CUDB_HLR_MNP, CUDB_SAPC, CUDB_DAE, CUDB_AAA_NSD, CUDB_MASSIVE_SEARCH, CUDB_AAA_MASSIVE_SEARCH, CUDB_EIR_MASSIVE_SEARCH, CUDB_HLR_MASSIVE_SEARCH, CUDB_HLR_MNP_MASSIVE_SEARCH, CUDB_SAPC_MASSIVE_SEARCH, CUDB_HLR_MASSIVE_UPDATE	All Blacklisted Empty
	CUDB-MASSIVE-OPER-GROUP	Failover		Empty
	CUDB-MASSIVE-UPDATE-GROUP	Failover		Empty
	DAE-NOTIFICATION-GROUP	Round-Robin	DAE_NOTIFICATION	Empty
	HLRFE-GROUP	Round-Robin	HLR_COMMON_DATA	Empty
	HLRFE-MASSIVE-UPDATE-GROUP	Round-Robin	HLR_MASSIVE_UPDATE	Empty
	HLRFE-VALIDATION-GROUP	Round-Robin	HLR_MNP, HLR_RED, HLR_VALIDATION	Empty
	HSSFE-AVG-NOTIFICATION-GROUP	Round-Robin	HSS_FE_AVG	Empty
	HSSFE-EPS-NOTIFICATION-GROUP	Round-Robin	HSS_FE_EPS	Empty
	HSSFE-IMS-NOTIFICATION-GROUP	Round-Robin	HSS_FE_IMS	Empty
	M2MFE-GROUP	Round-Robin	M2M_COMMON_DATA	Empty
	M2M-HLR-VALIDATION-GROUP	Round-Robin	M2M_HLR_RED, M2M_HLR_VALIDATION	Empty
	MTAS-GROUP	Round-Robin	MTAS	Empty
	MTAS-SIPTRUNKING-GROUP	Round-Robin	MTAS_SIPTrunking	Empty

Figure 17 Network Element Groups Window

In **Network Elements Groups**, a table displays all configured NE groups. It shows the group name, the group type, the Network Elements Type, and the group status. It is possible to **Add**, **View**, **Edit**, and **Remove** routing for NE types by clicking appropriate icons. It is also possible to add or remove NEs from NE groups.



8.3.2.1 Adding a Network Element Group

New groups can be created, although this can be unnecessary. To add a new group, complete the following steps. For information about the parameters to be specified, see Table 18.

1. Click **Add**.
2. In **Network Element Groups - Add - Step 1 / 2**, type the group name and select the group type. Click **Next**.
3. In **Network Element Groups - Add - Step 2 / 2**, select the NEs to include in the group. For Round-Robin, assign **Weight**, for Failover assign **Order** to the selected NEs.
4. Click **Apply**.

An `Add operation successful` page is displayed. The page shows all the parameters defined for the NE group. Users can continue to change the parameters as needed by clicking the appropriate icons. If the parameters are set correctly, click **Done**.

8.3.2.2 Editing a Network Element Group

Users can add NEs to or remove NEs from a Network Element group.

To edit a Network Element Group, follow these steps:

1. Click the change icon  for the group to modify.

A page with **General** and **Network Elements** tabs is shown.

2. To add or remove NEs, go to the **Network Elements** tab and change the settings as desired.
3. Click **Apply**.

8.3.2.3 Removing a Network Element Group

Note: Before removing the NE Group, remove all the NEs from the group.

To remove a Network Element Group, follow these steps:

1. Click the remove icon  for the Network Element Group.

A window opens to confirm the remove operation.

2. Click **OK**.

8.3.2.4 Network Element Group Parameters

A Network Element Group is defined by the following parameters.



Table 18 Network Element Group Parameters

Parameter	Description
Name	The name for the NE group.
Group Type	<p>The algorithm that is to be used by the group to distribute the requests between the NEs in the group. The possible choices are <code>Round Robin</code> and <code>Failover</code>.</p> <p>Note: This parameter can only be set during creation of the group. The only way to change the type of a group is to delete it and recreate it again with the correct type.</p> <p><code>Round Robin</code> - A load sharing algorithm that distributes the requests among all the available NEs according to their weight factor (see parameter <code>Weight</code>).</p> <p><code>Failover</code> - An algorithm that always sends the requests to a primary NE as long as it is available. If the primary NE is not available, the group can have multiple stand-by NEs. The <code>Order</code> parameter decides in which order the NEs must be chosen (see parameter <code>Order</code>).</p> <p><code>Active-Active</code> - An algorithm that sends the requests to all active NEs in the group and is only supported by NE type <code>AAA_FE_NSD</code>.</p>
Status	<p>The status for an NE group.</p> <p><code>OK</code> = All NEs belonging to this group are working properly.</p> <p><code>Empty</code> = This group has no NEs.</p> <p><code>All Blacklisted</code> = All NEs connected to this Group are unusable. Check the NEs for alarms to identify what is wrong. Once the faulty NEs can be used again, the group status automatically changes.</p> <p><code>Partly Blacklisted</code> = At least one of the NEs belonging to this group is unusable. Go to the Network Elements tab to see which NEs are down. Check the NEs for alarms to identify what is wrong. Once the faulty NEs can be used again, the group status automatically changes.</p>
NE Type	The NE type to which the NE group belongs to, see <i>Configuration Manual for Subscriber Activation</i> , Reference [2].
Weight	<p>For the <code>Round-Robin</code> distribution type, the weight factor is used to balance the load among NEs in an NE group. For example, if there are three active NEs with weight factors 1, 4 and 5, the data is distributed as follows:</p> <ul style="list-style-type: none">• 10% (1/10) for the first NE• 40% (4/10) for the second NE• 50% (5/10) for the third NE <p>Value range: 1–100</p>
Order	<p>For the <code>Failover</code> group type, the order number is used to decide in which order the group must try the different NEs.</p> <p>A <code>Failover</code> group always choose the NE that is available (Status is <code>Up</code>) and has the lowest order to handle the request.</p>

8.3.3

Routing

From **Routing** it is possible to administer relations between NE and NE Types and Routing Methods, see Figure 18. To configure the default NE routing methods, refer to *System Administrators Guide for Native Deployment*, Reference [5].



Ericsson Dynamic Activation
Operation & Management

Activation Logic | **Network Elements** | System | Access Control | Walkthroughs

Network Elements | Network Element Groups | **Routing** | CAI3G DC Routing

Routing

View/Edit

		Network Element Type	Routing Method
		AAA_FE_NSD	UnconditionalRouting
		AUC_MASSIVE_UPDATE	UnconditionalRouting
		AUC_VALIDATION	UnconditionalRouting
		CADB	UnconditionalRouting
		CADB_AAA	UnconditionalRouting
		CADB_AAA_MASSIVE_SEARCH	UnconditionalRouting
		CADB_AAA_NSD	UnconditionalRouting
		CADB_DAE	UnconditionalRouting
		CADB_EIR	UnconditionalRouting
		CADB_EIR_MASSIVE_SEARCH	UnconditionalRouting
		CADB_HLR	UnconditionalRouting
		CADB_HLR_MASSIVE_SEARCH	UnconditionalRouting
		CADB_HLR_MASSIVE_UPDATE	UnconditionalRouting
		CADB_HLR_MNP	UnconditionalRouting
		CADB_HLR_MNP_MASSIVE_SEARCH	UnconditionalRouting
		CADB_MASSIVE_SEARCH	UnconditionalRouting
		CADB_SAPC	UnconditionalRouting
		CADB_SAPC_MASSIVE_SEARCH	UnconditionalRouting
		DAE_NOTIFICATION	UnconditionalRouting
		HLR_COMMON_DATA	UnconditionalRouting
		HLR_MASSIVE_UPDATE	UnconditionalRouting
		HLR_MNP	UnconditionalRouting
		HLR_RED	RegularExpressionRouting
		HLR_VALIDATION	UnconditionalRouting
		HSS_FE_AVG	UnconditionalRouting
		HSS_FE_EPS	UnconditionalRouting
		HSS_FE_IMS	UnconditionalRouting
		M2M_COMMON_DATA	UnconditionalRouting
		M2M_HLR_RED	RegularExpressionRouting
		M2M_HLR_VALIDATION	UnconditionalRouting
		MTAS	UnconditionalRouting
		MTAS_SIPTrunking	UnconditionalRouting

Figure 18 Routing Window



In **Routing** window, a table displays **Network Element Types** and their respective **Routing Method**. Operators can Add, View, Edit, and Remove routing for **Network Element Types** by clicking appropriate icons.

Note: When configuring **Routing** for IPWorks/ENUM provisioning, Dynamic Activation can be configured to provision either layered or monolithic IPWorks/ENUM, not both of them at the same time. For more information, refer to *Configuration Manual for Resource Activation*, Reference [2].

8.3.3.1 Adding a Routing

To add and configure a routing, follow these steps:

1. Click **Add**.
2. In the **Routing - Add - Step 1 / 3, General** menu, choose **Network Element Type** from the drop-down list.
3. Click **Next**.
4. In the **Routing - Add - Step 2 / 3, Network Elements** menu, if any NE, NE Groups, or Cluster Strategies are configured, select the *<NE Group>* as **Available Network Element Group(s)** or *<Cluster Strategy>* as **Available Cluster Strategy(s)** to the corresponding *<NE Type>*.
5. In **Routing - Add - Step 3 / 3**, operators can select routing method and edit routing items for selected managed object.
 - a Select a routing method from the drop-down list for selected managed object:
 - Number Range Routing
 - Number Series Routing
 - Regular Expression Routing
 - Unconditional Routing

The detailed routing item parameters are changed according to method selection. Operators can have several routing items in the list.

- b Configure the routing information for the chosen method.
 - **Number Range Routing**
 - 1 Select a **Network Element (Group)** and **Attribute Name**.
 - 2 Specify the start range and stop range.
 - 3 Click **Add**.
 - 4 Repeat the previous steps for more routing items.



- 5 Click **Apply** to finish adding rules. A verification page is displayed.
 - 6 Click **Change This...** to change the configured routing rules.
 - 7 Click **Done**.
- **Number Series Routing**
- 1 Select a **Network Element (Group)** and **Attribute Name**.
 - 2 Specify the number series in the **Series** field.
 - 3 Click **Add**.
 - 4 Repeat the previous steps for more routing rules.
 - 5 Click **Apply** to finish adding rules. A verification page is displayed.
 - 6 Click **Change This...** to change the configured routing rules.
 - 7 Click **Done**.
- **Regular Expression Routing**
- 1 Select a **Network Element (Group)** and specify an **Attribute Name**.
 - 2 Specify the expression in the **Regular Expression** field.
- Regular expression** can be used to express number series and number ranges. The format is `^number[numbers] [from number - to number] ... \d*$` where `^` and `$` quote the content of the definition, and `\d*` is the wildcard. For example, the expression `^46[379][2-8]\d*$` represents number ranges of 4632*-4638*, 4672*-4678* and 4692*-4698*.
- Note:** Characters “|” and “,” are not allowed in **Regular Expression** field, because they are used as separators in **Regular Expression Routing** configuration. For alternation constructs which uses “|” character to separate the alternatives, each alternative must be configured separately.
- 3 Click **Apply** to finish adding algorithm rules. A verification page is displayed.
 - 4 Click **Change This...** to change the configured routing rules.
 - 5 Click **Done**.
- **Unconditional Routing**




- 1 Select the **Network Element (Group)** to which all requests are directed.
- 2 Click **Apply**.
- 3 Click **Change This...** to change the configured routing rules.
- 4 Click **Done**.

8.3.3.2 Editing a Routing

Users can edit a routing by changing the routing methods, editing related Network Element (Group), attribute type and specific algorithm parameters.


To edit a routing, follow these steps:

1. Click the change icon  for the routing to modify.
A page with **General**, **Network Elements**, and **Routing Details** tabs is shown.
2. In the **General** tab, change the managed object, if needed.
3. In the **Network Elements** tab, add or remove **Available Network Element Group(s)** or **Available Cluster Strategy(s)**, if needed.
4. To change the routing methods, go to the **Routing Details** tab and change the settings as desired. For information about how to set the routing method, see Step 5.
5. Click **Apply**.

8.3.3.3 Removing a Routing

Note: Before removing a Routing, remove all the NE Groups from the Routing.

To remove a routing, follow these steps:

1. Click the remove icon  for the routing.
A window opens to confirm the remove operation.
2. Click **OK**.

8.3.3.4 Routing Parameters

A routing is defined by the following parameters.

Table 19 Routing Parameters

Parameter	Description
Network Element Type	The logical representation of an NE function



Parameter	Description
Network Element (Group)	Destination for a request which matches the routing algorithm rule
Routing Method	The type of routing method for the routing
Routing Items	A configuration item which contains match rules and destination for number ranges or series
Algorithm Rule	Routing method parameter for regular expression

8.4 System

This section covers the **System** tab in the Dynamic Activation GUI. It consists of the **Licenses**, **Options**, and **Notification email configuration** subtabs.

8.4.1 Licenses

In the **Licenses** tab, all licenses and PC keys existing in the system are presented. Operators can **View** and **Update** licenses, see Figure 19.

Ericsson Dynamic Activation
Operation & Management

Activation Logic

Network Elements

System

Access Control

Walkthroughs

Log Management

Loose Error Handling

Licenses

Options

Notification E-Mail Configuration

Synchronize Configuration

Licenses

View/Edit

	License ID	Name	Type	Capacity used	Capacity	Percent used	Expiration date
	FAT1023848/1	EDA Maximum servers	Value Package	1	100	1 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/2	EDA SW Advanced	Value Package	1	100	1 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023848/2	EDA Max VMs	Value Package	1	100	1 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023848/3	EDA Max CPUs	Value Package	0	100	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/5	EDA 2G 3G	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/6	EDA Subscriber Services	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/7	EDA IMS Core	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/8	EDA LTE EPC	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/9	EDA Multimedia Telephony	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/10	EDA Policy Control	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/11	EDA MV Subscriber Services	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/12	EDA Charging	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/13	EDA Billing and CBI	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/14	EDA Wi-Fi Calling	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/15	EDA eSIM	Value Package	0	10000000	0 %	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/16	EDA Shared Networks	Value Package	N/A	N/A	N/A	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/20	EDA Access	Value Package	N/A	N/A	N/A	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/21	EDA Aggregation	Value Package	N/A	N/A	N/A	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/22	EDA Edge/Core	Value Package	N/A	N/A	N/A	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/23	EDA Service Configuration	Value Package	N/A	N/A	N/A	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/24	EDA Small Access	Value Package	N/A	N/A	N/A	Fri Apr 13 23:59:59 CEST 2018
	FAT1023849/101	EDA Base Package	Value Package	1	20	5 %	Fri Apr 13 23:59:59 CEST 2018

Figure 19 Example of Licenses Window



Table 20 Licenses Table Columns

Column	Description
License ID	The ID of the license
Name	The name of the license.
Type	The license type, can be Value package or PC license.
Capacity used	The capacity being consumed by the system.
Capacity	The capacity the system is entitled to.
Percent Used	A round indicator showing green up to 80% subscriber capacity used, yellow between 80% and 100% and red when exceeding 100%
Expiration Date	The date the license expires.

8.4.2 Options

In the **Options** tab operators can turn ON or OFF **Alarm Supervision**, set **Maximum Consecutive Unsuccessful Login Attempts**, turn ON or OFF **Login Locking**, configure different **User Password Settings**, set **Target Pool Max**, and turn ON or OFF **CUIDB Lookup**, see Figure 20.

The screenshot shows the 'Options' window within a system configuration interface. The top navigation bar includes tabs for 'Activation Logic', 'Network Elements', 'System' (selected), 'Access Control', 'Walkthroughs', 'Log Management', and 'Loose Error Handling'. Below this, a sub-navigation bar shows 'Licenses' and 'Options' (selected), with links for 'Notification E-Mail Configuration' and 'Synchronize Configuration'. The main content area is titled 'Options' and contains several sections: 'Alarm Configuration' with 'Alarm Supervision' checked; 'Login Authentication' with 'Maximal Consecutive Unsuccessful Login Attempts' set to 3 and 'Login Locking' checked; 'User Password Settings' with fields for 'Minimum Length' (8), 'Minimum Occurrence of Lower Case Characters' (1), 'Minimum Occurrence of Upper Case Characters' (1), 'Minimum Occurrence of Digits Characters' (1), and 'Minimum Occurrence of Special Characters' (1); 'Core Properties' with 'Target Pool Max' set to 160, 'CAI3G corresponding to MML family' unchecked, and 'Prevent Concurrent Subscriber Provisioning' unchecked; and 'Administration of Multi-region' with 'CUIDB Lookup' unchecked. An 'Apply' button is located at the bottom left of the form.

Figure 20 Options Window



Table 21 Options Configurations

Type	Configuration	Description
Alarm Configuration	Alarm Supervision	Turns all system SNMP alarms ON or OFF.
Login Authentication ⁽¹⁾	Maximal Consecutive Unsuccessful Login Attempts	Maximal number of consecutive unsuccessful login attempts. If this number is reached, the user is locked. If this number is exceeded, an event is sent.
	Login Locking	Turns the Login Locking feature ON or OFF. If the feature is ON, and if wrong password is entered <number> times, the user is locked. Only the super user or user administrator can unlock a locked user.
User Password Settings ⁽¹⁾	Minimum Length	Range 4–32 characters. Default value is 8.
	Minimum Occurrence of Lower Case Characters	Range 0–32 characters. Default value is 1.
	Minimum Occurrence of Upper Case Characters	Range 0–32 characters. Default value is 1.
	Minimum Occurrence of Digits Characters	Range 0–32 characters. Default value is 1.
	Minimum Occurrence of Special Characters	Range 0–32 characters. Default value is 1. The following are considered as special character s: !"#%&'()*+,-./:;<=>?@[\\]^_`{ }~
Core Properties	Target Pool Max	Defines the maximum number of internal threads for each Dynamic Activation node. The value on this parameter can have a large impact on system performance.
	CAI3G corresponding to MML family	Enables or disables traffic for MOs of this type. Default is disabled. ⁽²⁾
	Prevent Concurrent Subscriber Provisioning	Enables or disables the Prevent Concurrent Subscriber Provisioning feature. It is used to prevent the concurrent provisioning to the same subscriber. Default is disabled.
Administration of Multi-region ⁽³⁾	CUDB Lookup	Enables or disables the CUDB Lookup feature. The CUDB Lookup feature is used to find the Region Identifier (RID) value for a subscriber when either of following: <ul style="list-style-type: none"> • RID is not included in an incoming request. • There are no MSISDN rules defined in the Administration Domain.

(1) For provisioning clients configuration.

(2) These MOs are considered as deprecated and the recommendation is to avoid using them.

(3) This property is license dependent.



8.4.3 Notification Email Configuration

In the **Notification email Configuration** tab operators add email addresses to where notifications are sent if the capacity license is exceeded, see Figure 21.

For more information, refer to information about **Subscriber Licensing** in *Function Specification Resource Activation*, Reference [4].

Activation Logic Network Elements **System** Access Control Walkthroughs

Licenses Options **Notification E-Mail Configuration**

Notification E-Mail Configuration

E-Mail Address Configuration

Mail From Address:

Mail To Addresses: *

SMTP Server Configuration

SMTP Host: *

SMTP Port Number: *

Use SMTP Authentication: ☐

SMTP User Name:

SMTP Password:

Figure 21 Notification email Configuration Window

The following tables describe the variables in the **Notification email Configuration** window.

Table 22 Email Address Configuration

Variable	Description
Mail From Address	The email address used as the sender of notification emails.
Mail To Address	The receiver of notification emails. If several addresses are specified they must be separated with comma (,).

Table 23 SMTP Server Configuration

Variable	Description
SMTP Host	The SMTP hostname, fully qualified hostname, or IP address for the notification email address. Upon successful account verification, a notification email is sent to the specified SMTP host.
SMTP Port Number	The SMTP port number used for the notification email address.



Use SMTP Authentication	A check box that defines if SMTP Authentication is used or not. Disabled by default.
SMTP username	The username for the SMTP server.
SMTP Password	The password for the username to the SMTP server.

8.4.4 Synchronize Configuration

Attention!

Synchronize Configuration can only be applied among clusters at the same software level.

Applying synchronization to a cluster at a different software level causes problems.

In this tab, it is possible to manually synchronize configuration from one cluster to one or two other clusters. During this process, configuration data from the cluster where **Synchronize Configuration** is executed on, is sent to one or two receiving clusters. The whole configuration of receiving clusters is to be replaced by the configuration data of the sending cluster.

All clusters that are used in a configuration synchronization need to be set up first. For more information about how to set up the clusters for synchronization, see *System Administrators Guide for Native Deployment*, Reference [5].

The screenshot shows a web-based management interface. At the top, there is a navigation bar with tabs: 'Activation Logic', 'Network Elements', 'System' (selected), 'Access Control', and 'Walkthroughs'. Below this, a sub-navigation bar contains 'Licenses', 'Options', 'Notification E-Mail Configuration', and 'Synchronize Configuration' (selected). The main content area is titled 'Synchronize Configuration'. It contains a red warning icon followed by the text: 'Note, If parameters from Access Control are included, the performance of the receiving cluster can be impacted'. Below this is a label 'Include parameters from Access Control in synchronization of configuration:' followed by an unchecked checkbox. At the bottom of the form is an 'Apply' button.

Figure 22 Synchronize Configuration Window

The **Synchronize Configuration** window displays a check box. If this check box is checked, parameters from access control are included in the synchronization of the configuration. If the check box is left empty, the configuration synchronization does not include any parameters from access



control. For more information about parameters in access control, see Section 8.5 on page 78. If parameters from access control are included in the configuration synchronization, performance of the receiving cluster can be affected.

Note: Before synchronizing the configuration, the traffic interface on all PL nodes on the receiving cluster must be disabled to avoid traffic disturbances. For more information about how to disable and enable traffic, see *System Administrators Guide for Native Deployment*, Reference [5].

When pressing **Apply** button, a message is displayed saying that synchronization is ongoing. This process can take several minutes depending on, for example, the number of NEs. If the configuration synchronization fails to one or both clusters, an error message is shown.

Caution!

Before pressing the **Apply** button, make sure to be logged in on the correct cluster, the one that contains the configuration to be sent for synchronization. If performed on the wrong cluster, this action can cause loss of configuration on active, provisioning cluster, and total stop of provisioning.

8.5 Access Control

The **Access Control** tab is used to manage and configure provisioning clients. It consists of the **Users**, **Policies**, **Attribute Rules**, and **Administration Domains** subtabs.

8.5.1 Users

Provisioning clients can be added, modified, and deleted in the **Users** tab, see Figure 23.

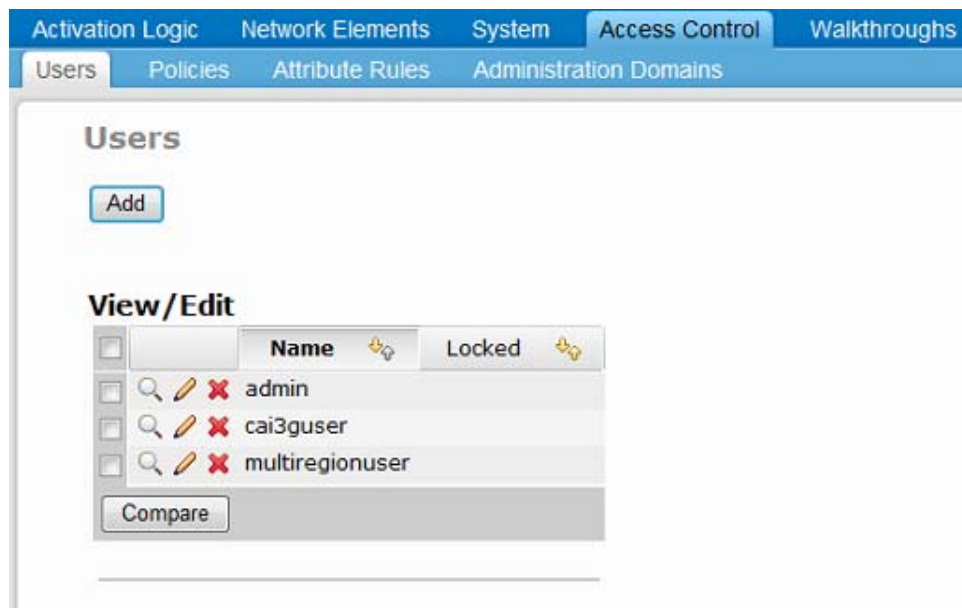


Figure 23 Users

8.5.1.1 Adding a Provisioning Client

To add a provisioning client (referred as a user), follow the instruction:

1. In **Users** tab, click **Add**.

The **Users - Add - Step 1 / 3** shows as in Figure 24:



Users - Add - Step 1 / 3

General

<- Back Next -> Apply Cancel

Name: *

Password: *

Confirm password: *

Description:

Locked: ☐

Max CAI3G sessions:

Max CAI sessions:

Max MML sessions:

Min HLR sustainable CSO/sec:

Value 0 or 0.0 means no limitations enforced

Advanced...

<- Back Next -> Apply Cancel

Figure 24 Users - Add - Step 1 / 3

A user is defined by the parameters described in Table 24.

By clicking **Advanced**, the two SSH related parameters are available: **Max SSH sessions** and **SSH Public Key**.

The two parameters only take effect when SSH CA project is deployed. For details, refer to *Northbound Interface Adapter Customization Development Guide for CLI-Based Protocol*, Reference [11].



Table 24 Users Parameters

Parameter	Description
Name	<p>Name of the user</p> <p>Mandatory</p> <p>Username criteria:</p> <ul style="list-style-type: none"> • A username must be within the regular expression; [a-zA-Z0-9]*. • A minimum of 1 character and a maximum of 32 characters. • No control or space characters.
Password	<p>Password, used to access the user menu</p> <p>Mandatory</p> <p>Password criteria:</p> <ul style="list-style-type: none"> • Contains only characters from the ISO-8859-1 character set. That is, the numbers from 0 through 9, the uppercase and lowercase English alphabet, and the following commonly used special characters: !"#%&'()*+,-./:;<=>?@[\\]^_`{ }~ • A minimum of 4 and a maximum of 32 characters • No control or space characters
Description	<p>A short description of the user</p> <p>Optional</p>
Locked	<p>Locking a user at this stage can be used in case the user needs to be locked until the system is properly configured</p>
Max CAI3G sessions ⁽¹⁾	<p>Fill in this Capacity Attribute text field to limit the number of CAI3G sessions for the user.</p> <p>Value 0–25000</p> <p>Default value for this parameter is 0 which means no limitations are enforced for the particular user.</p> <p>Optional</p>
Max CAI sessions ⁽¹⁾	<p>Fill in this Capacity Attribute text field to limit the number of CAI sessions for the user.</p> <p>Value 0–250</p> <p>Default value for this parameter is 0 which means no limitations are enforced for the particular user.</p> <p>Optional</p>
Max MML sessions ⁽¹⁾	<p>Fill in this Capacity Attribute text field to limit the number of MML sessions for the user.</p> <p>Value 0–160</p> <p>Default value for this parameter is 0 which means no limitations are enforced for the particular user.</p> <p>Optional</p>
Min HLR sustainable CSO/sec ⁽¹⁾	<p>Fill in this Capacity Attribute text field to limit Customer Service Operations (CSOs) per second for the user.</p> <p>Default value for this parameter is 0.0 which means no limitations are enforced for the particular user.</p> <p>Optional</p>



Parameter	Description
Max SSH Sessions	Fill in this Capacity Attribute text field to limit the number of SSH sessions for the user. Value 0-250 Default value for this parameter is 0 which means no limitations are enforced for the particular user. Optional This parameter is only available in Advanced mode.
SSH Public Key	Public key for the user. Optional Public key criteria: <ul style="list-style-type: none">Match the regular expression: <code>^\$ ^((ssh-rsa ssh-dss) .*)</code> Default value for this parameter is empty string which means SSH login is not supported. This parameter is only available in Advanced mode.

(1) This parameter is available when the **Administration of Multi-region >CUDB Lookup:** property is enabled, see Section 8.4.2 on page 74

2. Fill in the mandatory fields to create a **User**.

When done, click **Next**.

The **Users - Add - Step 2 / 3** shows, as in Figure 25:

Role	Access Type	Description
<input type="checkbox"/> Users Administrator	<input checked="" type="radio"/> Full <input type="radio"/> Read-only	Permission to manage system users
<input type="checkbox"/> Network Elements Administrator	<input checked="" type="radio"/> Full <input type="radio"/> Read-only	Permission to setup network elements and routing
<input type="checkbox"/> Activation Logic Administrator	<input checked="" type="radio"/> Full <input type="radio"/> Read-only	Permission to change activation logic
<input type="checkbox"/> System Administrator	<input checked="" type="radio"/> Full <input type="radio"/> Read-only	Permission to modify system-wide configuration
<input type="checkbox"/> System Integrator	<input checked="" type="radio"/> Full <input type="radio"/> Read-only	Permission to manage system integrator configuration
<input type="checkbox"/> Log Administrator	<input checked="" type="radio"/> Full <input type="radio"/> Read-only	Permission to manage logging

Figure 25 Users - Add - Step 2/ 3



3. Select the Configuration Management Authorities for the user.
 - If selecting **No authorities**, the user has no access to the GUI.
 - If selecting **Full authorities**, the user is given Configuration Management Administrator Role and has full permissions.
 - If selecting **Customize authorities**, it is possible to select roles manually for the user. A user can have more than one role.

When selection is done, click **Next**.

The **Users - Add - Step 3/3** shows, as in Figure 26:

Users - Add - Step 3 / 3

Provisioning Authorities - Authority Level

☐ No authorities
☐ Full authorities
☐ Customize authorities

Domain	Network Element	Managed Object	Operations
All: <input type="checkbox"/>			
<input type="checkbox"/> Voice	<input type="checkbox"/> HLR	<input type="checkbox"/> AdditionalMSISDN <input type="checkbox"/> CAMELExtendedInformation <input type="checkbox"/> CAMELSubscriptionData <input type="checkbox"/> CAMELTriggeringCriteria <input type="checkbox"/> ClosedUserGroup <input type="checkbox"/> ClosedUserGroupBasicServiceGroupOptions <input type="checkbox"/> HECDAF <input type="checkbox"/> HECDBD <input type="checkbox"/> HECDEQ <input type="checkbox"/> HECDGL <input type="checkbox"/> HECDGS <input type="checkbox"/> HECDDIX <input type="checkbox"/> HECDDRA <input type="checkbox"/> HECDDRP <input type="checkbox"/> HECDDZN <input type="checkbox"/> HEMSAP	<div> <input type="checkbox"/> CREATE <input type="checkbox"/> DELETE <input type="checkbox"/> UPDATE </div> <div> <input type="checkbox"/> CREATE <input type="checkbox"/> DELETE <input type="checkbox"/> READ <input type="checkbox"/> UPDATE </div> <div> <input type="checkbox"/> CREATE <input type="checkbox"/> DELETE <input type="checkbox"/> READ <input type="checkbox"/> UPDATE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div> <div> <input type="checkbox"/> INITIATE <input type="checkbox"/> END <input type="checkbox"/> PRINT <input type="checkbox"/> CHANGE </div>

Figure 26 Users - Add - Step 3 / 3

4. Select the Provisioning Authorities for the user.
 - If selecting **No authorities**, the user has no provisioning authorities.
 - If selecting **Full authorities**, the user is given full provisioning authorities.
 - If selecting **Customize authorities**, it is possible to select **Domain** manually, **Network Element**, **Managed Object**, and **Operations** for the user.



When selection is done, click **Apply**.

Note: The **Policies** must be updated to activate the changes made. See Section 8.5.2 on page 85.

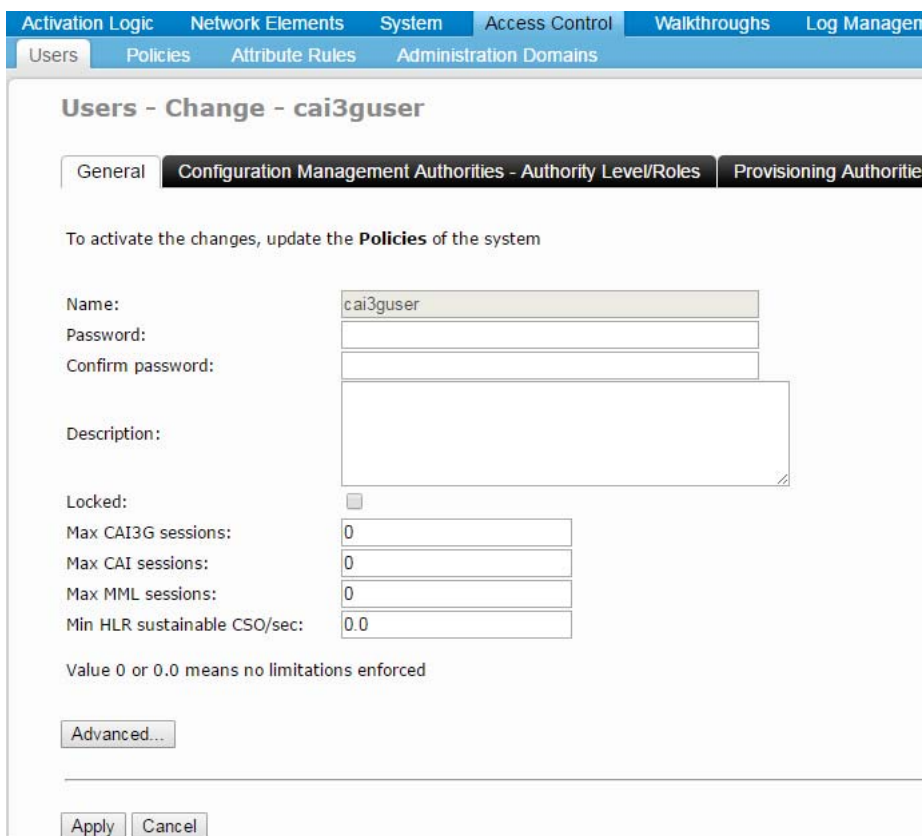
8.5.1.2 Editing a Provisioning Client

Provisioning clients can be edited by changing password, description, locked-status, authorities, and related Administration Domains.

To edit a provisioning client (referred as a user), follow these steps:

1. In **Users** tab, click the change icon  for the user to modify.

A page with **General**, **Configuration Management Authorities - Authority Level/Roles**, **Provisioning Authorities - Authority Level** and **Administration Domains** tabs is shown, see Figure 27.



Activation Logic Network Elements System Access Control Walkthroughs Log Management

Users Policies Attribute Rules Administration Domains

Users - Change - cai3guser

General Configuration Management Authorities - Authority Level/Roles Provisioning Authorities

To activate the changes, update the **Policies** of the system

Name: cai3guser

Password:

Confirm password:

Description:

Locked: ☐

Max CAI3G sessions:

Max CAI sessions:

Max MML sessions:

Min HLR sustainable CSO/sec:

Value 0 or 0.0 means no limitations enforced

Advanced...

Apply Cancel

Figure 27 Users - Change

2. In the **General** tab, it is possible to change **Password**, **Description**, **Locked** - status and change the number of **Max CAI3G sessions**, **Max CAI sessions**, **Max MML sessions**, and **Max SSH sessions** as well as set **Min HLR sustainable CSO/sec** and **SSH Public Key**.



Click **Advanced** to edit the values of the parameters **Max SSH sessions** and **SSH Public Key**.

Note: It is not possible to change the name of the **User**.

3. In the **Configuration Management Authorities - Authority Level/Roles** tab, it is possible to change the Configuration Management Authorities for the specific user.
4. In the **Provisioning Authorities - Authority Level** tab, it is possible to change the Provisioning Authorities for the specific user.
5. In the **Administration Domains** tab, it is possible to change (assign or remove) Domains for the specific user.

Note: A user that is created does not get a default **Administration Domains** role. If a user must have an **Administration Domains** role assigned, it is made afterwards.

6. Click **Apply**.

Note: The **Policies** must be updated to activate the changes made. See Section 8.5.2 on page 85.

8.5.2 Policies

In the **Policies** tab, click **Apply** to activate changes made in the **Users**, **Attribute Rules**, and **Administration Domains** tabs.

Note: Updating policies can have a temporary impact on the system performance. It is therefore wise to update policies during off-peak hours.

8.5.3 Attribute Rules - Restriction Rules

In the **Attribute Rule** tab, it is possible to set or change restriction rules on attribute level for a specific user. These attribute rules are checked for incoming requests. It is not possible to restrict the response that is to be returned.

Note: The user must have Provisioning Authorities set to **Customize authorities** to be able to use the **Attribute Rule** function.

Figure 28 shows the users that already have restriction rules set on attribute level. It is possible to use appropriate icon to:

- View the details of the rules for the user.
- Change the user attribute rules.
- Delete the rules for the user.

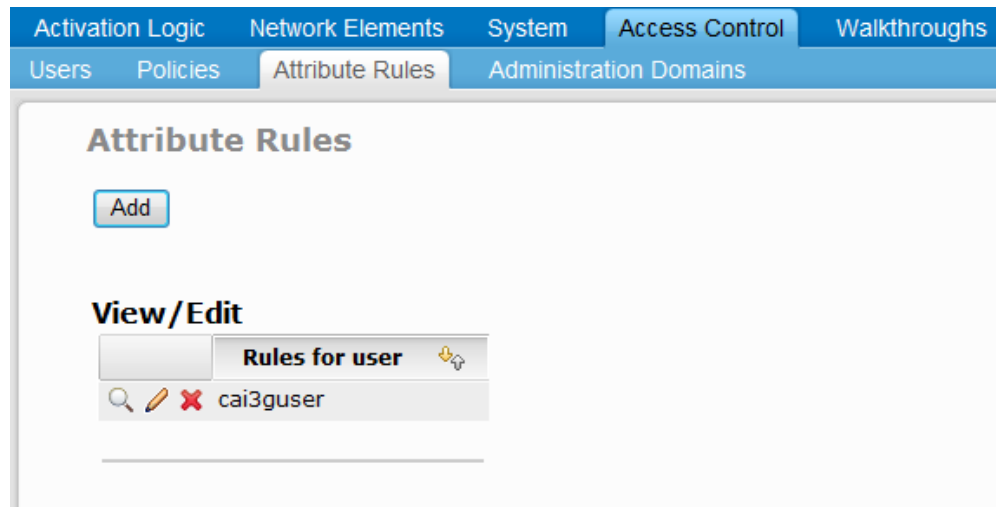


Figure 28 Attribute Rule

Click **Add** in the **Attribute Rule** window.

The **Attribute Rule-Add-Step 1 / 2** window is displayed, as in Figure 29.

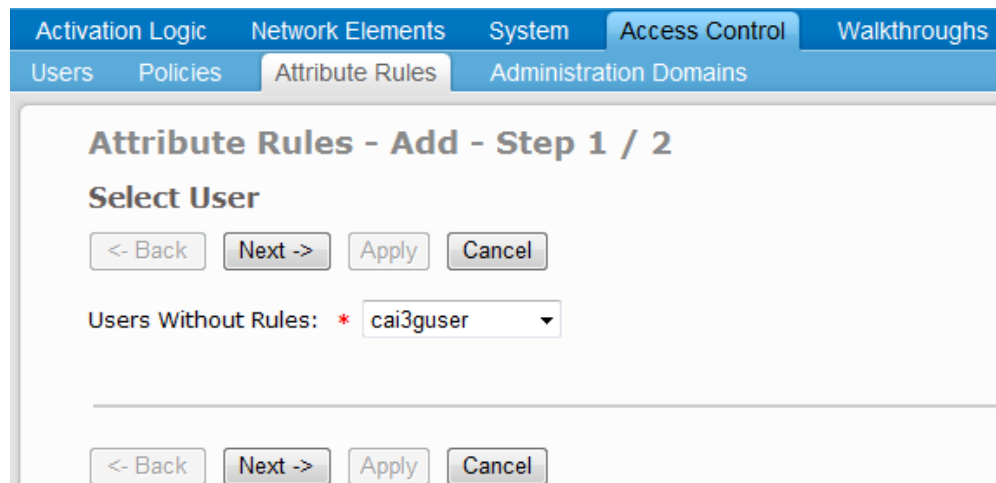


Figure 29 Attribute Rule - Add-Step 1 / 2

The users that have been defined in the system, but have no restriction rules, are visible in the **Users Without Rules** scrollbar.

Click **Next** to set the restriction rules for the selected user.

In the **Attribute Rule - Add-Step 2 / 2** window, add the wanted restriction rule on attribute level, as shown in Figure 30.

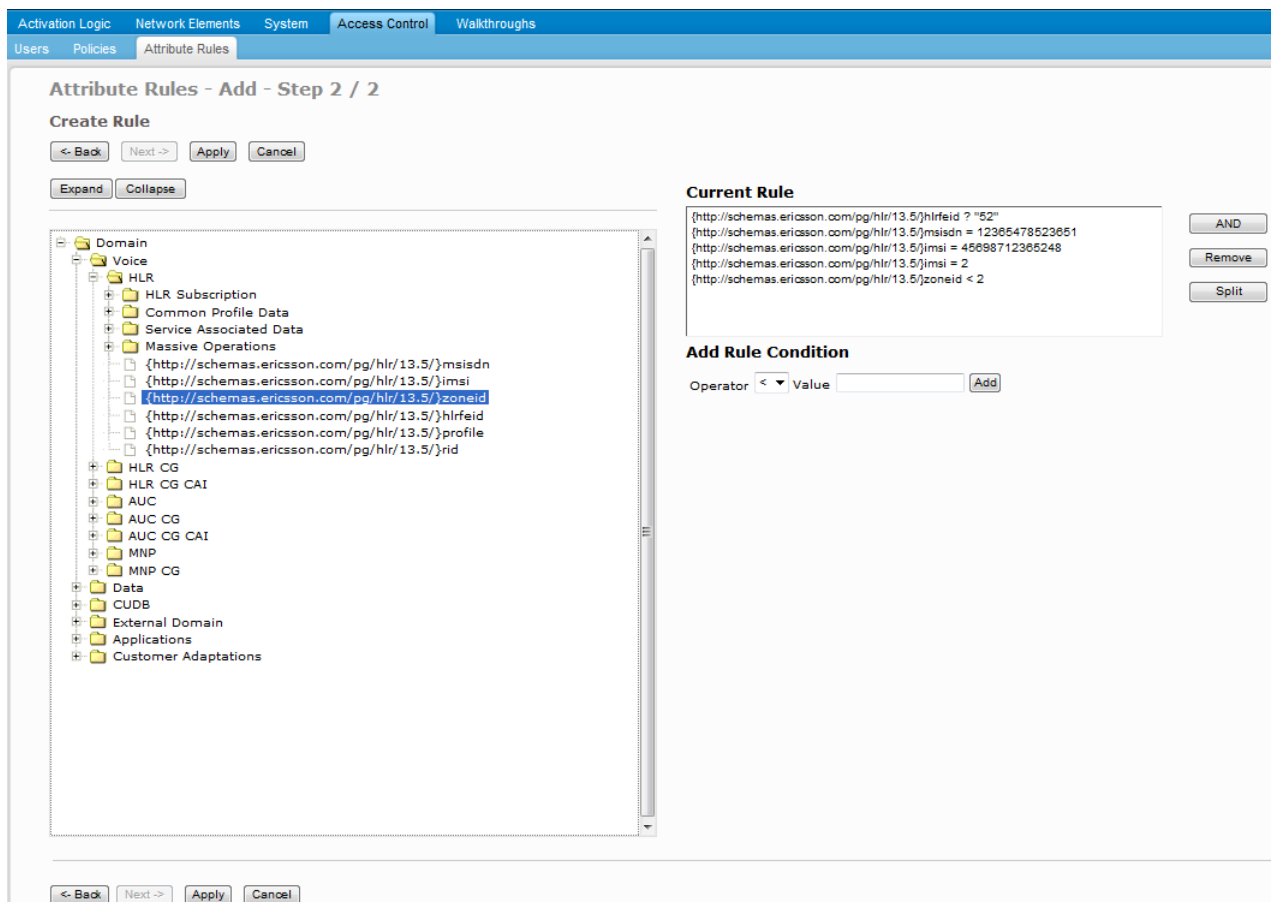


Figure 30 Attribute Rule - Add- Step 2 / 2

When an attribute is selected, the operator that can be used for that type of attribute is shown in the **Operator** scrollbar.

The **Value** must be specified according to the interface specifications, see chapter **Interface**, in the *Library Overview*, Reference [1] document.

To add a logical **AND** between two conditions (or more), select two rows (or more) and click **AND**.

To add a logical **OR** between conditions, leave the conditions on separate rows. An **OR** is added between the rows in the **Current Rule** window.

A condition that is based on an attribute not included in the incoming request is evaluated to:

- true if this is the only condition in the rule.
- false if it is part of an **OR** condition.
- true if it is part of an **AND** condition.

The **Condition View** shows how the condition is built up.



It is possible to split a condition containing one or more **AND** operators by selecting a row and then clicking **Split**.

Removing a row is done by clicking **Remove**.

Click **Apply** to activate the restriction rule made.

Note: The **Policies** must be updated to activate the changes made. See Section 8.5.2 on page 85.

To modify the current rule, change values for an attribute under the **Edit View**. This option updates the selected rules with the values entered in the operator.

8.5.4 Administration Domains

The **Administration Domains** tab is available when adequate license is obtained.

In the **Administration Domains** tab Administration Domains can be added, modified, or changed. It is also possible to add, edit, view details or delete rules on attribute level for a specific Administration Domains role.

Note: This feature is only supported for HLR and M2M in the data layered architecture.

Figure 31 shows the existing **Administration Domains**.

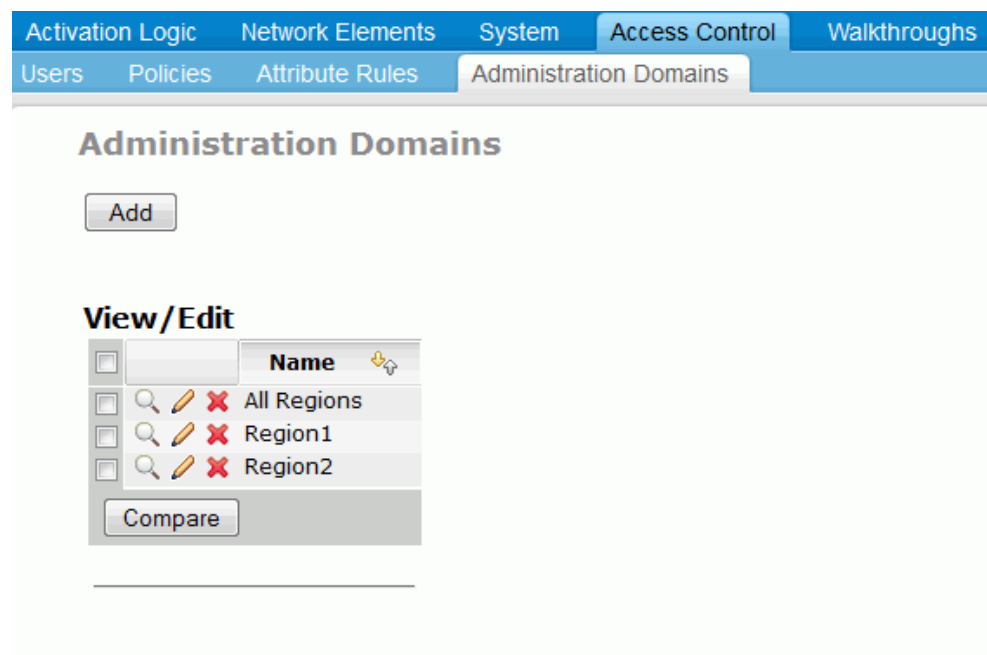


Figure 31 Administration Domains



To compare values for two different Administration Domains, fill in check boxes on the left from the Domains to be compared and click **Compare**. The **Administration Domains - Compare - <Domain name 1>, <Domain name 2>** window is displayed, as shown in Figure 32.

Administration Domains - Compare - Region1, Region2		
General		
Property	Value	Value
Name	Region1	Region2
Description	This is the region in area 1	This is the region in area 2
Min HLR sustainable CSO/sec	0.0	0.0
Sysadm	false	false
Add RID to Subscriber Profile	false	true
Rules		
Property	Value	Value
rid	rid = 1	rid = 2
imsi	imsi Starts with 1111	imsi Starts with 2222

Change Region1... Change Region2... Done

Figure 32 Compare Window

It is also possible to edit values for each compared domain by clicking **Change <Domain name>** button. For more information on how to edit Administration Domains, see Section 8.5.4.2 on page 94.

8.5.4.1 Adding Administration Domains

To add Administration Domains, follow the instruction:

1. Click **Add** in the **Administration Domains** window.

The **Administration Domains - Add-Step 1 / 2** window is displayed, as shown in Figure 33.



Figure 33 Administration Domains - Add-Step 1 / 2

Administration Domains are defined by the parameters described in Table 25.

Table 25 Administration Domains Parameters

Parameter	Description
Name	Name of the administration domain Allowed characters are a-z, A-Z, 0-9, -, _ and whitespace. Mandatory
Description	A short description of the administration domain Optional
Sysadm	Enable this check box to make the domain a System Administrator Administration Domain. A user that has such domain assigned as a role is able to run conditional searches via CLI interface towards all existing domains with higher performance. ⁽¹⁾ Optional



Parameter	Description
Add RID to Subscriber Profile	<p>The Subscriber Profile Ranges, CAMEL Profile Ranges, and GPRS Profile Ranges have been extended for Multi Region feature and Logical HLR feature in HLR. Subscriber Profile Range is extended from 256 profiles to 8192 (32*256) profiles and CAMEL/GPRS Profile Range is extended from 255 profiles to 8160 (32*255) profiles.</p> <p>The CAS system must include the real profile value in the provisioning request towards Dynamic Activation for CAMEL or GPRS profiles.</p> <p>The CAS system can use the range 0–255 (256 profiles) in the provisioning request towards Dynamic Activation for Subscriber Profiles, but the Add RID to Subscriber Profile check box must be enabled. Then the HLR-FE internally uses the RID and Subscriber Profile to calculate the real Subscriber Profile value.</p> <p>Optional</p>
Min HLR sustainable CSO/sec	<p>Fill in this Capacity Attribute text field to limit Customer Service Operations (CSOs) per second for the role.</p> <p>Default value for this parameter is 0.0 which means no limitations are enforced for the particular user.</p> <p>Optional</p>

(1) For a domain with **Sysadm** flag checked, do NOT set any restriction rules as this domain is meant to have no restrictions.

2. Fill in the mandatory fields to create an Administration Domain.

Click **Next** to set the attribute rules for the added **Administration Domains**.

3. In the **Administration Domains - Add-Step 2 / 2** window, add the wanted rules on attribute level, as shown in Figure 34.

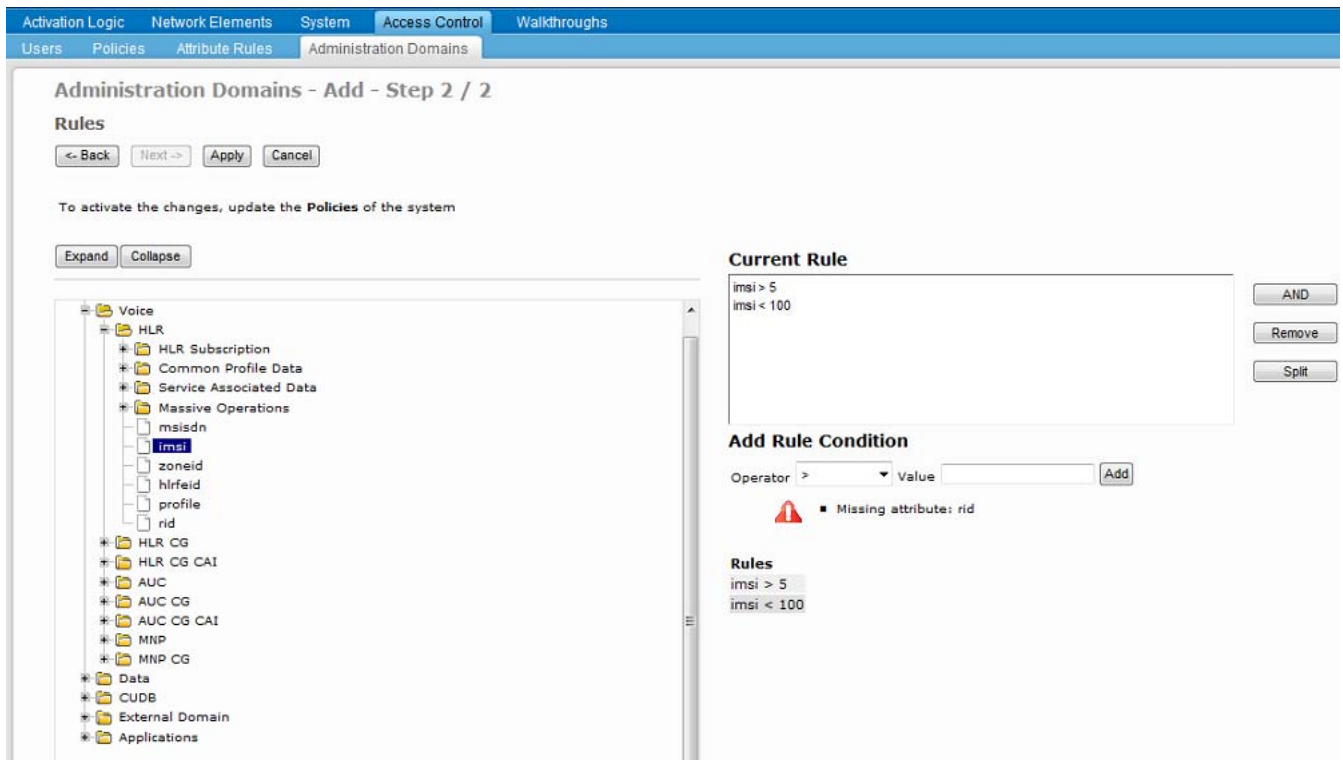


Figure 34 Administration Domains - Add- Step 2 / 2

4. The `rid` and the `imsi` attributes are mandatory and must always be defined for every **Administration Domain**.

Warning is given if RID or IMSI be undefined, see Figure 34.

Overlapping of RID, IMSI, and MSISDN between Domains is notified with warning messages.

The **Value** is to be specified according to the interface specifications, see chapter **2.3.7 Interface**, in the *Library Overview*, Reference [1] document.

Note: Default behavior is **AND** between rows with different attributes. However, between rows with same attribute, for example, MSISDN, the default behavior is **OR**.

To add a logical **AND** between two conditions (or more) for the same attribute, select two rows (or more) and click **AND**.

To add a logical **OR** between conditions for the same attribute, leave the conditions on separate rows and click **OR**.

It is possible to split a condition containing one or more **AND** operators by selecting a row and then clicking **Split**.

Removing a row is done by clicking **Remove**.

Administration Domains restriction rules are possible to define with:

- Value ranges.
- Series (that is value starts with a configured number, and allow any combination after the configured number.)
- Regular expressions.

Note: The restriction rules are only checked for incoming requests. It is not possible to restrict the response that is to be returned.

5. It is also possible for the user to define any SUD code and its value rule, both for value part 1 and value part 2, see Figure 35.

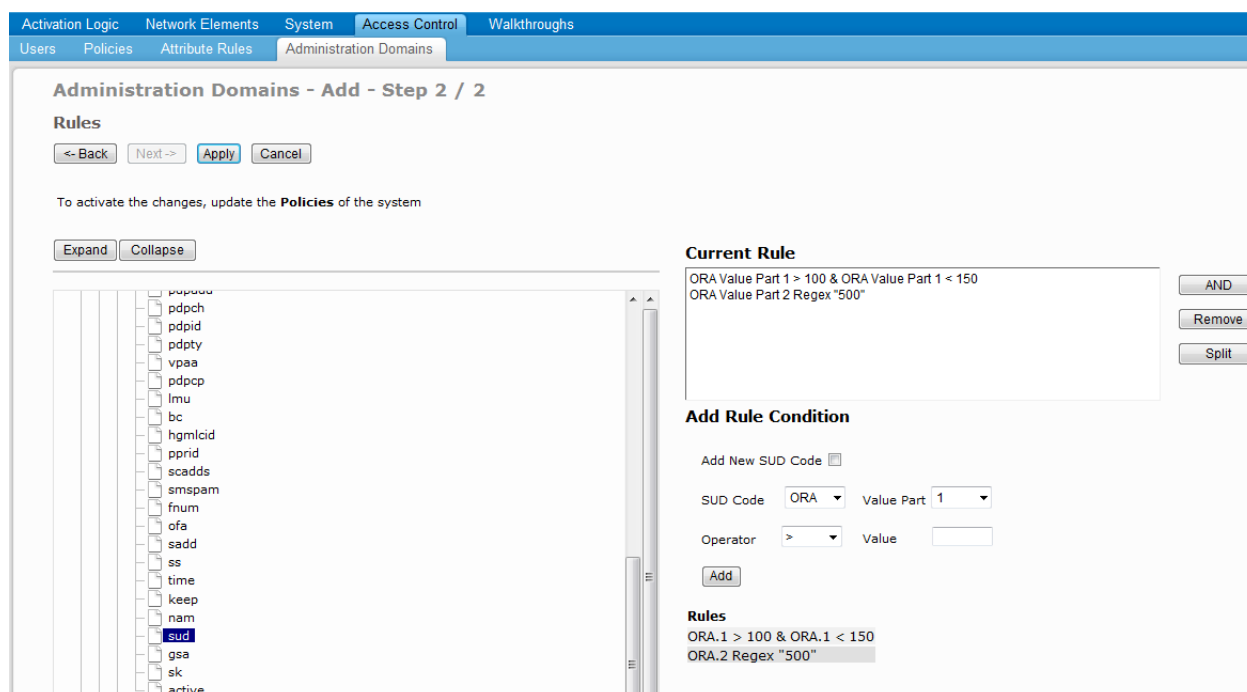




Figure 35 Administration Domains - Add- Step 2 / 2 SUD Codes

To add a new SUD Code for Standard HLR Subscriber, in the tree-view select Domain > Voice > HLR > HLR Subscription and sud, enable the **Add New SUD Code** check box, enter a unique SUD Code name, and specify the values for it.

6. Click **Apply**.
7. Click the **View Details** icon  to validate the **Administration Domains** restriction rules made.

If a SUD Code is added, details can be seen by clicking the **View Details** icon  for the specific Administration Domain in the **Administration Domains** tab.




8. Update the **Policies**.

Note: The **Policies** must be updated to activate the changes made. See Section 8.5.2 on page 85.

8.5.4.2 Editing Administration Domains

To edit Administration Domains, follow the instruction:

1. Click the change icon  to change settings of the **Administration Domain**.
2. The **Administration Domains - Change - <Domain name>** window with **General** and **Rules** is displayed.

Note: It is not possible to change the name of the **Administration Domain**.

3. Click **Apply** to set the restriction rules for the **Administration Domain**.
4. Update the **Policies**.

Note: The **Policies** must be updated to activate the changes made. See Section 8.5.2 on page 85.

8.6 Walkthroughs Control

This section covers the **Walkthroughs** tab in the Dynamic Activation GUI.

This feature is only visible for the super user and the Configuration Management Administrator.

8.6.1 Initial Setup

Go to the **Walkthroughs** tab to access the available walkthroughs, see Figure 36. A walkthrough can help when configuring certain parts of the GUI.

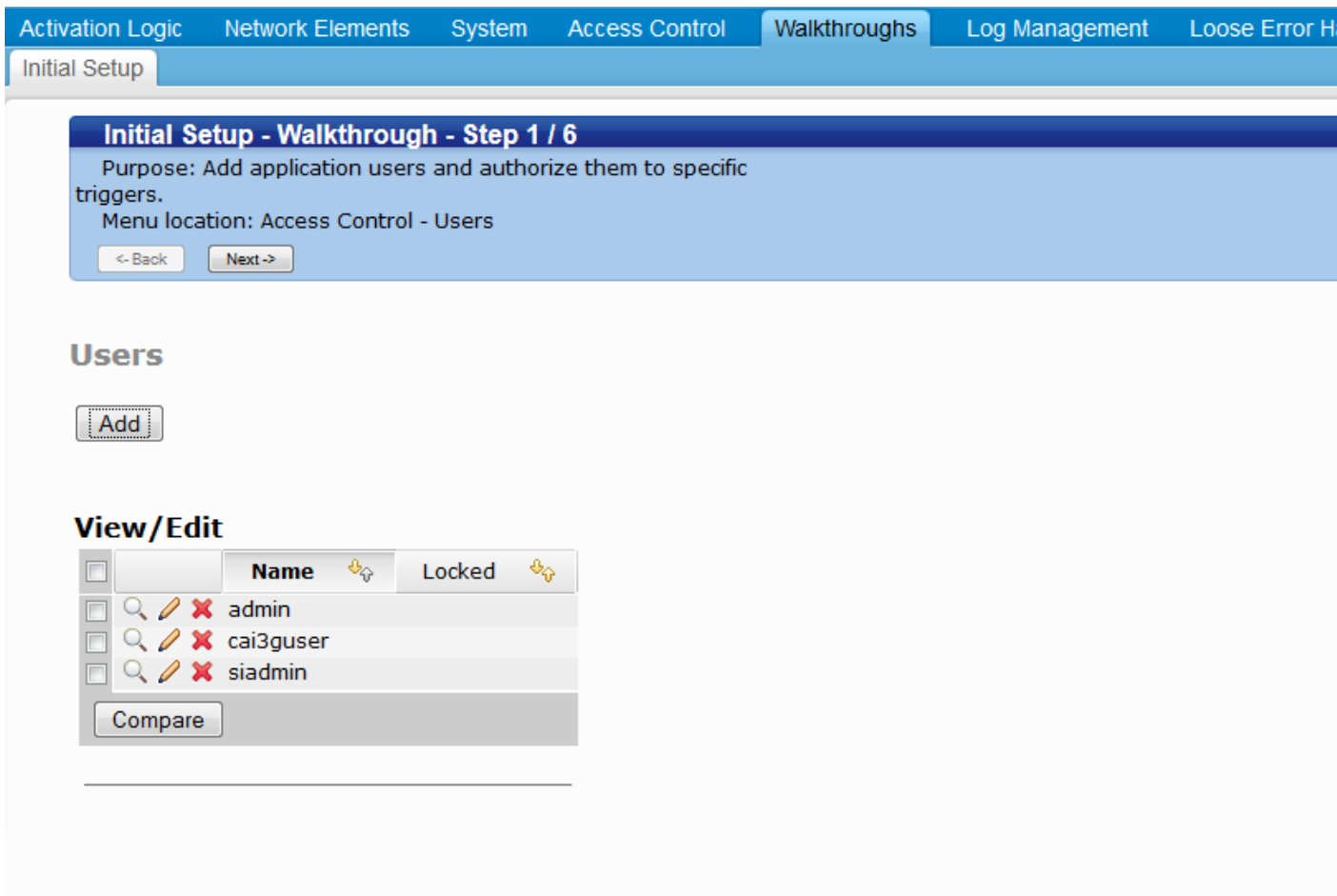


Figure 36 Walkthroughs Window

Select a walkthrough. Edit the settings on the page that is displayed. When ready, click **Next** and a new page is displayed. The walkthrough automatically takes the user to every page necessary for the procedure related to the walkthrough.





9 Priority Configuration

The **Priority Configuration** GUI shown in Figure 37 manages priority rule to be applicable on both Asynchronous CAI3G request and Synchronous CAI3G request.

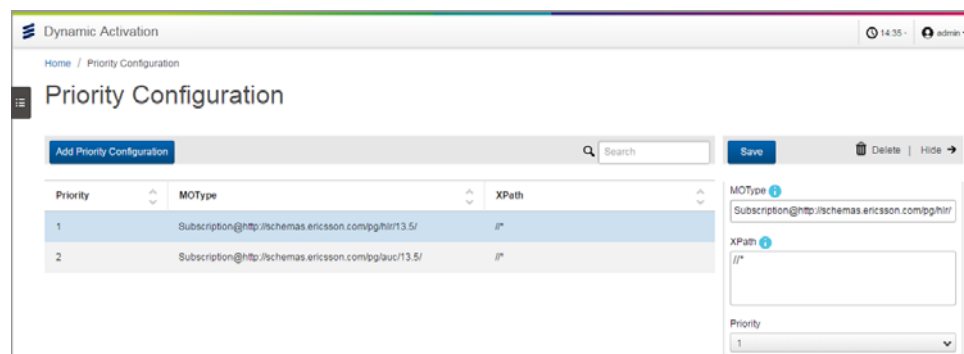


Figure 37 Priority Configuration GUI

In the **Priority Configuration** GUI:

- The table (to the left in Figure 37) lists all the configured priority rules.
- When clicking one item in the table, the slide-in panel (to the right in Figure 37) shows the details of a priority rule.

9.1 Add or Edit a Priority Rule



To add a priority rule (edit has a similar operation):


In the **Priority Configuration** GUI

1. Click **Add Priority Configuration** to open the priority rule slide-in panel.




Save

 Delete |  Hide →


MOType 

Subscription@http://schemas.ericsson.com/pg/hlr/

XPath 

//*

Priority

1 

2. Configure the priority rule condition according to the description in Table 26.

Table 26 Priority Rule Condition Fields

Field	Description
MOType	Specify the MOType of the Asynchronous CAI3G request or the Synchronous CAI3G request in this field.
XPath	<p>Specify the XPath condition expression in this field. The expression can be defined base on the content of the CAI3G request⁽¹⁾; the expression must compliant with the XPath semantics.</p> <p>It is allowed to configure different priorities using different XPath with same MOType. When the CAI3G request is to be matched by multiple XPath conditions, Dynamic Activation only assigns the highest priority (see the description of Priority) of the matched XPaths to the CAI3G request.</p> <p>For example:</p> <p>The priority of XPath <code>/root/*</code> has been set to 2. The priority of XPath <code>//*[local-name() = 'root']//*[local-name() = 'abc']</code> has been set to 6.</p> <p>The priority of XPath <code>/*</code> has been set to 5.</p> <p>The request is granted priority 2 if XPath <code>/root/*</code> has been matched.</p>
Priority	<p>The priority of the expected asynchronous CAI3G request or the expected synchronous CAI3G request. If there is no priority configuration provided, the default priority for asynchronous CAI3G request is 5, and the default priority for synchronous request is 1.</p> <p>Multiple rules can be assigned with the same priority.</p> <p>Priority ranges: from 1 to 10 where 1 is the highest priority.</p>

(1) XPath, the XML Path Language, is a query language for selecting nodes from an XML document, refer to Reference [12] with the exception that “|” must be expressed as “or”.

3. Click


Save

 to apply the configuration.



9.2 Delete a Priority Rule

To delete a priority rule:

1. Click the row of the priority rule to be deleted.
2. Click  **Delete** and then click  **Yes** to confirm the deletion.





10 Retry Rule Configuration

Note: The Retry Rules Configuration for Processing Queues and for Request Management are similar.

In this chapter, **Retry Rules Configuration for Request Management** are described as an example.

Figure 38 shows the GUI used for configuring retry rules of sub-requests in Resource Queues. The provisioning requests are executed asynchronously, and unsuccessful ones are to be retried according to the configured retry rules.

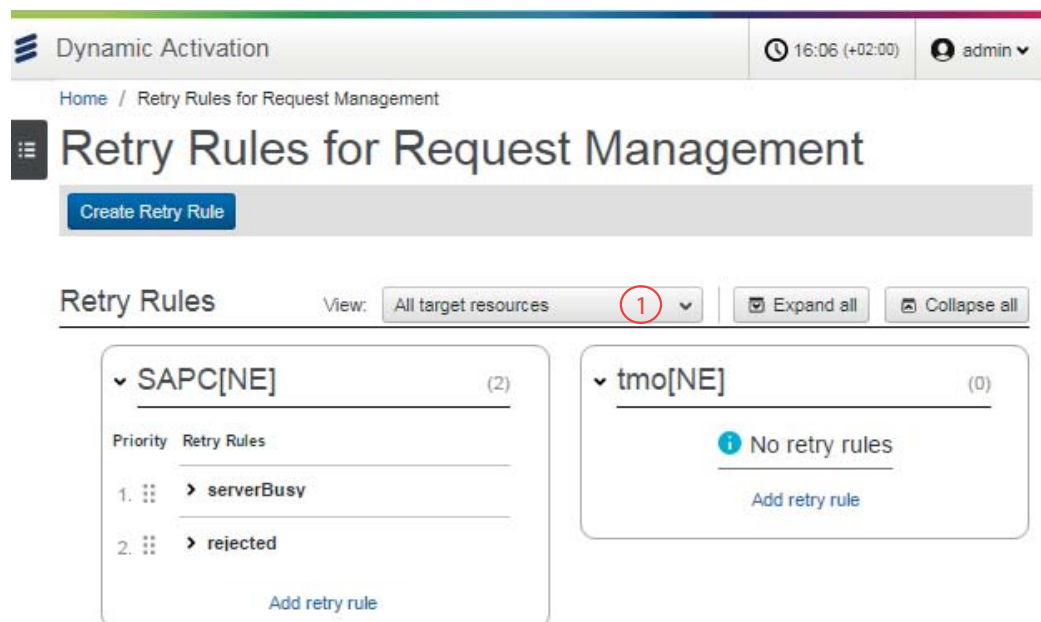


Figure 38 Retry Rule Configuration

By default, the **Retry Rule Configuration** displays all available target resources that Resource Queues are presenting. Users can choose to:

- Click the drop-down list (in area 1) and select desired target resources to display.
- Click **Expand all** (or **Collapse all**) to display (or hide) all retry rules that are configured in the displayed target resources.
- Click **Create Retry Rule** to add a new retry rule. See Section 10.1 on page 101.
- Expand a target resource and manage retry rules that are configured in it. See Section 10.2 on page 103.



10.1 Create Retry Rule

It is possible to add a retry rule based on a copy of an existing rule. For more information, see Section 10.2.4 on page 104.

To add a retry rule from scratch in the **Retry Rule Configuration** GUI:

1. Click **Create Retry Rule**. This opens the **Add Retry Rule** dialog.

Add Retry Rule

Rule Name
clientBusy

Target Resource
HLRFE-GROUP(group)

If either/both of the following occur

Error Code
1005

Error Message
The client is busy.

Then perform

Number of Retries
2

Retry Interval
2 Seconds

If number of retries is reached

Mark Subrequest as
Expired

Enabled

[Advanced settings](#)


☐ Send SNMP event

Save **Cancel**

2. Follow the instruction of GUI to configure the retry rule.

**Note:**

- Rule name must be unique within one target resource.
- If multiple retry rules have overlap conditions (Error code or Error message, or both), the rule with the highest priority in the target resource is applied to a sub-request.
- Mark Subrequest as Expired can be applied only to asynchronous traffic.

3. Click  to apply the configuration.

10.2 Manage Retry Rules

In the **Retry Rule Configuration**, an expanded target resource lists all retry rules that are configured in the Resource Queue, as shown as in Figure 39.

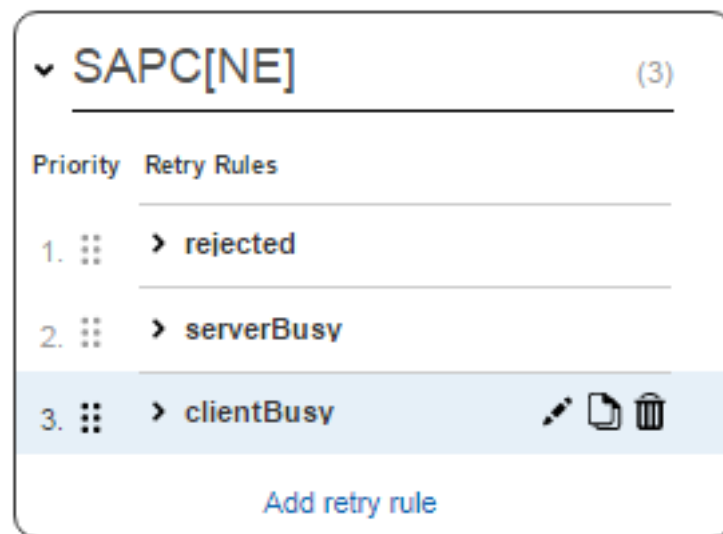


Figure 39 Manage Retry Rules

The retry rules are listed in a priority order (1 is the highest priority). A rule applies to a sub-request if one or more conditions of the rule are met, and the rest of the rules with lower priorities are not to be evaluated.

Hovering the mouse over a retry rule highlights the rule and shows more management operations.


10.2.1 View Retry Rule Details

In an expanded target resource, click > to view the details of a retry rule.



10.2.2 Change Retry Rule Priority

In an expanded target resource:

1. Hover the mouse over the  retry rule.
2. Drag and drop this rule to change its priority.

10.2.3 Edit Retry Rule

In an expanded target resource:

1. Hover the mouse over a retry rule, and click .

This opens a slid-in panel **Edit Retry Rule**.

2. Change the configuration of the retry rule. For more information, see Section 10.1 on page 101.


Note: The `Target Resource` cannot be changed when editing a rule.

3. Click  to apply the change.


10.2.4 Copy Retry Rule

It is possible to copy a retry rule to another target resource.

In an expanded target resource:


1. Hover the mouse over a retry rule, and click .

This opens the **Add Retry Rule** dialog.

2. Change the `Target Resource` to another target resource into which the retry rule is copied.
3. If needed, change the configuration of the copy.
4. Click  to add the copy as a new retry rule.

10.2.5 Delete Retry Rule

In an expanded target resource:

1. Hover the mouse over a retry rule, and click .
2. Click **OK** to confirm the deletion.



11 Asynchronous Request Management

The Asynchronous Request Management GUI shown in Figure 40 browses the information of asynchronous CAI3G requests that have not been executed successfully.

Dynamic Activation 14:35 admin

Home / Asynchronous Request Management

Asynchronous Request Management

① Mon May 16 2016 08 X Mon May 16 2016 08 X Priority priority1,priority2,... All Pending Executing Failed Search

②

Message Id	Priority	User	Message Id	MoType
JobId500	10	admin	6 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/
JobId499	9	cai3guser	6 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/
JobId498	8	admin	Mon May 16 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/
JobId497	7	admin	Mon May 16 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/
JobId496	6	cai3guser	Mon May 16 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/tt/13.5/
JobId495	5	admin	Mon May 16 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/
JobId494	4	admin	Mon May 16 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/
JobId493	3	cai3guser	Mon May 16 2016 08:22:04 GMT+0800 (China Standard Time)	Subscription@http://schemas.ericsson.com/pg/ss/13.5/

< 1 2 3 4 5 6 7 8 9 ... 25 >

Figure 40 Asynchronous Requests Management GUI

In the **Asynchronous Requests Management** GUI:

- Area 1 specifies the searching condition.
- Area 2 lists all the items matched the searching condition. The items are listed in descending order of `FireTime`.

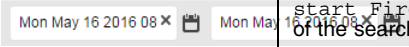
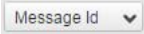

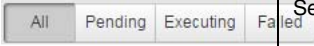
11.1 Search by Condition


To search the Asynchronous CAI3G Requests that have not been executed successfully:

1. In the searching bar, enter the search condition according to Table 27.



Table 27 Search Condition Fields

Field	Description
	<p>start Firetime and end Firetime are used to specify the time range of the search scope.</p> <p>If the start Firetime and end Firetime are both empty: the current time minus 30 mins is used as start FireTime. And the current time is used as end FireTime.</p> <p>If the start Firetime is empty, the end Firetime minus 30 mins is used as start FireTime.</p> <p>If the end Firetime is empty, the start Firetime plus 30 mins is used as end FireTime.</p>
	<p>Specify the keyword of the search condition.</p> <p>The search conditions are:</p> <ul style="list-style-type: none">• Message Id - specify the identity of the Asynchronous CAI3G request.• MoType - specify the MO Type of the asynchronous CAI3G request.• User - specify the username performed the request.• Priority - specify the priority of the Asynchronous CAI3G request.
	<p>Specify the value of the search condition. The search condition does not work if the text field is empty.</p> <p>Message Id and Priority support multiple entries separated by ",".</p>
	<p>Select condition based on the status of the requests.</p> <ul style="list-style-type: none">• All: shows all the items of Asynchronous CAI3G requests that have not been executed successfully.• Pending: shows the items of Asynchronous CAI3G requests in pending status.• Executing: shows the items of Asynchronous CAI3G requests in executing status.• Failed: shows the items of the failed Asynchronous CAI3G requests. Only the requests failed within 24 hours can be searched.

2. Click  to perform the search.

11.2 View Details of the Search Result

To view the details of the search result:

Note: There is no detail for failed request. To check the details of the failed requests, refer to *System Administrators Guide for Native Deployment*, Reference [5].

1. Click the row to be viewed, a slide-in panel is displayed to show details information.

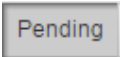

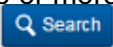


Details	Hide →
Message Id: JobId1	
Status: pending	
MoType: Subscription@http://schemas.ericsson.com/pg/tt/13.5/	
Receive Time: Mon May 16 2016 08:22:00 GMT+0800 (China Standard Time)	
Fire Time: Mon May 16 2016 08:22:00 GMT+0800 (China Standard Time)	
Group: gp_3	
User: admin	
Log Id: node11603310738370644CAI3G1_2/1	

- **Message Id** – see Table 27.
- **Status** – see Table 27.
- **MoType** – see Table 27.
- **Receive Time** – Indicates the time that the request has been received by system.
- **Fire Time** – Indicates the scheduled execution time of the request.
- **Group** – Indicates the Group ID of the request.
- **User** – see Table 27.
- **Log Id** – Indicates the Processing Log ID of the request.

11.3 Delete Pending Items

To delete one or more pending items:

- In searching bar, select  and specify other conditions (if needed) to list items of Asynchronous CAI3G request in pending status.
- Select the check box of one or more items to be deleted. Then a  button is displayed next to .



Message Id	Priority	User	FireTime	MessageType
a6b079e-c24a-431a-a5a0-76f501611115	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
e0bc847f-1719-4a48-a7b5-d0543784c1ac	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
72ba2527-4b08-405a-9b7e-30933567eb	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
88fa3244-a531-4802-a0f2-4bf5674243	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
689ea17c-080b-410f-4aae-12b2a09679c	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
13453816-cd2e-4b66-9a71-334f1b0a4e94	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
ac7c301c-5cd3-443f-9065-c7ac9cc9b02a	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/
6db0de5f-c291-43ec-9ab2-9da3d51dbcc5	5	ca3guar	1479672160000	Subscription@http://schemas.ericsson.com/ma/CS/AR/

- Click **Delete** and click **Yes** to confirm deletion.

11.3.1 Result of Delete Operation

A message that indicates the result of the delete operation shows on the top right corner of the window.

Message
Delete 8 pending jobs successfully.

Figure 41 Return Message of Delete Operation

Table 28 lists all the possible messages.

Table 28 Result of Delete Operation

Message ⁽¹⁾	Description
Delete <n> pending jobs successfully.	Indicates all the selected pending items have been successfully deleted. For example, Delete 7 pending jobs successfully.
Failed to delete pending jobs. Internal Server Error	Indicates that failed to delete any selected pending item.
Delete <total amount>-<n> of the pending jobs successfully, and skip <n> pending jobs.	Indicates that delete operation skips items that have been changed from pending to executing or other status during the deletion. The rest of the selected pending items have been successfully deleted. For example, Delete 5 of the pending jobs successfully, and skip 2 pending jobs.
Failed to delete job <n>, and delete <m> pending jobs successfully.	Indicates that system catches an exception when deleting (n) th pending item. m items are deleted successfully, n-1-m items are skipped. And the delete operation is ended. For example, Failed to delete job 5, and delete 3 pending jobs successfully.

(1) n,m=1,2,3...



The pending item that successfully deleted on GUI is sent a notification to BSS. This notification can be searched in the related Processing Log by its message ID, see Section 16 on page 143.



12 Request Management

The **Request Management** default GUI shown in Figure 42 provides visualized statistics of sub-requests in Resource Queues.

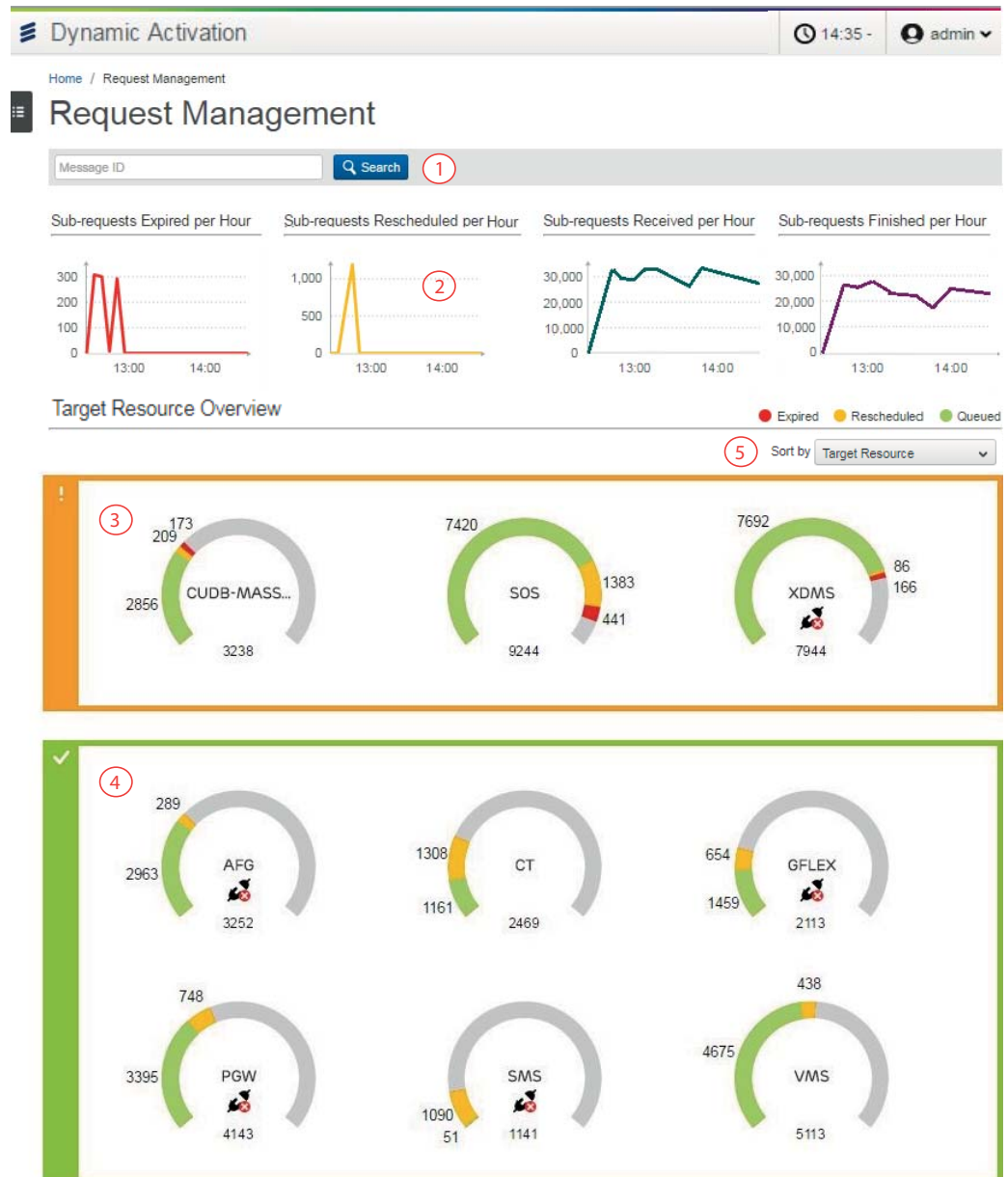


Figure 42 Request Management Default GUI

Area 1 provides search function to find all sub-requests that belong to one particular asynchronous request. This can be used for troubleshooting purpose. See Section 12.1 on page 113.

In area **2**, the line charts show the historical numbers of sub-requests over the latest 24 hours in all Resource Queues. Hover the mouse over the lines to see how many sub-requests there were at a certain time.

In area **3** and **4**, the gauge graphs show the current statistics of the individual Resource Queues.

The Resource Queues include:

- A default Resource Queue, `DefaultQueue`, contains requests that do not have a matching MO Type to NE Type mapping. Typically such requests target towards devices in the Resource Configuration solution, which do not involve NE or NE groups. But it can also be a request that targets an MO without a mapped NE Type.
- Each of the other Resource Queues represents an NE or NE group that is configured in the **Network Element GUI**. And each queue contains requests according to **MO Type to NE Type Mapping** configuration. See Section 8.3 on page 48 and Section 6 on page 27.

Figure 43 shows an example.

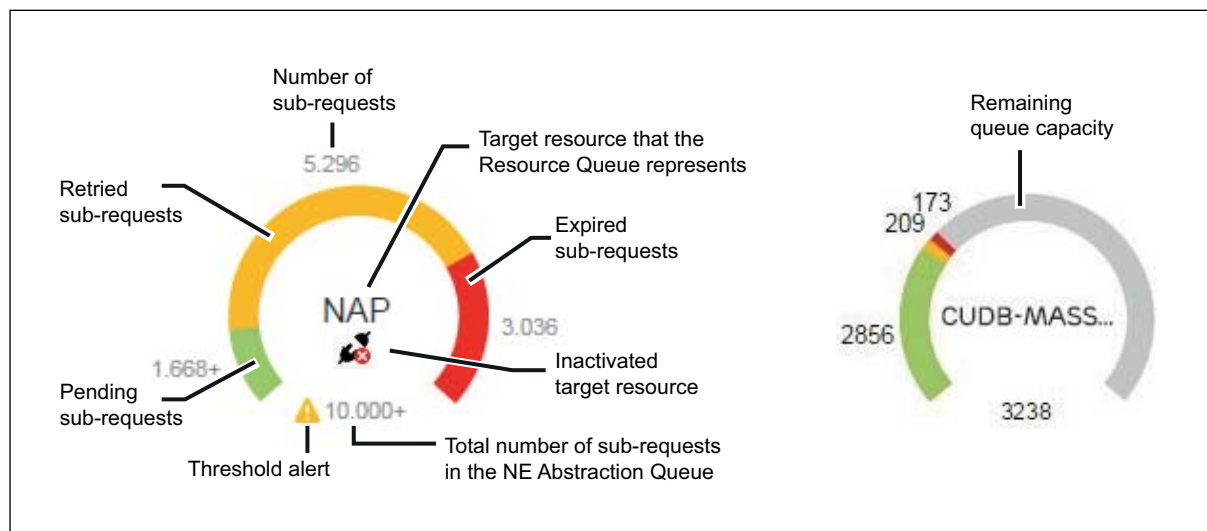


Figure 43 Resource Queue Statistics

Resource Queues that meet one or more of the following conditions are moved to area **3** from area **4** automatically:

- Includes expired sub-requests.
- With a threshold alert, which means that the number of sub-requests exceeds a specified capacity of the Resource Queue.

Note: The capacity configuration is not supported in the current release.

Available operations are:



- In area **3** and **4**, click a gauge graph to view details and manage the sub-requests in the Resource Queue. For more information, see Section 12.2 on page 114.
- In area **5**, use the drop-down list to sort the gauge graphs.

12.1 Search in Request Queues

Use the `Message Id` of an asynchronous request as a keyword for search, the **Request Management** GUI searches all Resource Queues in the Dynamic Activation, and lists all sub-requests that belong to the asynchronous request as a search result. Figure 44 shows an example.

The screenshot shows the 'Request: 441335348' page. It is divided into several sections:

- Request Information (Area 1):** Contains details about the request, including Message ID (441335348), Status (Halted), and Added to Queue time (Tue, 09 Aug 2016 14:40:40 GMT+02:00). It also has a 'Delete Request' button.
- Pending Sub-requests (Area 2):** A table listing sub-requests that are still in the Resource Queue. It includes columns for Status, Target Resource, Operation, Execute After, Last Triggered, and Retries. There are 'Send' and 'Cancel' buttons at the top.
- Finished Sub-requests (Area 3):** A table listing sub-requests that have been executed. It includes columns for Status, Target Resource, Operation, and Mo-Type.

Red circles in the original image highlight specific areas: (1) Delete Request button, (2) Pending Sub-requests header, (3) Finished Sub-requests header, and (4) Close button.

Figure 44 Search in Request Queues

Area **1** lists the detail information of the asynchronous request, whose `Message Id` has been searched. Users can delete this request or view its log if necessary.

Area **2** lists all the sub-requests that belong to the asynchronous request and are still in the Resource Queues. The following operations can be performed if needed:

- Click a row to view the sub-request details in a slide-in panel. For more information, see Section 12.2.2 on page 115.
- Tick the ☐ of one or more requests, and then click Send to resend those sub-requests, or click Cancel to delete them.

In area **2** and **3**, use to sort the sub-request lists in ascending or descending order.

Area **3** lists all the sub-requests that belong to the asynchronous request and have been executed.



Click **Close** **X** in area **4** to return to the default **Request Management** GUI.

12.2 Monitor and Manage Sub-requests

In the **Request Management** default GUI, click a gauge graph to show detail statistic or manage sub-requests in a chosen Resource Queue.

12.2.1 Monitoring Operations

The **Request Management** GUI provides filtering function for monitoring sub-requests that match certain criteria. Figure 45 shows an example.

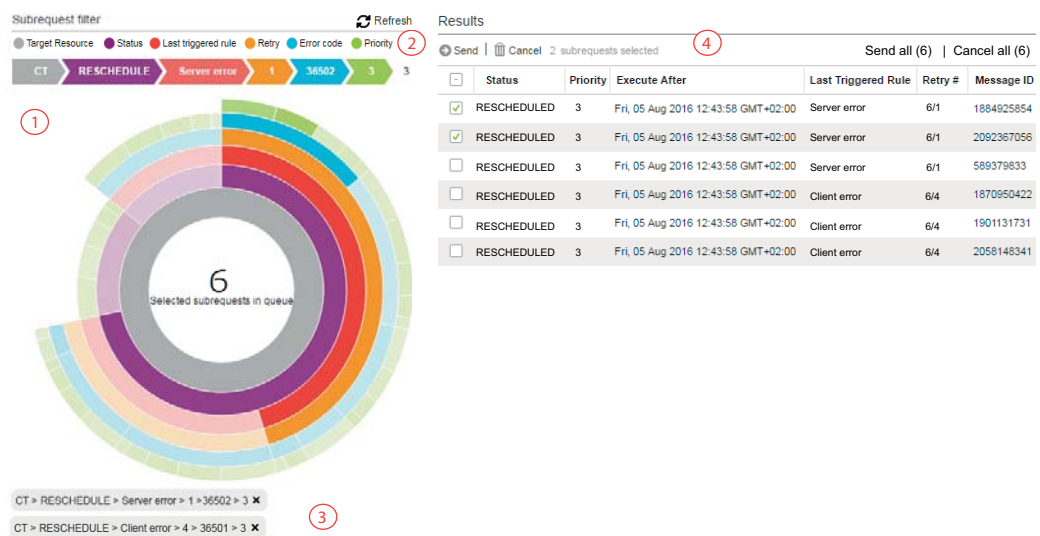


Figure 45 Monitor Requests in a Resource Queue

Without a Selected Filter

When there is no filter selected, the sunburst chart center in area **1** shows the total number of sub-requests in the current queue.

When hovering the mouse over the sunburst chart, area **2** shows the filter that is using, and the number of filtered-out sub-requests.

With Selected Filters

To select a filter, click the sunburst chart at where the desired filter is using. Multiple filters can be selected one by one.

When one or more filters are selected:

- Area **1** shows the number of filtered-out sub-requests in the center of the sunburst chart.



- Area **2** shows the selected filter, and the number of sub-requests that are filtered-out by the filter.

Click **Refresh** to reload the filters.

- The selected filters are listed in area **3**.
- Area **4** lists all the filtered-out sub-requests. For each sub-request, some or all the following information is given:
 - **Status** – Indicates that the sub-request is `QUEUED`, `RESCHEDULED`, or `EXPIRED`.
 - **Priority** – The priority of the associated northbound MO type of the request.



Note: For information on priority configuration, see Section 9 on page 97.

- **Execute After** – Indicates the scheduled date and time to send the sub-request.
- **Last Triggered Rule** – Indicates the retry rule that resents the sub-request.

Note: For information on retry rule configuration, see Section 10 on page 101.

- **Retry #** – Indicates maximum retry number and how many times the sub-request has been retried.
- **Message ID** – Indicates the identity of the corresponding asynchronous request.

Available operations in area **4** are:

- Click **Send all (n)** to resend all filtered sub-requests, or click **Cancel all (n)** to delete them.
- Click a row to view the sub-request details in a slide-in panel. For more information, see Section 12.2.2 on page 115.
- Tick the ☐ of one or more sub-requests, and then click  **Send** to resend those sub-requests, or click  **Cancel** to delete them.

Remove a Selected Filter

To remove a filter, click  of a desired filter in area **3**.



12.2.2 View Details of a Sub-Request

Click a row in area 4 of Figure 45, a slide-in panel is displayed to show more details of the selected sub-request.

Figure 46 shows an example.

Sub-request Details ✕

➔ Send | 🗑 Cancel

Status
EXPIRED

Target Resource
asd[NE]

Operation
Create

Execute After
Fri, 05 Aug 2016 12:43:58
GMT+02:00

Added to Queue
Fri, 05 Aug 2016 12:18:32
GMT+02:00


MO ID
uid: 10000

MO Type
Mock@http://schemas.ericsson.com/ma/CA/Test/

Retry #
11/10

[Copy Request](#)

[Copy Response](#)





[Log Management](#) >

Figure 46 Sub-request Details Slide-In Panel



The following operations can be performed if necessary:

- Click  **Send** to resend the sub-request.
- Click  **Cancel** to delete the sub-request.
- Click the **Copy Request** or **Copy Response** link to copy the sub-request message to clipboard.
- Click **Log Management** to view the log.
- Click **X** in the slide-in panel to close the panel.

12.3 Reschedule Expired Sub-requests

The **Request Management** GUI allows scheduling retry jobs for expired sub-requests in a chosen Resource Queue, as shown in Figure 47.

[Home](#) / [Request Management](#)

Request Management

asd[NE]

Close X

Schedule New Retry Job

Scheduled Retry Jobs

Wed, 10 Aug 2016 01:30:00 GMT+...

Figure 47 Add Scheduled Retry Jobs

Multiple retry jobs can be scheduled, where:


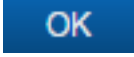

- All the expired sub-requests in a chosen Resource Queue is to be retried according to one or more scheduled jobs.
- Only one job is executed at a time, meanwhile other jobs are pending.

12.3.1 Add a Scheduled Retry Job

1. In the **Request Management** default GUI, choose a desired Resource Queue and click its gauge graph.

This shows the scheduler field for the Resource Queue.







2. Click  to choose a date and time, and click .
3. Click  to add a scheduled job.

12.3.2 Manage Scheduled Retry Jobs

When hover the mouse on a scheduled job, the editor and deletion buttons are

shown: .

Available operations are:

- Click  to edit the scheduled job:
 - 1 Select a new date and time for the job.
 - 2 Click  (or ) to apply (or cancel) the change.
- Click  to delete the scheduled job.

13 Processing Queue

Queued provisioning commands are executed in parallel for different subscribers, while in serials for the same subscriber. The **Processing Queue** GUI enables users to browse and manage sub-requests of these provisioning commands.

13.1 Browser Processing Queues

In **Processing Queue** default GUI, users can browse sub-requests per NE or NE group, or per cluster instance, and can sort the sub-requests by status, as shown in Figure 48.

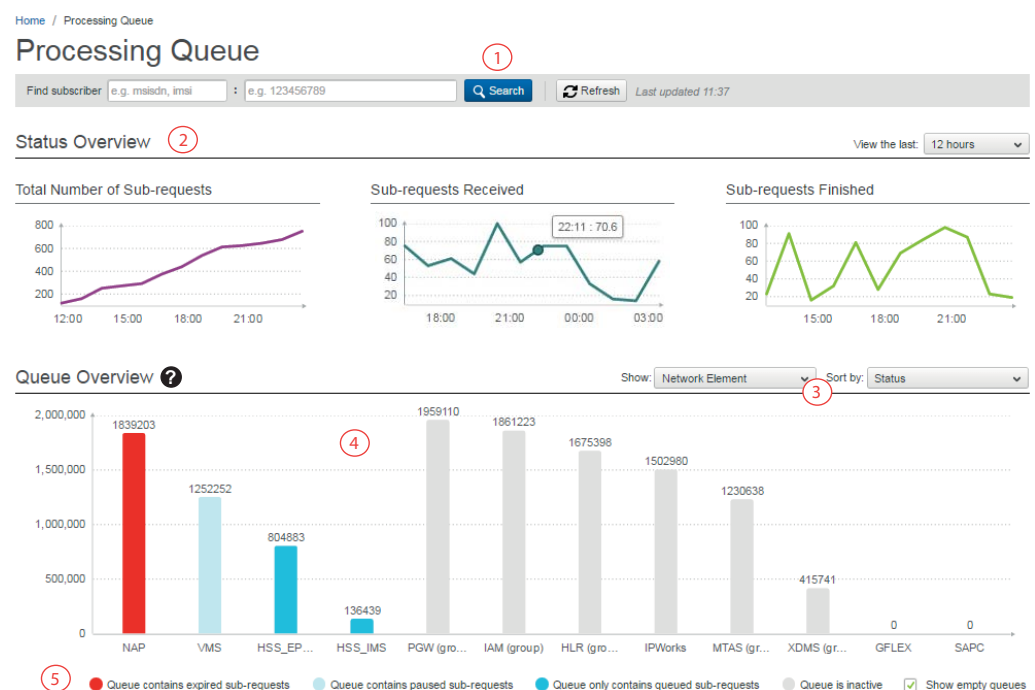


Figure 48 Processing Queue

In Figure 48:

- Area 1 provides search function to find all sub-requests that belong to particular subscribers, which are identified by the MO ID as follows:
(<MO ID type>:<MO ID value>)

For more information on the search results, see Section 13.2 on page 121.

- In area 2, the line charts show the historical numbers of sub-requests among all queues. Users can:



- Select the historical period as last 1, 12, or 24 hours.
- Hover the mouse over the line charts to see how many sub-requests there were at a certain time.

Note: The charts join sampling data points with straight-line segments, not showing exactly trend of the historical data.

For 1 or 12 hours history period, 12 data points are sampled. And 24 data points for 24-hour period.

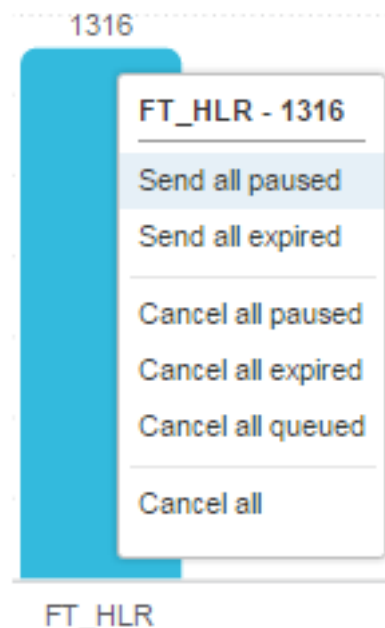
- In area **3**, use the **Show** drop-down list to select queues on what level to show:
 - Network Element – Show queues on all NE or NE groups.

Note: For NE or NE group configuration, see Section 8.3 on page 48.
 - Cluster – Show queues on all cluster instances.

Note: For NE cluster configuration, see Section 5 on page 19.

Use the **Sort by** drop-down list to sort the queues.

- Area **4** provides an overview of every queue. A column represents a queue.
 - For any queues, click a queue to manage sub-requests in the queue. For more information, see Section 13.2 on page 121.
 - For queues on Network Element level (selected in area **3**), right-click on a queue to pop up a shortcut menu.

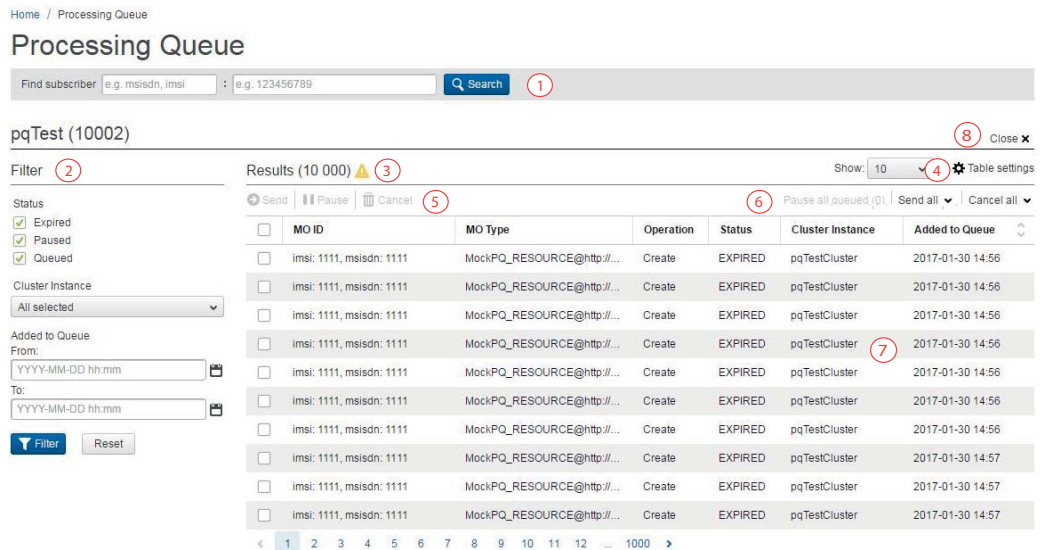


- Legends in area 5 can be used as filters. Click a legend to hide or show queues that match the filter.

13.2 Manage Processing Queues

Either by using search function, or by clicking a column that represents a queue, the **Processing Queue** lists all sub-requests that meets the criteria. Figure 49 shows an example.

Note: When the web page is reloaded, it is refreshed with new data from the system.



Home / Processing Queue

Processing Queue

Find subscriber e.g. msisdn, imsi : e.g. 123456789 1 Search

pqTest (10002) 8 Close x

Filter 2 Results (10 000) 3 Show: 10 4 Table settings

Status 5

- ☒ Expired
- ☒ Paused
- ☒ Queued

Cluster Instance

Added to Queue

From: YYYY-MM-DD hh:mm

To: YYYY-MM-DD hh:mm

Filter Reset

MO ID	MO Type	Operation	Status	Cluster Instance	Added to Queue
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:56
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:57
imsi: 1111, msisdn: 1111	MockPO_RESOURCE@http://...	Create	EXPIRED	pqTestCluster	2017-01-30 14:57


1 2 3 4 5 6 7 8 9 10 11 12 1000

Figure 49 Manage Sub-requests in Process Queues

In Figure 49:


- In area 1, the search function is used for searching all sub-requests of particular subscribers from system. This means that it refreshes the **Results** table with new sub-requests, instead of searching in the current table.
- Area 2 lists available filters that can be used to filter the sub-requests in the current **Results** table.

Set one or more filters and click  to apply the filters.

- In area 3, If  is shown, it means that the results exceed the table capacity and only 10000 of them are list in the table. (For example, in Figure 49, the total result is 10002) The listed results are displayed by status priorities (Expired>Paused>Queued), and then by time (oldest first).

Users can:



- Use the filters in area **2** to narrow down the results.
- Sort the results by using Added to Queue .

Note: The sort function takes effect on the data since last refresh, not in the real-time system.

- In area **4**, users can set the properties of the **Results** table.
 - **Show** drop-down list – Set how many rows to show on a page.
 - **Table settings** – Hide or show table columns, or change columns order.
- Area **5** is used to change status for selected sub-requests. See Section 13.2.1 on page 123.
- Area **6** is used to change status for all sub-requests in a bunch. See Section 13.2.2 on page 124.
- In area **7**, click a row to view details of the selected sub-request in a slide-in panel.



Sub-request Details

×

MO ID:

msi: 41484140166228

msisdn: 41484140166228

MO Type:

Operation::

Create

Status

QUEUED

Network Element

FT_HSS_EPS

Cluster Instance:

FT_ActiveActive

Added to Queue:

2017-01-11 14:09

Last Sent:

2017-01-11 14:09

Last Triggered rule:

Number of Retries:

0

[View response](#)

[Find request in Log Management](#) >

Available operations are:

- Click **View response** link to view the response of the sub-request.
- Click **Log Management** to view the log.
- Click **×** to close the slide-in panel.
- In area **8**, click **×** to return to the **Processing Queues** default GUI.

13.2.1 Change Status for Selected Sub-requests

Users can change status for specific sub-requests among *Queued*, *Paused*, and *Expired*, or cancel the sub-requests.

To select sub-request(s) and change their status, do the following in the **Results** table in Figure 49.



1. Tick the ☐ of one or more sub-requests to select them.
2. In area **5** in Figure 49, do one of the followings:
 - Change status to **Queued** – Click **Send** to resend the sub-request to the queue.

This also changes all the former sub-requests for the same subscriber to **Queued** status.

When click **Send** on an **Expired** sub-request, all the sub-sequent requests for the same subscriber are changed to **Paused** status.

- Change status to **Paused** – Click **Pause**.

This also changes all the sub-sequent requests for the same subscriber to **Paused** status.

- Click **Cancel** to delete the sub-request if it is not ongoing.

Ongoing sub-requests cannot be deleted.

13.2.2 Change Status for All Sub-requests

Users can change status in a bunch for all sub-requests which are listed in the **Results** table, as shown in Figure 50.

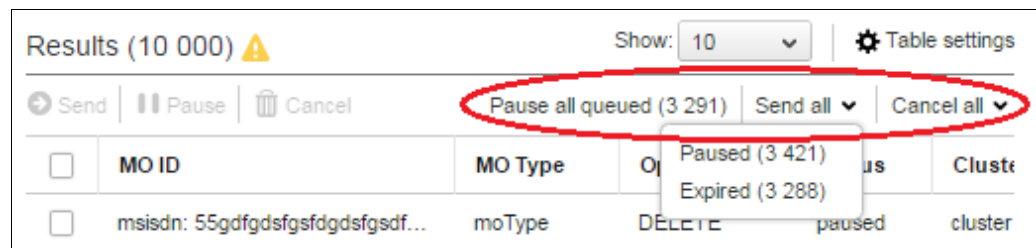


Figure 50 Change Status for All Sub-requests

To change status for all sub-requests in a bunch, click one of the following:

- **Pause all queued** – Set all listed sub-requests to wait in the queues.

The sub-requests statues are changed to **Paused**. If is shown, those sub-requests for the same subscribers but not listing in the **Results** table are also paused.

Note: This is a 1-click change. No confirmation is required.

- **Send all** – Depending on choice, resend all listed **Paused** or **Expired** sub-requests to the queues.

The sub-requests statues are changed to **Queued**.



Note: This is a 1-click change. No confirmation is required.

- **Cancel all** – Depending on choice, delete all listed Queued, Paused, Expired, or all the listed sub-requests from the queues.

After a confirmation, the change takes effect.





14 Dashboard

Dashboard shows provisioning performance in the last 36 hours. With the SW Advanced license, a seven days historical performance can be shown.

Note: The time displayed in the **Dashboard** refers to the server time instead of the local time.

14.1 General Settings

This section describes general settings in **Dashboard**.

14.1.1 Refresh Dashboard



Figure 51 Refresh Settings

- When **Auto-refresh** is enabled, dashboard refreshes the performance statistics from real-time system every 60 seconds.
- When **Auto-refresh** is disabled, use **Refresh** to refresh the performance statistics manually.
- If the monitoring period does not include the current time (Now), the **Auto-refresh** is inoperable.



If you want to enable the **Auto-refresh**, click **Latest** to include Now.

14.1.2 Select Monitoring Period

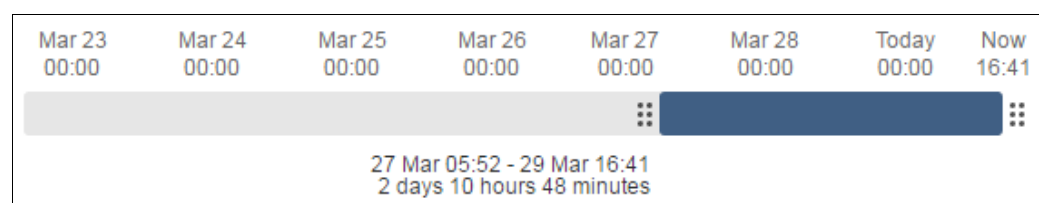


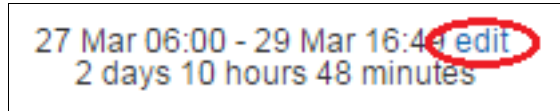
Figure 52 Select Monitoring Period

There are two ways to select a time span of the monitoring period.

- Fuzzy selection – Drag or in the time bar.




- Precise selection – Hover the mouse over the time text below the time bar, follow the **edit** link to specify the start and end points.




Note: If the end point is not **Now**, the **Auto-refresh** is disabled for the **Dashboard**.

14.1.3

Choose Widgets

Click **Settings**  and then choose desired widgets to display in **Dashboard**.

- Use ☐ to (un)hide a widget.
- Drag and drop  to reorder a widget.

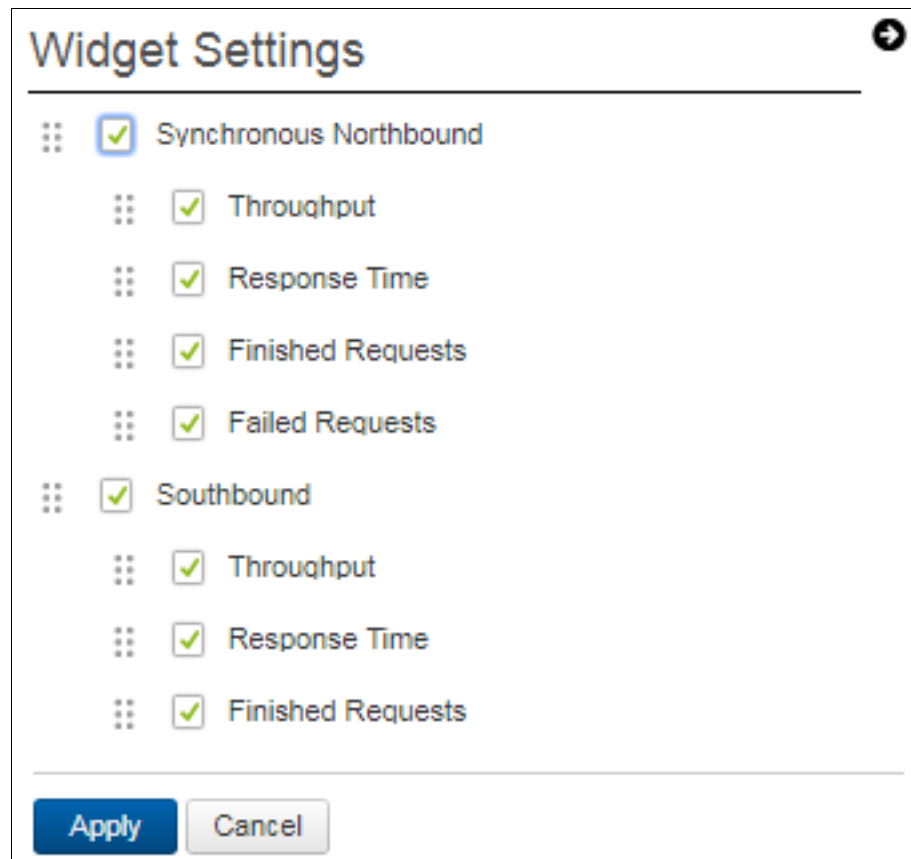
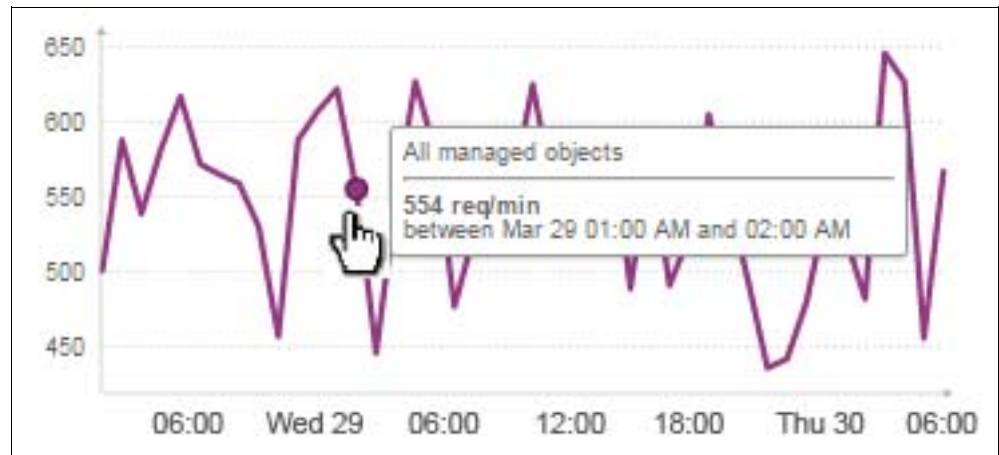


Figure 53 Change Widget Settings



14.1.4 View Statistics Details


- Hover the mouse over the chart.




- Expand the table below the widgets for details. For example, click [View each managed object](#) ▼

14.1.5 Change Table Settings

Click the setting button over the table header to change table settings, for

example Show: All operations ▼  :

- Use ☐ to (un)hide a column.
- Drag and drop  to reorder a column.



Northbound Table Settings

Finished Requests

Success Count

Success Rate

Failed Count

Fail Rate

Throughput (req/min)

Mean

Max

Min

Response Time (ms)

Mean

Max

Min

Apply

Cancel

Figure 54 Change Table Settings Example

14.2 Northbound Performance

Figure 55 shows the provisioning performance on the synchronous northbound interface.

Note: In the current release, only the synchronous interfaces are monitored.

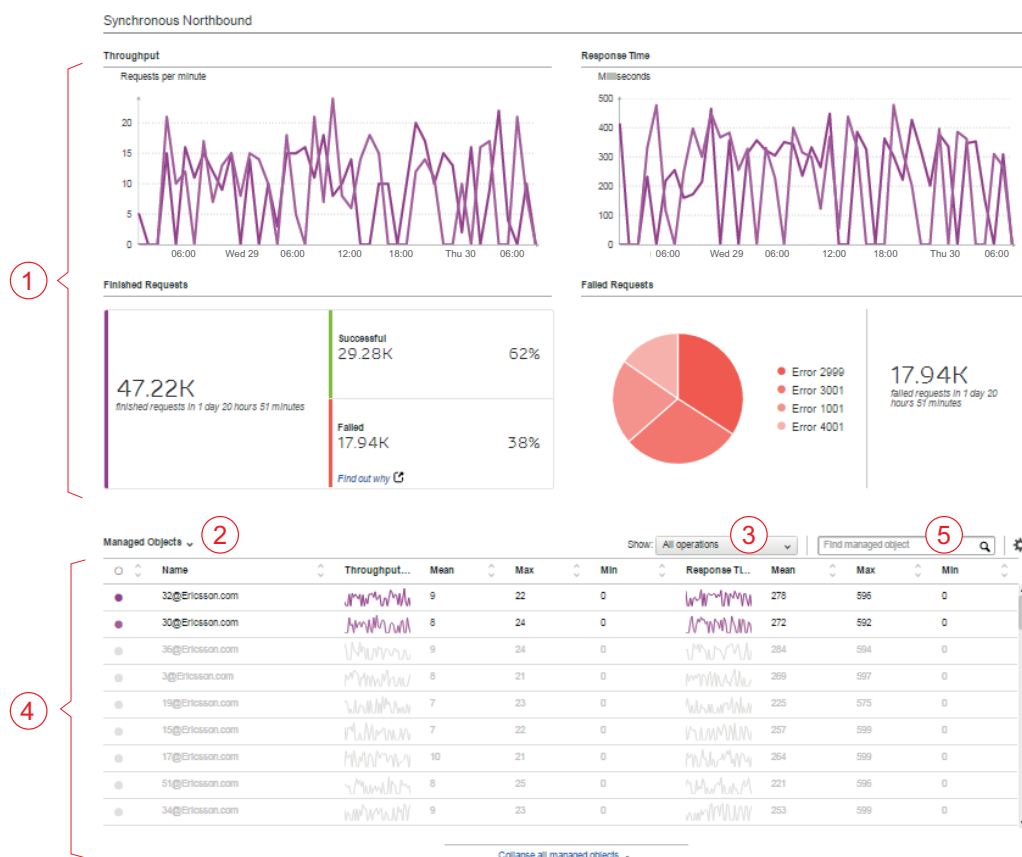
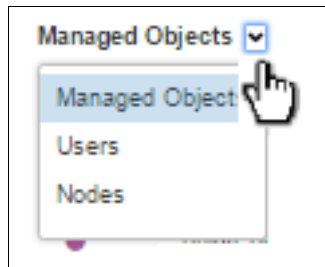
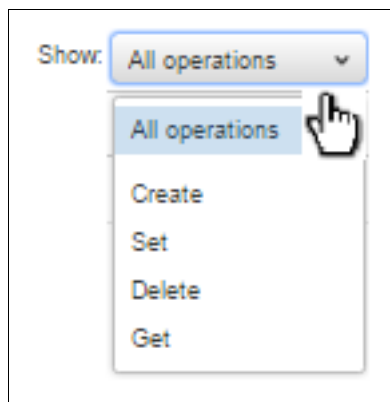


Figure 55 Synchronous Northbound Performance

- Area 1 displays widgets that are chosen in Section 14.1.3 on page 128.
 - When the table (area 4) is collapsed, the widgets show an overall performance trend.
 - When users expand and interact with the table (area 4), the widgets update the performance statistics accordingly.
 - In **Finished Requests** widget, click **Find out why** link to navigate to **Log Management** to view relevant logs for the failed provisioning statistics.
 - View charts in the widgets, see Section 14.1.4 on page 128.
- In area 2, user can select provisioning statistics based on Managed objects, Users, or Nodes.




- In area **3**, users can choose to view provisioning statistics of each or all operations.



- In area **4**, the table lists all provisioning statistics that are chosen in area **2** and **3**.

Available operations are:

- Click a row to select or deselect it. The performance statistics of all selected rows are shown in the charts in area **1**.

Note: The spot color in a row (for example ) always matches the color of the corresponding lines in the charts.

- Click the spot in the table header to select or deselect all rows.



- Click a column heading to sort the rows in the table.
- Change table settings, see Section 14.1.5 on page 129.

- Area **5** provides search function for users to locate desired items.

Note: The search function is available when the table is expanded.

14.3 Southbound Performance

Figure 56 shows the southbound provisioning performance monitor of the **Dashboard** GUI. This monitor is displayed when the **Southbound** widgets are selected. For more information, see Section 14.1.3 on page 128.

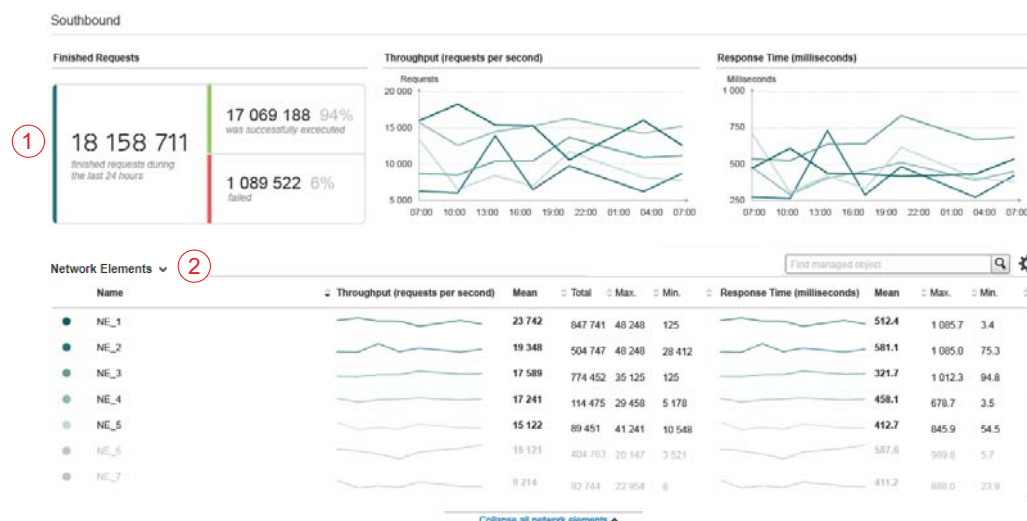


Figure 56 Southbound Performance Monitor

The southbound performance monitor has similar functions as the northbound one does, except:

- In area 1, there is NOT a **Find out why** link or a **Failed Requests** widget available for southbound performance monitor.
- In area 2, users can select provisioning statistics based on **Network Elements** or **Nodes**, but can not view statistics of each type of operations.

For more information, see northbound performance monitor described in Section 14.2 on page 130.





15 User Management

The **User Management** GUI is visible only for System Administrator users.

The default user admin (email admin@eda.com) is a System Administrator.

In this GUI, System Administrator users can create and manage GUI users as shown in Figure 57.

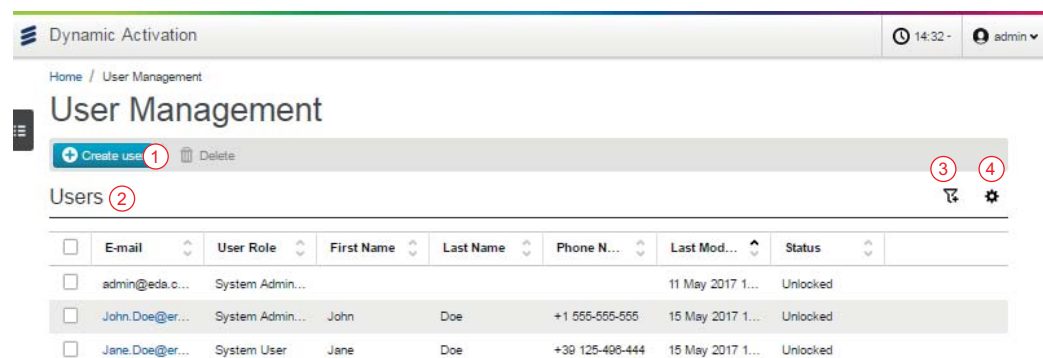



Figure 57 User Management

- In area 1, click **Create User** to add a new user. See Section 15.1 on page 136.
- Area 2 lists a **User** table, where available operations are:
 - Hover the mouse over a row to edit (✎) or delete (🗑) the selected user.
For edit operation, see Section 15.2 on page 138.
 - Unlock a locked user. See Section 15.3 on page 140.
 - Click a user email to view user details.
 - Delete one or more users by ticking ☐ and then clicking 🗑 Delete.
 - Click a column heading to sort the rows in the table.

Note: The default user admin@eda.com is defined during the installation. This user cannot be locked or deleted.


Deleting one or more users requires a confirmation in the popped up dialog.

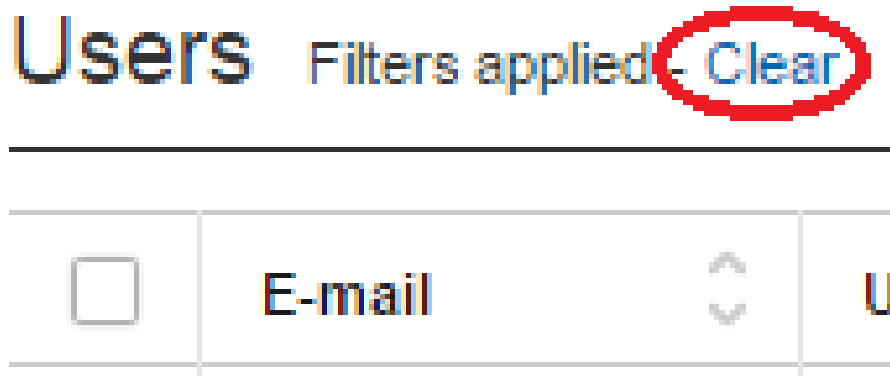



- In area **3**, click  to show the following filters in the **Users** table.


<input type="checkbox"/>	E-mail	User Role	First Name	Last Name	Phone Nu...	Last Modi...	Status
Type to filter	All	Type to filter	Type to filter	Type to filter	Type to filter	DD MMM YYYY	All

Available operations are:

- Type or select in the filters to narrow down the listed user.
- To clear a filter, do one of the following:
 - Clear the input field.
 - Set the filter to .
- To clear all filters, click **Clear** that is displayed besides the table title.



- In area **4**, click  to change the table settings.
 - Use ☐ to (un)hide a column.

Note: **Email** column cannot be hidden.
 - Drag and drop  to reorder a column.

15.1 Create a User

To create a user, do the following:

1. In the **User Management** GUI, click **Create User**.



Home / User Management / Create User

Create User

[Save](#) [Cancel](#)

User Information

E-mail*

forrest.gump@ericsson.com

First Name Last Name

Phone Number

Country 123-456 789

User Role*

Please select

- System Administrator
- System User

2. Enter the user information.

- If **First Name** and **Last Name** are not defined, the user email will be shown on the top of the GUI after the user logs in.
- When selecting the **User Role**:
 - System Administrator – A user that has access to the **User Management** GUI. Therefore s/he can create and manage other users.
 - System User – A user that can only view or edit her or his own user profile.

3. Click **Save** to go to the next page to get a generated password for the user.

Home / User Management / Create User

Create User


[Back](#)

The user was successfully created

Copy the password and send it to
forrest.gump@ericsson.com
for him/her to use at the first time login

<[r+]K2IK7P



4. Click  to copy the newly generated password, and then manually send it to the user through an email.

The user will be forced to change password after the first logon.

Note: Password rules to fulfill for a new password can be configured. For instructions, refer to:

- *System Administrators Guide for Native Deployment*, Reference [5]
- *System Administrators Guide for Virtual and Cloud Deployment*, Reference [6]

5. Click **Back** to return to the **User Management** GUI.

The newly created user is listed in the **Users** table.


15.2 Edit a User

This section describes how to change a user profile.

To edit a user, do the following:

1. In the **User Management** GUI, find the desired user to be edited.


Filters can be enabled by clicking  for a quick search.

2. In the **Users** table, do one of the following to open the **Edit User** GUI.
 - Hover the mouse over the row of the user, and then click .
 - Click the user email to go to the **User Details** GUI, and then click **Edit**.



Home / User Management / Edit User

Edit User

 Save Cancel

User Information

E-mail


First Name Last Name

Phone Number

User Role*

System Administrator
System User

Generate New Password





Send the newly generated password to the user.

3. Edit the user information as desired.

Note: **Email** cannot be edited. Delete the old email and create an one if desire to change.

4. To create a password for the user, do the following:
 - a. Click **Generate**, and confirm the operation.

Note: The password takes effect immediately, even before clicking **Save**.

- 
 - b. Click  to copy the newly generated password, and then manually send it to the user through an email.

The user will be forced to change password after the first login.



Note: Password rules to fulfill for a new password can be configured. For instructions, refer to:

- *System Administrators Guide for Native Deployment*, Reference [5]
- *System Administrators Guide for Virtual and Cloud Deployment*, Reference [6]

5. Click **Save** to apply the change.


15.3 Unlock a User

A user is locked if there are too many invalid logon attempts.

When unlocking a user:

- There are two ways to unlock a locked user:
 - In the **User Management** GUI, hover the mouse over the locked user and click the unlock icon.



Note: If **Status** column is not shown, click  to unhide it.

- In the **User Details** GUI, which is accessed by clicking the user email in the **User Management** GUI, click **Unlock**.



Home / User Management / User Details

User Details

← Back Edit Delete user

Sherlock Holmes

E-mail	First Name	Last Name
sherlock.holmes@ericsson.com	Sherlock	Holmes

Phone Number

(+46) 708-866534

User Role

System User

Status

Locked (due to too many invalid login attempts)

Unlock

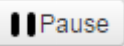
- Normally a new password needs to be generated for the user.
For instructions, see Section 15.2 on page 138.



16 Log Management

From the **Log Management** link it is possible to retrieve processing log information about the provisioning traffic, see Figure 59.

To view processing logs, a search is to be done first, as described in Section 16.1 on page 146. When the search is started, northbound requests are visible to the right. By clicking one of the requests, detailed information about the

whole transaction is displayed. Also, a new button is displayed . This to be able to pause the current search to, for example click a specific log and see detailed information about it.

For supported **Log Management** search use cases, see Figure 58.

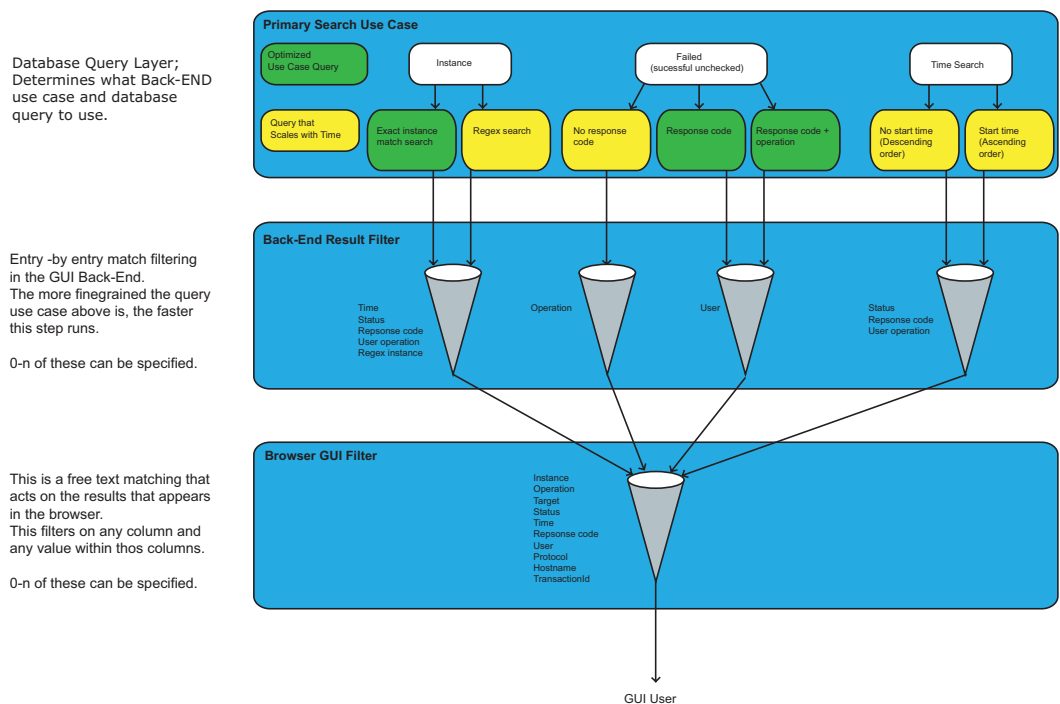


Figure 58 Log Management Search Use Cases

A general search rule is that the more specific the Time interval for the search is, the faster and more exact the result is to be.

The primary search functionality is determined by the given search input, which is prioritized in the following order:

- 1 Instance
- 2 Failed (successful unchecked)



3 Time search

One search follows only one path (see Figure 58), and ends up in the user GUI.

The **Table Settings** is used to set column preferences of the search results. Available operations are:

- Display or hide columns.
- Change column orders.

The **Go to page** field is used to more easily navigate to a specific page.

Dynamic Activation

14:35 - admin

Home / Log Management

Log Management

← Hide

Search

Clear

Instance

Regex

Start Time

Mon Dec 14 2015 16:01:46 GM

End Time

Tue Dec 15 2015 16:01:52 GM

Advanced

Successful

Failed

Response Code

User

Hostname

vmx1827 vmx1828

Managed Object

Operation Type

All operations

Results Per Page

50

Max Results

1000

Search

Cancel

Northbound results (13)

Filter...

Instance	Hostname	Operation	Status	Time	Respons...
batchJobId=c52e396d-5f2c-425c-a...	vmx1827	SET	●	2017-05-24 13.42.30.686	200
batchJobId=	vmx1827	CREATE	●	2017-05-24 13.42.24.255	200
batchJobId=c40caa35-f088-4d91-b...	vmx1827	SET	●	2017-05-24 13.39.46.295	500
batchJobId=c40caa35-f088-4d91-b...	vmx1827	SET	●	2017-05-24 13.39.30.850	200
batchJobId=	vmx1827	CREATE	●	2017-05-24 13.39.15.650	200
batchFile=test1	vmx1827	CREATE	●	2017-05-24 13.38.55.685	200
batchFile=test	vmx1827	CREATE	●	2017-05-24 13.38.28.749	200
	vmx1827	CREATE	●	2017-05-23 12.10.56.649	0
	vmx1827	CREATE	●	2017-05-22 14.06.44.394	0
	vmx1827	DELETE	●	2017-05-22 14.04.31.355	
	vmx1827	DELETE	●	2017-05-22 14.04.17.667	
	vmx1827	CREATE	●	2017-05-22 14.03.29.874	
	vmx1827	CREATE	●	2017-05-22 11.15.21.249	0

Go to page

1

Table Settings

Figure 59 Log Management First Page

The following table describes the parameters used for **Log Management**.



Table 29 Log Management Parameters

Parameters	Description
Instance	<p>For CAI3G request:</p> <p>Unique identifier, for example <code>msisdn</code>, <code>imsi</code>, <code>context</code>.</p> <p>What identifier that is used as Instance depends on what is included in the MOld and also the <code>context</code> in the header of the request message. The MOld for a specific MO type can be found in the respective CAI3G interface specification.</p> <p>For CAI request:</p> <p>All parameters that have only one value are used as Instance except Subscriber Data (SUD) and Password (PWD). The parameters are separated by colon ":".</p> <p>For MML request:</p> <p>All parameters that have only one value are used as Instance except SUD. The parameters are separated by comma ",".</p> <p>Note: It is possible to search for several parameters at once by enabling regular expression search (selecting the regex check box), and then use the regular expression.</p>
Regex	<p>Enables the possibility to run an instance search with regular expressions.</p> <p>Select the check box <code>Regex</code> and type a valid regular expression, before performing a Search.</p> <p>For example: <code><instanceType>=<instanceValue> <instanceType>=<instanceValue></code>. This search returns anything that matches either the first or the second statement separated by the " " operator.</p> <p>Note: Regular expression syntax must be followed strictly. In the above example, spaces are not allowed before or after the " " operator.</p> <p>If an exact match search is required, leave the <code>Regex</code> check box unselected.</p>
Start Time	<p>The start date and time (Local time-zone for user). Limits the search to only return logs after specified time.</p> <p>Only dates that contain logs can be selected in the pop-up dialog. It is also possible to select hour, minute, and second.</p> <p>The Start Time can also be set manually.</p>
End Time	<p>The end date and time (Local time-zone for user). Limits the search to only return logs before specified time.</p> <p>Only dates that contain logs can be selected in the pop-up dialog. It is also possible to select hour, minute, and second.</p> <p>The End Time can also be set manually.</p>
Successful	Checked if the search returns logs with status "successful".
Failed	Checked if the search returns logs with status "failed".
Response Code	If information is entered here, the search only returns logs of the specified response code.
User	If information is entered here, the search only returns logs of transactions initiated by the specified user. Multiple users can be used as search conditions.
Hostname	If information is entered here, the search only returns logs of requests that are processed on the specified node. Multiple nodes can be used as search conditions.
Managed Object	If information is entered here, the search only returns logs of the specified MO type. Multiple MO types can be used as search conditions.



Parameters	Description
Operation Type	If information is selected here, the search only returns logs of the specified operation type. Available operation types are GET, CREATE, SET, LOGIN, LOGOUT, DELETE, and All operations.
Results Per Page	Number of logs in the northbound result table. Available options are 10, 20, 50, and 100.
Max Results	Maximum number of logs to be fetched before terminating the search. Available options are 1000, 2000, 3000, 5000 and 10000.
Managed Object	Shows the MO type of the log.
Protocol	The protocol of in the specific request.
Hostname	The hostname of the node where the request is processed.
RootLogId	RootlogId identification of every log entry is a global unique with sublogId. It consists of: <i>[Hostname] [datetime] [sequence number] [protocol]</i> Example: E7009C021F0A271410201537470018CAI3G1_2
Time	Time when the log was stored. (Presented as local time-zone of the Dynamic Activation cluster server)
Execute time	Total time of a complete Northbound or Southbound request.
Response Code	The response code received for the request.
Transaction Id	The transaction id for the specific request.

16.1 Invoke a Log Search

To invoke a log search, enter information for the required parameters in the search area, as visualized in Figure 59. Details of the parameters are described in Table 29. The search returns logs that match the entered information.

The **Clear** button erases the information entered in the search area.

The **Pause** button is used to pause the current search to, for example click a specific log and see detailed information about it.

16.2 Filter Search

Filtering on search results is only possible when the search is terminated, either by cancellation or completion.


The filtering functionality filters the northbound result table. Type free text in the filter field. It filters on all columns of the result table and northbound request and response. Examples of filter queries are `msisdn=12345677` and `SET`.



16.3 Sort Search

Sorting on search results is only possible when the search is terminated, either by cancelation or completion.

The sorting functionality sorts the northbound result table. Click the arrows to the right of the parameter that the results are sorted by. For example, the following picture shows the result table sorted by instance.

Instance 	Operation	Managed Object
publicId=sip:12357	GET	Subscription@http://schemas.ericsson.com/ema/UserPr...
publicId=sip:12345	DELETE	Subscription@http://schemas.ericsson.com/ema/UserPr...
publicId=sip:12345	SET	Subscription@http://schemas.ericsson.com/ema/UserPr...
publicId=sip:+4688200701@t...	CREATE	Subscription@http://schemas.ericsson.com/ema/UserPr...
	LOGIN	
	LOGOUT	

16.4 Cancel Search

It is possible to cancel an ongoing search by pressing the **Cancel** button. The already found results are displayed on the screen until the user creates a search or refreshes the page.

16.5 View Detailed Northbound and Southbound Information

To be able to view detailed information about the log, it is necessary to have an ongoing or finished search.

As shown in Figure 60, the northbound and southbound requests are shown down at the left of the page. When pressing one of these requests, the information field on the upper left-hand side displays general information about the request. The right side of the page displays the full request and response.

Note: Because of limitations on the GUI component, the GUI is limited to show 1000 southbound operations at a time, it could be that the entire log with all its southbound operations is not shown.

If that is the case, to view the entire log, use the Admin Tool to export the time-span containing the log. And then search for the southbound operations within that time-span. For more information about the Admin Tool and the export function, see section *Processing Log Admin Tool* in *System Administrators Guide for Native Deployment*, Reference [5] document.



Dynamic Activation

Home / Log Management / Detail

Log Management

← Hide

Information

Instance	publicId=sip:0102900026
Operation	DELETE
Managed Object	Service@http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/...
Status	SUCCESSFUL
User	cai3guser
Protocol	CAI3G1_2
Hostname	CL19-1-PL-3
RootLogId	CL19-1-PL-31506221150411575CAI3G1_2
Time	2015-06-22 11:50:41:157
Execute time	00:00:00:121
Response Code	0
Transaction Id	123123

Requests

Log type	Operation	Status	Time	Response...
↑ Northbound	DELETE	●	2015-06-22 11:50:41:157	0
↓ Southbound	DELETE	●	2015-06-22 11:50:41:261	0

Full Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns="http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared">
  <soapenv:Header>
    <cai3:SequenceId>083836c25d3441dc9813ade2f9dfb52d</cai3:SequenceId>
    <cai3:TransactionId>123123</cai3:TransactionId>
    <cai3:SessionId>083836c25d3441dc9813ade2f9dfb52d</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Delete>
      <cai3:MOTType>Service@http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared
      <cai3:NOId>
        <publicId>sip:0102900026</publicId>
      </publicId>
    </cai3:NOId>
    </cai3:Delete>
  </soapenv:Body>
</soapenv:Envelope>
```

Full Response

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Header>
    <SessionId xmlns="http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared">083836c25d3441dc9813ade2f9dfb52d</SessionId>
    <TransactionId xmlns="http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared">123123</TransactionId>
    <SequenceId xmlns="http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">083836c25d3441dc9813ade2f9dfb52d</SequenceId>
  </S:Header>
  <S:Body>
    <DeleteResponse xmlns="http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared">
      <NOId>
        <publicId>publicId xmlns="http://schemas.ericsson.com/ema/UserProvisioning/MTAS/Service/MME1Shared">sip:0102900026</publicId>
      </publicId>
    </NOId>
  </DeleteResponse>
</S:Body>
</S:Envelope>
```

Figure 60 Northbound Information



17 Loose Error Handling Management

From the **Loose Error Handling** it is possible to define and configure the Loose Error Handling rules, see Figure 61.

Note: The **Loose Error Handling** GUI is only accessible for the account who has the System Integrator role, the default account is `siadmin`.

Dynamic Activation					14:35
Home / Loose Error Handling					
Loose Error Handling					
Add Rule					
Rules					
<input type="checkbox"/>	Name	NE (Group) Name	Error Codes	Rule Description	
<input type="checkbox"/>	rulename_1	NE_1	1501	this is a description of rulename_1	
<input type="checkbox"/>	rulename_test	NE_2	1501 , 1502	this is a description of rulename_test	

Figure 61 Loose Error Handling

When click the rule name, a **Rule Detail** window shows on the right of the front page. It displays the details of a rule and supports the action of edit, duplicate, delete.



Dynamic Activation

14:35

Home / Loose Error Handling

Loose Error Handling

Add Rule

Delete

Rules

	Name	NE (Group) Name	Error Codes	Rule Description
<input type="checkbox"/>	rulename_1	NE_1	1501	this is a description of rulename_1
<input checked="" type="checkbox"/>	rulename_test	NE_2	1501 , 1502	this is a description of rulename_test

Rule Detail

rulename_test

this is a description of rulename_test

Network Element Type

CLASSIC_CUSTOM3

Network Element/Network Element Group

NE_2

Inbound Triggers

DeleteCustom3User@http://schemas.ericsson.com/ma/CA/Custom3/
SetCustom3User@http://schemas.ericsson.com/ma/CA/Custom3/

Outbound Triggers

CreateCustom3User_RESOURCE@http://schemas.ericsson.com/ma/CA/Custom3/
SetCustom3User_RESOURCE@http://schemas.ericsson.com/ma/CA/Custom3/

Error codes

1501 - User Already Exists.
1502 - User does not exist.

Edit

Duplicate

Delete

Cancel

Figure 62 Rule Detail

17.1 Rule Parameters

The following table describes the parameters for defining a rule.

Table 30 Rule Parameters

Parameters	Description
Name	Name of the rule, must be unique and fewer than 80 characters in length. And the characters ~ ! @ # \$ % ^ & * () < > + . ? are illegal. For example, rulename_test.
Description	Description of the rule, less than 1024 characters in length.
Network Element Type	Type of the network element For example, CLASSIC_CUSTOM3.
Network Element/Network Element Group	NE or NE Group that needs to deploy the Loose Error Handle rule. For example, NE_2.



Parameters	Description
Inbound Triggers	List of service JDV triggers For example, CreateCustom3@http://schemas.ericsson.com/ma/CA/Custom3/ .
Outbound Triggers	List of resource JDV triggers. For example, CreateCustom3_RESOURCE@http://schemas.ericsson.com/ma/CA/Custom3/ ,
Error codes	The Looseable Error Code which can be ignored by NE or NE Group. For example, 1001 - External Errors.

17.2 Adding a Rule

To add a rule, follow these steps:

1. Click **Add Rule**.
2. In **General**, specify the **Name**, **Description rule**, **Network Element Type**, and **Network Element/Network Element Group** of the rule according to Table 30.

Click **Next** or **JDV Information**.

3. In **JDV Information**, choose **Pre-defined Rules** or **Advance Rule**.
 - **Pre-defined Rules**- select a rule from the pre-defined rule list.
 - **Advanced Rule**- specify **Inbound Triggers**, **Outbound Triggers**, **Error codes** of the rule according to Table 30 .

Click **Next** or **Summary**.

4. In **Summary**, Click **Finish** to add this rule to system.

17.3 Removing rules

To Remove one or more rules, follow these steps:

1. In front page, check the check box on the left of the rule to be deleted.
2. Click **Delete**.

or

1. In **Rule Detail** page of the rule to be deleted, click **Delete**.

17.4 Editing a Rule

To edit a rule, follow these steps:

1. In **Rule Detail**, click **Edit** to edit this rule.



2. Click **Apply**.

17.5 Duplicating a Rule

To duplicate a rule, follow these steps:

1. In **Rule Detail**, click **Duplicate** to duplicate an existing rule.
2. Click **Apply**.



18 Appendix A - Standard Product Activation Logic

Table 31 shows all the standard product activation logic components that are available in Dynamic Activation.

Table 31 Standard Product Activation Logics

JDV-AAA-Monolithic-Provisioning
JDV-AAA-Provisioning
JDV-AF-Monolithic-Resource-Provisioning
JDV-AF-Monolithic-Service-Provisioning
JDV-AIR-Monolithic-Resource-Provisioning
JDV-AIR-Monolithic-Service-Provisioning
JDV-AUC-Massive-Provisioning
JDV-AUC-Subscriber-Provisioning
JDV-BCE-Resource-Provisioning
JDV-BCE-Service-Provisioning
JDV-CA-Provisioning
JDV-CG-AUC-CAI-Provisioning
JDV-CG-AUC-Provisioning
JDV-CG-HLR-CAI-Provisioning
JDV-CG-HLR-Provisioning
JDV-CG-MNP-CAI-Provisioning
JDV-CG-MNP-Provisioning
JDV-CSAPC-Monolithic-Resource-Provisioning
JDV-CUDB-IMSI-Changeover-Provisioning
JDV-CUDB-SUBDEL-Provisioning
JDV-CUDB-Subscriber-Provisioning
JDV-DAE-Provisioning
JDV-EIR-Provisioning
JDV-ENUM-Layered-Resource-Provisioning
JDV-ENUM-Monolithic-Resource-Provisioning
JDV-ENUM-Service-Provisioning
JDV-ESIM-SV-Provisioning
JDV-FNR-Monolithic-Subscriber-Provisioning
JDV-HLR-Massive-Provisioning
JDV-HLR-Profile-Provisioning



JDV-HLR-Service-Associated-Data-Provisioning
JDV-HLR-Monolithic-Subscriber-Provisioning
JDV-HSS-AVG-Provisioning
JDV-HSS-EPS-Massive-Provisioning
JDV-HSS-EPS-Provisioning
JDV-HSS-IMS-Provisioning
JDV-HSS-Monolithic-Provisioning
JDV-ILF-Resource-Provisioning
JDV-ILF-Service-Provisioning
JDV-M2M-Provisioning
JDV-M2M-Service-Profile-Provisioning
JDV-MML-Converter
JDV-MNP-Provisioning
JDV-MTAS-Resource-Provisioning
JDV-MTAS-Service-Provisioning
JDV-PGM-Document-Resource-Provisioning
JDV-PGM-Document-Service-Provisioning
JDV-PGM-User-Resource-Provisioning
JDV-PGM-User-Service-Provisioning
JDV-EMA-Scheduled-Procedures
JDV-SAPC-Layered-Resource-Provisioning
JDV-SAPC-Monolithic-Resource-Provisioning
JDV-SAPC-Service-Provisioning
JDV-VoWifi-SV-Provisioning



Reference List

Ericsson Documents

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *Configuration Manual for Resource Activation*, 2/1543-CSH 109 628 Uen
- [3] *Customer Adaptation Development Guide for Resource Activation*, 5/1553-CSH 109 628 Uen
- [4] *Function Specification Resource Activation*, 3/155 17-CSH 109 628 Uen
- [5] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [6] *System Administrators Guide for Virtual and Cloud Deployment*, 3/1543-CSH 109 628 Uen
- [7] *MTAS Provisioning over CAI3G*, 30/155 19-CSH 109 628 Uen
- [8] *User Guide for Designer Studio*, 10/1553-CSH 109 628 Uen
- [9] *Function Specification Dynamic Activation Execution Environment*, 3/155 17-CSH 109 628 Uen
- [10] *User Guide for Batch Handler*, 12/1553-CSH 109 628 Uen
- [11] *Northbound Interface Adapter Customization Development Guide for CLI-Based Protocol*, 26/1553-CSH 109 628 Uen

Online References

- [12] *XML Path Language (XPath) 3.0* <https://www.w3.org/TR/xpath-30/>